

**ВІЙСЬКОВИЙ ІНСТИТУТ
КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
ІМЕНІ ТАРАСА ШЕВЧЕНКА**

**ЗБІРНИК НАУКОВИХ ПРАЦЬ
ВІЙСЬКОВОГО ІНСТИТУТУ
КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
ІМЕНІ ТАРАСА ШЕВЧЕНКА**

Виходить 4 рази на рік

№ 80

Згідно Наказу МОН №1188 від 24.09.2020, п. №156 Додатку 5 «Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка» включено до категорії «Б» за спеціальностями:

- 124 – «Системний аналіз»;
- 126 – «Інформаційні системи та технології»
- 254 – «Забезпечення військ (сил)»
- 255 – «Озброєння та військова техніка»

КИЇВ – 2024

ISSN 2524-0056 (Print)
ISSN 2519-481X (Online)

**MILITARY INSTITUTE OF TARAS SHEVCHENKO NATIONAL
UNIVERSITY OF KYIV**

**COLLECTION OF SCIENTIFIC WORKS
OF THE MILITARY INSTITUTE OF TARAS SHEVCHENKO NATIONAL
UNIVERSITY OF KYIV**

It comes out 4 times a year

№ 80

According to the Order of the Ministry of Education and Science No. 1188 from 09/24/2020, item No. 156 of Appendix 5 «Collection of scientific works of the Military Institute of Taras Shevchenko National University of Kyiv» is included in category «B» by specialties:

- 124 – «System analysis»;
- 126 – «Information systems and technologies»
- 254 – «Supply of troops (forces)»
- 255 – «Armament and military equipment»

KYIV – 2024

УДК621.43
ББК 32-26.8-68.49

Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. К.: ВІКНУ, 2023. № 80. 144 с.

Голова редакційної колегії:

Ленков С.В. доктор технічних наук, професор, ВІКНУ;

Члени редакційної колегії:

Анісімов А.В.	доктор фізико-математичних наук, професор, член-кор. НАНУ, КНУ;
Барабаш О.В.	доктор технічних наук, професор, НТУУ «КПІ»;
Гунченко Ю.О.	доктор технічних наук, професор, ОНУ;
Жиров Г.Б.	кандидат технічних наук, старший науковий співробітник, КНУ;
Заславський В.А.	доктор технічних наук, професор, КНУ;
Карпінський М.П.	доктор технічних наук, професор, Університет у Бельсько-Бялій (Польща)
Лепіх Я.І.	доктор фізико-математичних наук, професор, ОНУ;
Петров О.С.	доктор технічних наук, професор, УНТ, Краків (Польща);
Погорілий С.Д.	доктор технічних наук, професор, КНУ;
Толок І.В.	кандидат педагогічних наук, доцент,
Хайрова Н.Ф.	доктор технічних наук, професор, НТУ «ХПІ»;
Хлапонін Ю.І.	доктор технічних наук, професор, КНУБіА;
Шаронова Н.В.	доктор технічних наук, професор, НТУ «ХПІ».

Редакційна колегія прагне до покращення змісту та якості оформлення видання і буде вдячна авторам та читачам за висловлювання зауважень і побажань.

Зареєстровано Міністерством юстиції України, свідоцтво про державну реєстрацію друкованого засобу масової інформації – серія КВ № 11541 – 413Р від 21.07.2006 р.

Відповідно до Наказу МОН України від 24.09.2020 № 1188 «Збірник наукових праць ВІКНУ імені Тараса Шевченка» внесено до категорії «Б» (технічні науки).

Затверджено на засіданні Вченої ради ВІКНУ від 25.01.24 р., протокол № 7.

Відповідальні за макет:

Литвиненко Н.І.,
Коваль Н. Б.
Романова О.Г.

Відповідальність за новизну і достовірність наведених результатів, тактико-технічних та економічних показників і коректність висловлювань несуть автори. Точка зору редколегії незавжди збігається з позицією авторів. Усі матеріали надруковані в авторській редакції.

Усі статті, що публікуються у збірнику, проходять обов'язкове рецензування, яке здійснюється за анонімною формою як для авторів, так і для рецензентів. Незважаючи на перевірку статей на антиплогіат остаточну відповідальність за плогіат несуть автори.

Видання безкоштовне.

Примірники збірників знаходяться у Національній бібліотеці України ім. В.І. Вернадського, у науковій бібліотеці ім. М. Максимовича, у бібліотеці Військового інституту та в наукових бібліотеках України згідно списку МОН. Електронна версія збірника розміщена на відповідних сайтах.

Видання індексується Google Scholar.

Адреса редакції: 03189, м. Київ, вул. Ю. Здановської, 81, тел./факс +38 (044) 521 – 33 – 82

Наклад 50 прим. Ел.адреса редактора: lenkov_s@ukr.net

Офіційний сайт журналу: <http://miljournals.knu.ua>

Chairman of the editorial board:

Lienkov S.V. doctor of technical sciences, professor, VIKNU;

Members of the editorial board:

Anisimov A.V. doctor of physics and mathematics, professor, corresponding member of. NASU, KNU;
Barabash O.V. doctor of technical sciences, professor, NTUU «KPI»;
Gunchenko Yu.O. doctor of technical sciences, professor, ONU;
Zhirov G.B. candidate of technical sciences, senior researcher, KNU;
Zaslavsky V.A. doctor of technical sciences, professor, KNU;
Karpins'kyj M.P. doctor of technical sciences, professor, University of Bielsko-Biala (Poland)
Lepikh Ya.I. doctor of physics and mathematics, professor, ONU;
Petrov O.S. doctor of technical sciences, professor, UNT, Krakow (Poland);
Pogorilyy S.D. doctor of technical sciences, professor, KNU;
Tolok I.V. candidate of pedagogical sciences, docent,
Khairova N.F. doctor of technical sciences, professor, NTU «KhPI»;
Khlaponin Yu.I. doctor of technical sciences, professor, KNUBiA;
Sharonova N.V. doctor of technical sciences, professor, NTU «KhPI».

The editorial board strives to improve the content and quality of the publication and will be grateful to the authors and readers for their comments and wishes.

Registered by the Ministry of Justice of Ukraine, certificate of state registration of printed mass media – KV series No. 11541 – 413P from 07/21/2006.

In accordance with the Order of the Ministry of Education and Science of Ukraine from September 24, 2020 No. 1188, «Collection of Scientific Works of the Military Institute of Taras Shevchenko National University of Kyiv» is included in category «B» (technical sciences).

Approved at the meeting of the Scientific Council of VIKNU from 25.01.24, protocol No. 7.

Responsible for the layout:

Lytvynenko N.I.,
Koval N. B
Romanova O. G.

The authors are responsible for the novelty and reliability of the given results, tactical-technical and economic indicators and the correctness of statements. The point of view of the editorial board does not always coincide with the position of the authors. All the materials are printed in the author's edition.

All articles published in the collection undergo a mandatory review, which is carried out anonymously for both authors and reviewers. Despite checking the articles for anti-plagiarism, the final responsibility for plagiarism lies with the authors.

The publication is free.

Copies of the collections are in the National Library of Ukraine named after V.I. Vernadsky, in the scientific library named after M. Maksymovych, in the library of the Military Institute and in the scientific libraries of Ukraine according to the list of the Ministry of Education and Science. The electronic version of the collection is posted on the relevant websites.

The publication is indexed by Google Scholar.

Address of the editorial office: 03189, Kyiv, str. Y. Zdanovska, 81, phone/fax +38 (044) 521 – 33 – 82

Edition of 50 copies

E-mail address of the editor: lenkov_s@ukr.net

Official website of the journal: <http://miljournals.knu.ua>

ЗМІСТ

ВІЙСЬКОВА ТЕХНІКА І ТЕХНОЛОГІЇ ПОДВІЙНОГО ПРИЗНАЧЕННЯ

Stepanov M., Lavrinenko V. An overview of components for energy efficient multimedia networks based on 5g radio access technologies	7
Георгадзе О.А., Пехота С.Г., Ключак О.М., Чайковська О.Є., Кондратюк С.М., Чорномаз О.О. Методичний підхід до оцінювання рівня боєздатності військової частини	14
Городнов В.П., Ковальов І.В., Дружинін В.С. Модель оцінки математичного сподівання швидкості витрати пального підрозділом Збройних Сил України	25
Купрінєнко О.М., Нагачевський В.Й., Кривцун В.І., Фтемов Ю.О., Міщенко Я.С., Заверуха Г.В. Методика визначення потреби в наземних роботизованих комплексах підрозділів Сухопутних військ	36
Маміч В. В., Максименко Ю.А., Шаршаткін Д.Ю., Маляганов В.В., Кароль Д.А. Особливості забезпечення військ розвідувальною інформацією	45
Муженко В., Цибізов А., Пекуляк Р. Метод антикризового управління в системі забезпечення національної безпеки щодо послаблення впливу негативних тенденцій безпекового середовища на процеси реалізації національних інтересів держави	51
Фелінський Г.С., Жиров Г.Б., Корчак О.В., Рєзніков М.І., Кононенко А.А. Моделювання розподіленого нелінійно-оптичного підсилення у телекомунікаційних волокнах TRUEWAVE ^{RS} та G.652	59
Фтемов Ю.О., Купрінєнко О.М., Ленков С. В., Мірошніченко О. В., Літвіненко Н. І. Удосконалення способів ведення інженерної розвідки в інтересах інженерної підтримки бойових дій військ (сил)	72

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Batrak Y., Tsopa N, Troianovska A. Automated invoice processing sistem based on rpa technologies An exploration of public key infrastructure applications across diverse domains: a comparative analysis	87
Khlaponin Y.I., Qasim N.H, Tarasiuk D.M Forecasting the state of telecommunication networks using quantile and logistic regression methods	91
Бармак О.В., Боровик О.В., Боровик Д.О., Скрипнік Т.К. Можливі варіанти удосконалення існуючих підходів до виявлення фейкових новин на основі використання потенціалу алгоритмів машинного та глибокого навчання, сегменту новинного контенту й емоцій у коментарях користувачів	98
Живилю Є.О., Злобін К.В., Кузь В.С. Вимоги з кіберзахисту інформаційно-комунікаційних систем та сервісів зв'язку під час їх розгортання та експлуатації на пунктах управління складових сил оборони та безпеки	118
Дані про авторів	132
Алфавітний покажчик	135
Редакційна політика та етичні норми	136
Порядок подання і оформлення статей до "Збірника наукових праць Військового інституту Київського національного університету імені Тараса Шевченка"	138

CONTENTS

MILITARY EQUIPMENT AND TWO-DESTINATION TECHNOLOGIES

Stepanov M., Lavrinenko V. An overview of components for energy efficient multimedia networks based on 5g radio access technologies	7
Heorhadze O.A., Piekhota S.H., Klyuchak O.M., Chaikovska O.E., Kondratiuk S.M., Chornomaz O.O. Methodological approach to assessing the level of combat capability of a military unit	14
Gorodnov V.P., Kovalev I.V., Druzhinin V.S. Model for assessment the mathematical expectation speed of fuel consumption by military subunits of the Armed Forces of Ukraine	25
Kuprinenko O., Nagachevskyi V., Kryvtsun V., Ftemov Y., Mishchenko Y., Zaverukha H. Methodology for determining the need for ground combat vehicles of the Army units	36
Mamich V. V., Maksimenko Y.A., Sharshatkin D.Y., Malyaganov V.V., Karol D. A. Features of providing troops with intelligence information	45
Muzhenko V.M., Tsybizov A.L., Pekuliak R.O. Method of anti- crisis management in the national security support system concerning impact reducing of the safe environment negative	51
Felinskyi G.S., Zhyrov G.B., Korchak O.V., Reznikov M.I., Kononenko A.A. Modeling of distributed nonlinear optical amplification in true wave and G.652 telecommunication fibers	59
Ftemov Y., Kuprinenko O., Lienkov S. V., Miroshnichenko O. V., Litvinenko N. I. Improvement of methods of conducting engineering reconnaissance in the interests of engineering support of combat operations of troops (Forces)	72
INFORMATION TECHNOLOGIES	
Batrak Y., Tsopa N., Troianovska A. Automated invoice processing system based on RPA technologies	87
Khlaponin Y.I., Qasim N.H., Tarasiuk D.M. Forecasting the state of telecommunication networks using quantile and logistic regression methods	91
Barmak O. V., Borovyk O.V., Borovyk D.O., Skrypnyk T.K. Possible options for improving existing approaches to fake news detection based on using the potential of machine and deep learning algorithms, sentiment of news content and emotions in user comments	98
Zhivilo E.O., E.A., Zlobin K.V., Kuz V.S. Requirements for cyber protection of information and communication systems and communication services during their deployment and operation at the control points of the components of the defense and security Forces	118
Data on Authors	132
Alphabetical Index	135
Editorial policy and ethical standard	136
The order of submission and registration of articles to the "Collection of scientific works of the Military Institute of the Taras Shevchenko National University of Kyiv "	138

**AN OVERVIEW OF COMPONENTS FOR ENERGY EFFICIENT MULTIMEDIA
NETWORKS BASED ON 5G RADIO ACCESS TECHNOLOGIES**

Modern society is actively transitioning into an information-based one, and multimedia technologies have become an integral part of this process. Thanks to the proliferation of wireless access networks, users are becoming more mobile, and the development of the fifth generation of mobile networks, known as 5G, is a significant step in the advancement of information and communication technologies. 5G networks offer low latency and reliable connectivity, expanding the capabilities of mobile internet and machine communication. However, along with the opportunities provided by multimedia communication, there is a responsibility to consider the impact of associated technologies on the environment, as well as to address new challenges and the need for prudent resource utilization. The article defines the concept of "multimedia" and discusses various aspects of this concept, including digital storage and processing of information, components (text, photos, audio, and video), interactivity, and hypertextuality. It is noted that the transmission of multimedia data and the use of information technologies are closely linked to wireless access networks.

The authors discuss challenges and solutions in the field of energy efficiency for networks. They provide statistics indicating that the information and communication technology (ICT) industry is responsible for a significant portion of global energy consumption and CO₂ emissions, with radio access networks being a major contributor. Various components and technologies that can contribute to the development of energy-efficient multimedia networks based on 5G radio access technologies are examined. Specifically, heterogeneous networks, non-orthogonal multiple access (NOMA) technologies, and multiple-input multiple-output (MIMO) technologies are highlighted as key components for achieving energy efficiency. The importance of using heterogeneous networks to reduce the distance between transmitters and receivers is emphasized, along with the possibility of putting small base stations into sleep mode when there is no network load. Technologies like NOMA and MIMO are discussed as crucial components for achieving spectral efficiency and energy efficiency. Additionally, the article focuses on wireless sensor networks (WSNs) and suggests ways to optimize them for energy efficiency. This includes operating sensor units only when necessary, implementing wireless charging, using energy-efficient optimization methods, and applying efficient routing schemes. The authors also highlight the role of green data centers in reducing CO₂ emissions and optimizing the use of green energy in high-performance networks. Methods such as using renewable energy sources, increasing the energy efficiency of hardware, and implementing energy-efficient routing are discussed. In conclusion, the article underscores the importance of energy efficiency and reduced CO₂ emissions in modern multimedia networks, particularly in the context of 5G networks. It calls for interdisciplinary efforts to address these critical challenges in the field of information and communication technologies.

Key words: multimedia, energy-efficient, WSN, 5G, HetNet.

Introduction. Modern society is shaping its socio-cultural and economic ties, effectively transforming itself into an information society. The modern technological form of the information society is multimedia technology [1].

The modern user of multimedia and information technology is a "mobile" user. Mobility is inextricably linked to wireless access networks. In particular, it is promising to increase the share of fifth-generation mobile networks, widely known as 5G networks, which is an important step in the development of information and communication technologies (ICT). 5G networks stand out from previous generations, providing low-latency and ultra-reliable connectivity, advanced mobile broadband and machine-type connectivity. 5G communication systems are aimed at continuously improving the "quality of experience (impressions)" (quality of experience, QoE), and increasing data rates.

Along with the opportunities provided by multimedia communication, comes the responsibility for the impact of related technologies on the environment, as well as new challenges and the need to use available resources wisely.

Multimedia. "Multimedia" refers to the complex manipulation of at least some of the information presented as continuous media data. Continuous media data means time-dependent data in multimedia systems (eg, audio and video data), which are manipulated in clearly defined parts over a time interval in accordance with established norms [2]. Thus, the multimedia resource is distinguished from the non-multimedia on several grounds [1]:

- Data is stored and processed digitally by using computer technology;
- Data consist of one or more components, such as text, photo, audio or video information;
- Interactivity, active interaction of resources, programs, services and people, etc;
- Contains hypertext.

Thus, "multimedia communications" refers to the transmission, protocols, services and mechanisms for discrete and continuous media over digital networks. But it is important to clarify that, for example, the transmission of digital video over a certain dedicated television network, is not multimedia data, if it is not possible to additionally transmit a certain type of discrete media data [2].

Challenges and solutions. The ICT industry is quite an energy-intensive environment. According to statistics, this industry is responsible for about 2-10% of world energy consumption and 2% of CO₂ emissions. It is important that radio access networks are responsible for 60% of the reported consumption and pollution [3]. The network does not stand still and constantly growing like a living organism. Intelligent devices are connected, and, in particular, the number of user devices is increased, cars, household appliances, etc. are connected. The number and quality of services provided in the network is growing, such as remote monitoring, road safety, real-time management, virtual, augmented reality and the development of the concept of the Internet of Things, etc. [4]. As a result, data traffic and networks' growth are expected to continue to grow exponentially.

Literature review. Increasing energy consumption and growing carbon footprint from cellular networks have led to constant offers of "green" solutions from researchers, governments, and in particular telecommunications providers. In addition to its environmental value, the goal of energy efficiency (EE) is also to reduce the operating costs of mobile network operators and increase user satisfaction by increasing the battery life of their devices. Thus, energy efficiency is an integral part of the new generation of networks. To control energy consumption, the need for efficient allocation of resources, optimal network planning, and the use of renewable sources has been identified. The challenge is to keep energy consumption at the same level, or even reduce it, against the background of increasing data transmission, along with an increase in the number of base stations (BS).

When describing an energy efficient network, it means the ability of radio interface technology to minimize energy consumption by the access network, relative to traffic bandwidth. An EE device is a device that can minimize the power consumed by its device modem, depending on specific traffic characteristics. The same definition applies to user equipment, which should support the speed of mobile broadband data while reducing power consumption. In general, the devices must meet the requirements set out in ITU-R M.2410-0 (Minimum requirements related to technical performance for IMT-2020 radio interface (s))[5].

In general, the mobile network consists of base stations and access points that allow mobile terminals to interact with the network core. In mobile communications, base stations are the main source of energy consumption. The reality of today's, is that 5G New Radio consume three times more energy than the base stations of the same LTE and use 10% of their energy efficiency.

Methodology. When discussing the energy efficiency indicators of base stations, certain metrics are used. The most commonly used efficiency metric is bit / joule. Therefore, the basic value of EE [6]: $EE (bit / joule) = (Data\ rate) / (Energy\ consumption)$.

One method to reduce consumption is to turn off BSs' components that they do not need or use during this period of time. From the point of view of the use of hardware resources, there are

several paradigms, namely - resource consolidation, virtualization, selective connection and proportional calculations [7]. These include the following:

- Resource consolidation involves the regrouping of underutilized resources. At different times, network infrastructure resources are loaded differently, depending on the specific traffic. Thus, all equipment that is designed for peak loads may not be needed at a particular time.
- Distributed selective connection mechanisms allow individual components on the edge of the network to stand for as long as possible, staying in standby mode, avoiding supporting network connection tasks in an open environment to the rest of the network.
- Virtualization allows more than one service to operate effectively within a single physical environment. This is effective because, for example, one heavily loaded computer can consume less than a few lightly loaded computers.
- The paradigm of proportional calculations is based on the correspondence of the amount of work performed to the amount of energy consumed by the device, described by Prem et al. [7].

The environmental friendliness of technology has become a must for wireless networks. Researchers talk about environmentally friendly "green radio". This term is firmly entrenched in

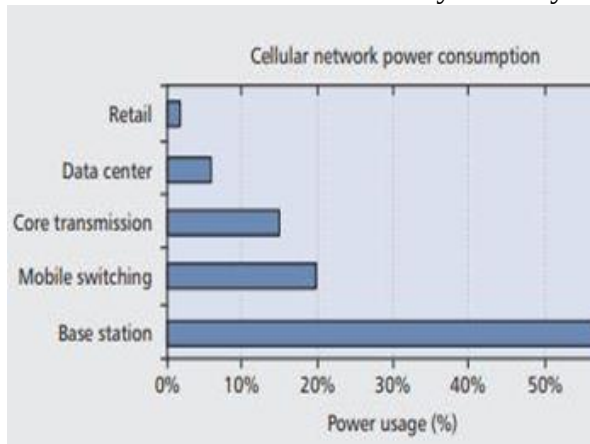


Figure - 1 Power consumption of a typical wireless cellular network [8]

academia and industry as a guideline in research and development of wireless networks, on the way to high energy efficiency [8]. Different elements of wireless networks consume different percentages of energy. Figure 2 shows an example of the power consumption of a typical wireless network. It is clear that it is necessary to increase the energy efficiency of base stations and access points. It is extremely important to increase the percentage of EE in networks with a large number of heterogeneous BS, without loss of bandwidth. Studies are being conducted to balance energy, spectral efficiency (SE) and sustainability of the 5G

network. From this point of view, three goals were set: first, to use unused spectrum, in particular unlicensed spectrum; second, to reduce the distance between receiver and transmitter, and to improve the frequency reuse; to increase spectral efficiency by deploying structures in large numbers. The technologies that achieve these goals increase system throughput.

HetNet. To reduce the distance between the receiver and the transmitter, it is proposed to use so-called heterogeneous networks (HetNETs). A heterogeneous wireless network uses a variety of connectivity technologies. That is, a heterogeneous network consists of subnets, with different technologies, and they all form a single integrated environment, which provides a seamless invisible to the user transition from one subnet to another. An access network consists of a macrocell and several small cells, such as a microcell, a picocell, or a femtocell. The backhaul network is formed by connecting the base station using a mixed, wired or wireless architecture. An example of a heterogeneous network is shown in Figure 3 [9].

Although macrocells control powerful radio beams and have a large coverage area, they can sometimes cover areas, most of which may be empty, i.e. without users. Thus, the power can be excessive and used in vain. Femtocells provide power where needed. Because they are closer to the user, they need less RF power for high bandwidth. The femtocell also offers EE features such as denser user coverage, better QoS capabilities, and longer battery life. Also, it is important that it is possible to put small cells in sleep mode, in the absence of load on the network [10]. It is important to be able to integrate femtocells into macrocells, creating different, necessary combinations for more efficient network planning.

Thus, HetNETs bring end users closer to network access, thus improving the signal-to-noise ratio as well as more efficient reuse of frequencies [9].

When describing the transfer of cells to sleep mode, it means a system that has been used in mobile transmitters in order to save battery life for a long time. The discontinuous transmission (DT) system makes it possible to transmit only when the need arises, otherwise the transmitter enters a low power state. As for the cell as a whole, this technology is already called cell DT and is based on hardware shutdown functions to ensure low power levels. There are two modes, fast-cell DT and long-cell DT. In the case of a fast-cell DT radio in the cell, may be in a microsleep state at intervals when user data is not transmitted. Long-cell DT works slower and belongs to the mode of low cell activity, this condition can be considered a cellular "sleep" with lower power consumption.

NOMA and MIMO. To achieve spectral efficiency and better frequency reuse, heterogeneous networks incorporate NOMA non-orthogonal multiple access technology. In NOMA, multiple users can operate in the same range simultaneously, being divided by power levels. The transmitter uses superposition coding so that the receiver, using a successive interference cancellation (SIC) unit, can separate users in both uplink and downlink lines. In SIC, decoding of simultaneously received packets is achieved by the receiver decoding first the stronger signal, subtracting it from the combined signal, and then decoding the difference as a weaker signal (fig.4) [11]. Thus, the incorporation of NOMA into small cells of heterogeneous networks using the well-known Multiple Input Multiple Output technology to serve N number of users, enabling efficient use of bandwidth and finding a trade-off between bandwidth and energy efficiency [12].

Also, a critical technology for building efficient wireless networks is multiple-input, multiple-output (MIMO) technology, which has already been successfully deployed in previous generation networks, both for time-division duplex (TDD) and for frequency division duplex (FDD). This technology is one of the mechanisms that allow achieving high speeds for data transmission with high spectral and energy efficiency in 5 G networks, at frequencies below 6 GHz [13]. It provides work at two levels: a macro level in the microwave bands for the implementation of control signals and a micro level in the bands mmWave for the transfer of user traffic. Massive MIMO is efficient in high-frequency bands and provides high antenna array gain, covering path losses

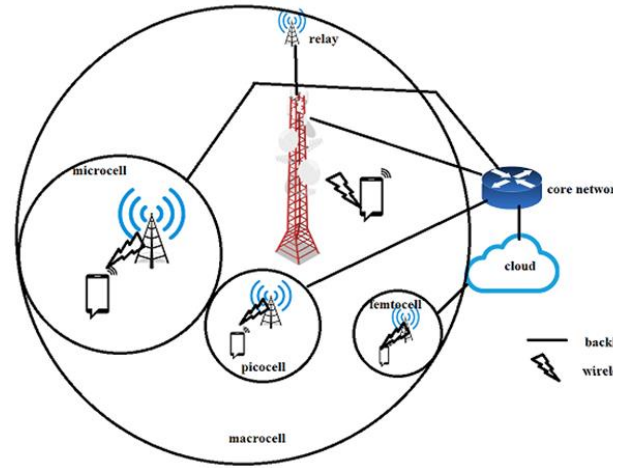


Figure - 2 Network Architecture of a 5G HetNets [9]

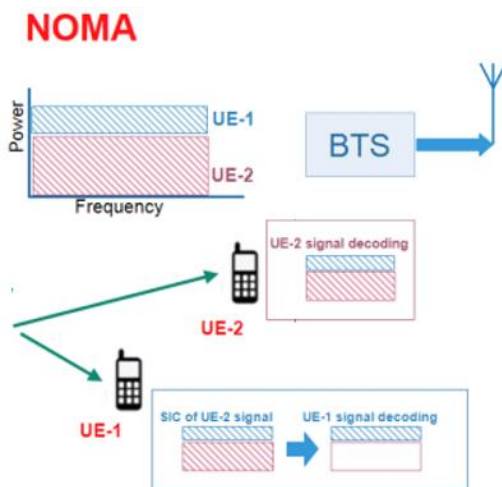


Figure - 3 Non-orthogonal multiple access technology (NOMA)

and providing spatial diversity. MIMO is a key tool for promoting all aspects of wireless communication. It plays an important role in 5G technology and influences how users interact with these technologies on a daily basis. These effects include the following:

- High network capacities;
- More coverage;
- Better user experience (UX).

Wireless sensor networks. Wireless networks are inextricably linked to the concept of the Internet of Things, which uses sensors, particularly for the industrial Internet of Things (IIoT). Sensors of various types in combination with wireless communication form the so-called wireless sensor networks (WSNs). Today, WSNs are the core of IIoT networks and are the main source of energy consumption. In the IoT, it is used to monitor objects, monitor the environment, identify threats, and more. WSN consists of sensors and base stations, the sensors in turn are distributed autonomously, monitoring the physical conditions of the environment. As this network will only grow, it is necessary to work in advance towards an ecological WSN, in order to improve the autonomy and efficient use of resources [14].

- Sensor units should be operated only when necessary;
- Apply a wireless charging, introduce mechanisms for collecting solar, kinetic, vibration energy;
- Use EE optimization methods (transmitter power control, modulation optimization, cooperative communication, directional antennas, cognitive radio(CR)).
- Apply rational routing schemes to reduce energy consumption;

Thus, by optimizing the processes of scanning, processing and connection in the WSN network, it is possible to gradually move to reduce the required energy. This optimized architecture can be divided into three layers, a sensor layer, a gateway layer, and a control layer.

Green data centers. Each high-performance network is based on data centers (DC). Improvements are also being made in this direction in order to reduce CO₂ emissions, optimize the use of green energy, and reduce electricity costs. To improve the EE in the environmental data center, the following methods can be used [4].

- Use renewable / green energy sources (wind, water, solar energy, heat pumps, etc.);
- Increasing the hardware operating in EE modes;
- Introduction of EE routing, in order to use the appropriate number of hardware;
- Build accurate DC power models;
- Establish a clear relationship between DC and wireless networks, in order to coordinate actions;

The technologies, systems, and algorithms discussed above lead to an understanding of smart grid and grid communications (SGGCs) designed to promote new insights that contribute to the design of computer and communication systems. Such systems control a large number of sensors, meters, etc., and accumulate a large amount of data for optimization and self-development. Several environmentally interconnected systems provide valuable services to people around the world, such as transportation, health care, utilities, and more, and can do so efficiently and energy-efficiently.

Conclusion. The realities of today are that protecting the environment is not a whim, but an extreme necessity. 5G wireless networks are evolving in conjunction with green energy technologies. There are a large number of tasks facing researchers. The issues facing the future telecommunications systems require interdisciplinary efforts from diverse networks, power systems, devices, customers, and corporations to address them.

5G networks stand out in previous generations, creating low-latency and ultra-reliable connectivity, expanding mobile broadband, and providing machine-type connectivity. Such advantages simultaneously expand the scope and set higher requirements for data rate, spectrum efficiency, bandwidth, coverage density, which in turn affects energy efficiency.

Thus, to ensure the integration of advanced technologies with maximum performance, systems, and models that allow the allocation of available resources efficiently and effectively, have become a new integral part of mobile multimedia communication systems.

REFERENCES:

1. Volynets V. Multimedia: concept, essence and scope // International Bulletin: Culturology. Philology. Musicology. 2016. Vip. 1. pp. 98–102.
2. Cvetković D. Interactive Multimedia - Multimedia Production and Digital Storytelling, ch 1, 2019, DOI: 10.5772/intechopen.85904.
3. Y.Li, et al.(2017), Green heterogeneous cloud radio access networks: Potential techniques, performance trade-offs and challenges,1–7. doi: 10.1109/MCOM.2017.1600807.
4. C. Zhu, et al (2015)., Green Internet of Things for Smart World, IEEE Access, vol.3. 2151 2162.
5. International Telecommunication Union (2017). Minimum requirements related to technical performance for IMT-2020 radio interface(s). Retrieved 07 May 2021 from <https://www.itu.int/pub/R-REP-M.2410-2017>.
6. E. Björnson. How Energy-Efficient Can a Wireless Communication System Become?. Björnson .E, G. Larsson E. pp.1–5, 2019. Retrieved 07 May 2021 from <https://arxiv.org/pdf/1812.01688.pdf>.
7. Prem Aruna & Rougier Jean-Louis & Rossi Dario & Chaudet Claude (2012). A Survey of Green Networking Research. IEEE Communications Surveys & Tutorials, 1-19.
8. C.Han, et al.(2011), Green radio: Radio techniques to enable energy efficient wireless networks, IEEE Communication Magazine, vol.49, no.6,.46–54.
9. Malik Nabeel & Ur Rehman Masood (2017). Green Communications: Techniques and Challenges. EAI Endorsed Transactions on Energy Web. , vol 4, 1-6. doi: 10.4108/eai.4-10-2017.153162.
10. Lee Woongsup & Jung Bang Chul. (2016). Improving Energy Efficiency of Cooperative Femtocell Networks via Base Station Switching Off. Mobile Information Systems. pp 1-6, 2016. doi: 10.1155/2016/3073184.
11. R.C. Kizilirmak. Non-Orthogonal Multiple Access (NOMA) for 5G Networks. doi 10.5772/66048. Retrieved 07 May 2021 from <https://www.intechopen.com/books/towards-5g-wireless-networks-a-physical-layer-perspective/non-orthogonal-multiple-access-noma-for-5g-networks>.
12. Z. Ding & F. Adachi & H. V. Poor (2016). The Application of MIMO to Non-Orthogonal Multiple Access. IEEE Transactions on Wireless Communications. vol.15, no.1, 537–552
13. Haralabos Papadopoulos, Chenwei Wang, Ozgun Bursalioglu, Xiaolin Hou. 2016. Massive MIMO Technologies and Challenges towards 5G. DOI:10.1587/transcom.2015EBI0002
14. Albreem Mahmoud & El-Saleh Ayman, Isa Muzamir & Salah Wael & Jusoh Muzammil. (2017). Green internet of things (IoT): An overview. 10.1109/ICSIMA.2017.8312021.

Д.т.н., проф. Степанов М. М., Лавріненко В. С.

ОГЛЯД КОМПОНЕНТІВ ДЛЯ ЕНЕРГОЕФЕКТИВНИХ МУЛЬТИМЕДІЙНИХ МЕРЕЖ НА ОСНОВІ ТЕХНОЛОГІЙ РАДІОДОСТУПУ 5G

Сучасне суспільство перебуває в активному переході до інформаційного типу, а технології мультимедіа вже невід'ємна частина цього процесу. Завдяки поширенню бездротових мереж доступу, користувачі стають більш мобільними, і розвиток п'ятого покоління мобільних мереж, відомих як 5G, виявляється важливим кроком у розвитку інформаційно-комунікаційних технологій. Мережі 5G надають низьку затримку та надійний зв'язок, розширюють можливості мобільного інтернету та машинного зв'язку. Однак разом з можливостями мультимедійного зв'язку приходить відповідальність за вплив супутніх технологій на навколишнє середовище, а також нові виклики і потреба раціонально використовувати наявні ресурси. У статті визначається поняття "мультимедіа" та розглядаються різні аспекти цього поняття, включаючи цифрове зберігання та обробку інформації, складові (текст, фото, аудіо та відео), можливість інтерактивної взаємодії та гіпертекстовий характер. Зазначається, що передача мультимедійних даних та використання інформаційних технологій тісно пов'язані з бездротовими мережами доступу.

Автори обговорюють виклики та рішення в галузі енергоефективності мереж. Вони наводять статистику, згідно з якою інформаційно-комунікаційна галузь відповідає за значну частку споживаної енергії та викидів CO₂, і звертають увагу на те, що мережі радіодоступу є основним джерелом споживання енергії та забруднення навколишнього середовища в цій галузі. Далі у статті розглядаються різні компоненти та технології, які можуть сприяти створенню енергоефективних мультимедійних мереж на базі технологій радіодоступу 5G. Зокрема, розглядаються гетерогенні мережі, технології неортогонального множинного доступу та

технології MIMO. Автори обговорюють важливість використання гетерогенних мереж для зменшення відстані між передавачем та приймачем, а також можливість використання режиму сну для малих базових станцій. Технології неортогонального множинного доступу (NOMA) та множинного введення-множинного виведення (MIMO) також розглядаються як ключові компоненти для досягнення спектральної ефективності та підвищення енергоефективності. Додатково, стаття звертає увагу на бездротові сенсорні мережі (WSN) та пропонує шляхи для їхньої оптимізації в напрямку енергоефективності. Також обговорюються можливості використання зелених дата-центрів для зменшення викидів CO₂ в інформаційно-комунікаційних технологіях. У висновку, стаття підкреслює важливість енергоефективності та зменшення викидів CO₂ в сучасних мультимедійних мережах, особливо в контексті мереж 5G, та закликає до міждисциплінарних зусиль для розв'язання цих важливих завдань у галузі інформаційно-комунікаційних технологій.

Ключові слова: мультимедіа, енергоефективність, WSN, 5G, HetNet.

МЕТОДИЧНИЙ ПІДХІД ДО ОЦІНЮВАННЯ РІВНЯ БОЄЗДАТНОСТІ ВІЙСЬКОВОЇ ЧАСТИНИ

Необхідність впровадження нових підходів щодо підвищення рівня боєздатності військових частин Збройних Сил України зумовлено збройною агресією російської федерації. Зазначене вимагає обґрунтованого підходу до питань удосконалення діяльності командувачів (командирів, начальників) та їх заступників з метою підвищення боєздатності підпорядкованих військових частин (підрозділів), що не можливо без використання відповідного науково-методичного апарату.

На основі науково-методичних підходів з оцінювання окремих складових (показників) боєздатності військових організаційних структур та досвіду проведення перевірок бойової готовності військових частин, у статті викладено методичний підхід до оцінювання рівня боєздатності військової частини. До показників, які здійснюють безпосередній вплив на рівень боєздатності військової частини віднесено: “ПЕРСОНАЛ”, який характеризує її рівень укомплектованості особовим складом та їх морально-психологічний стан; “ПІДГОТОВЛЕНІСТЬ”, який характеризує рівень індивідуальної підготовки (навченість військовослужбовців) та рівень колективної підготовки (злагодженість у складі структурних підрозділів); “ОЗБРОЄННЯ”, який характеризує рівень забезпеченості військової частини справними штатними зразками озброєння і військової техніки; “ЗАПАСИ”, який характеризує рівень забезпеченості військової частини придатними до використання матеріально-технічними засобами.

Даний методичний підхід дозволяє провести кількісну оцінку рівня боєздатності військової частини до виконання завдань за призначенням, а також виявити проблемні питання за її показниками. Результати проведеного дослідження можуть бути практично використані під час оцінювання боєздатності військових частин, при розробці керівних документів, що регламентують зазначене питання, а також у ході подальших досліджень з даного напрямку у наукових установах.

Ключові слова: боєздатність; військова частина; показники оцінювання; персонал; підготовленість; озброєння; запаси.

Вступ та постановка проблеми. Досвід застосування військових частин Збройних Сил (ЗС) України у ході проведення антитерористичної операції, операції Об’єднаних сил та відсічі збройної агресії російської федерації свідчить, що успішне виконання ними завдань за призначенням залежить від рівня їх боєздатності [1 - 4]. Широкомасштабна збройна агресія російської федерації із застосуванням засобів вогневого ураження створює передумови для нанесення силам оборони України втрат, тобто знижує їх боєздатність.

У зв’язку з цим триває робота в органах військового управління, військових частинах ЗС України щодо пошуку та впровадження нових підходів у діяльність командувачів (командирів, начальників) та їх заступників для підвищення рівня боєздатності військових частин.

Обмежені можливості існуючих методичних підходів з оцінювання окремих складових (показників) боєздатності військових організаційних структур для повноцінного застосування під час комплексного оцінювання рівня боєздатності військових частин спонукає до удосконалення науково-методичного апарату та обґрунтування запропонованих змін. Таким чином існує потреба у науковому обґрунтуванні методичного підходу до

оцінювання рівня боєздатності військової частини. Зазначене свідчить про актуальність теми, яка розглядається.

Аналіз останніх досліджень. Аналіз попередніх досліджень та публікацій з даного напрямку [5 - 12] свідчить про те, що вони базуються на оцінюванні деяких складових боєздатності військових організаційних структур, переважно розкривають лише один із показників, але не враховують решту. Так, у роботі [5] було запропоновано методичний підход до оцінювання ефективності системи комплектування персоналом. У статті [6] були визначені показники оцінювання мобілізаційної готовності територіального центру комплектування та соціальної підтримки, але порядок їх оцінювання не розкрито. Ряд попередніх робіт автора [7 - 12] присвячено оцінюванню підготовленості військових організаційних структур, або її складових. Тому, стосовно оцінювання рівня боєздатності військової частини зазначені методики потребують удосконалення та можуть бути застосовані лише частково. У той же час, наявний науково-методичний апарат є базовою основою для подальшого його удосконалення.

Виклад основного матеріалу. Боєздатність військової частини є складовою її бойової готовності та являється кількісно-якісною характеристикою готовності військової частини до виконання завдань за призначенням. Для розрахунку оцінки рівня боєздатності військової частини оберемо показник $M_F(t)$, за величиною якого визначається її готовність до виконання завдань за призначенням. Боєздатність військової частини залежить від її укомплектованості особовим складом, його підготовленості та морально-психологічного стану, забезпеченості технічно справними штатними зразками озброєння і військової техніки та запасами справних (придатних до використання) матеріально-технічних засобів.

Враховуючи зазначене, до показників, які здійснюють безпосередній вплив на рівень боєздатності військової частини пропонується віднести: “ПЕРСОНАЛ”, який характеризує її рівень укомплектованості особовим складом та їх морально-психологічний стан; “ПІДГОТОВЛЕНІСТЬ”, який характеризує рівень індивідуальної підготовки (навченість особового складу) та рівень колективної підготовки (злагодженість у складі структурних підрозділів); “ОЗБРОЄННЯ”, який характеризує рівень забезпеченості військової частини справними штатними зразками озброєння і військової техніки; “ЗАПАСИ”, який характеризує рівень забезпеченості військової частини придатними до використання матеріально-технічними засобами. Зважаючи на те, що зазначені показники не залежні один від одного, то для оцінювання рівня боєздатності військової частини $M_F(t)$ пропонується використовувати адитивну агрегацію [13 - 16]:

$$M_F(t) = C_{\Pi}(t) \cdot q_{\Pi} + C_H(t) \cdot q_H + C_O(t) \cdot q_O + C_3(t) \cdot q_3, \quad (1)$$

де $C_{\Pi}(t)$ – показник ПЕРСОНАЛ, який характеризує укомплектованість військової частини особовим складом та їх морально-психологічний стан на дискретний момент часу;

$C_H(t)$ – показник ПІДГОТОВЛЕНІСТЬ, який характеризує навченість особового складу та їх злагодженість у складі структурних підрозділів на дискретний момент часу;

$C_O(t)$ – показник ОЗБРОЄННЯ, який характеризує забезпеченість військової частини справними штатними зразками озброєння і військової техніки на дискретний момент часу;

$C_3(t)$ – показник ЗАПАСИ, який характеризує забезпеченість військової частини придатними до використання матеріально-технічними засобами на дискретний момент часу;

q_{Π}, q_H, q_O, q_3 – вагові коефіцієнти важливості показників $C_{\Pi}(t), C_H(t), C_O(t), C_3(t)$.

Розрахунок значення показника ПЕРСОНАЛ пропонується визначати за залежністю, яка враховує рівень укомплектованості військової частини особовим складом та їх морально-психологічний стан:

$$C_{\Pi}(t) = Y(t) \cdot q_y + X(t) \cdot q_x, \quad (2)$$

де $Y(t)$ – показник, який характеризує рівень укомплектованості військової частини особовим складом на дискретний момент часу;

$X(t)$ – показник, який характеризує морально-психологічний стан особового складу військової частини на дискретний момент часу;

q_y, q_x – вагові коефіцієнти важливості показників $Y(t), X(t)$.

Розрахунок рівня укомплектованості військової частини особовим складом $Y(t)$ пропонується визначати за залежністю, яка враховує співвідношення списочної чисельності особового складу до чисельності особового складу передбаченого штатом з урахуванням важливості посад:

$$Y(t) = \frac{\sum_{j=1}^{J_C} D_j \cdot q_j}{\sum_{j=1}^{J_{III}} D_j \cdot q_j}, \quad (3)$$

де J_C – кількість j -их посад особового складу військової частини за списком;

J_{III} – кількість j -их посад особового складу військової частини по штату;

q_j – ваговий коефіцієнт важливості j -ої посади у військовій частині;

D_j – індекс наявності j -го військовослужбовця у військовій частині.

$$D_j = \begin{cases} 1, & \text{при наявності} \\ 0, & \text{відсутній} \end{cases}, \quad (4)$$

Вагові коефіцієнти важливості j -ої посади особового складу у військовій частині q_j розраховуються шляхом нормування порівняльних рангів посад у відповідності з виразом, який запропоновано у роботі [7]:

$$q_j = \frac{R_{jn}}{\sum_{j=1}^J R_{jn}}, \quad (5)$$

де R_{jn} – порівняльний ранг j -ої посади особового складу у військовій частині;

$\sum_{j=1}^J R_{jn}$ – сума всіх рангів посад особового складу військової частини;

J – загальна кількість посад у військовій частині.

Порівняльний ранг j -ої посади особового складу у військовій частині визначається за залежністю:

$$R_{jn} = 1 - \frac{J_j - 1}{J}, \quad (6)$$

де J_j – порядковий номер j -ої посадової особи військової частини.

Оцінку морально-психологічного стану особового складу військової частини пропонується визначати за показниками, які характеризують їх нервово-психічну стійкість, військово-мотиваційну спрямованість особистості та професійну придатність до успішного

виконання функціональних обов'язків. Його розрахунок пропонується визначати за залежністю:

$$X(t) = L_{nnc}(t) \cdot q_{nnc} + L_{vnc}(t) \cdot q_{vnc} + L_{nn}(t) \cdot q_{nn}, \quad (7)$$

де $L_{nnc}(t)$ – показник, який характеризує рівень нервово-психічної стійкості особового складу військової частини;

$L_{vnc}(t)$ – показник, який характеризує рівень військово-мотиваційної спрямованості особового складу військової частини;

$L_{nn}(t)$ – показник, який характеризує рівень професійної придатності особового складу військової частини до успішного виконання функціональних обов'язків;

q_{nnc} , q_{vnc} , q_{nn} – вагові коефіцієнти важливості показників $L_{nnc}(t)$, $L_{vnc}(t)$, $L_{nn}(t)$.

Оцінку рівня нервово-психічної стійкості особового складу військової частини $L_{nnc}(t)$ пропонується визначати за допомогою стандартизованих тестових методик: “Характерологічні акцентуації особистості – нервово-психічна нестабільність” та “Психодіагностичний тест”. За визначеними методиками у особового складу військової частини визначається категорія нервово-психічної стійкості: ВИСОКА – 1-2 бали; ДОБРА – 3-5 балів; ЗАДОВІЛЬНА – 6-7 балів; НЕЗАДОВІЛЬНА – 8-10 балів.

Для переведення бального оцінювання рівня нервово-психічної стійкості особового складу військової частини до безрозмірної величини нами була розроблена шкала оцінювання, яка наведена в табл. 1.

Таблиця 1

Оцінка, бали	Значення показника
1	1,0
2	0,9
3	0,85
4	0,75
5	0,65
6	0,6
7	0,5
8	0,4
9	0,25
10	0,1

Оцінку рівня військово-мотиваційної спрямованості особового складу військової частини $L_{vnc}(t)$ пропонується визначати за допомогою методики “Спрямованість особистості (Смекала-Кучера)”. У залежності від отриманого результату за даною методикою визначається домінуюча спрямованість особистості. Виділяють три основні види спрямованості особистості: на себе (особиста спрямованість), на взаємодію (колективістська спрямованість), на завдання (ділова спрямованість). Для отримання значення показника у кількісних величинах пропонується кожному виду спрямованості особистості визначити такі значення:

ділова спрямованість – 0,95;

колективістська спрямованість – 0,75;

особиста спрямованість – 0,6.

Оцінка професійної придатності особового складу військової частини до успішного виконання функціональних обов'язків $L_{nn}(t)$ пропонується визначати за допомогою стандартизованої тестової методики “Матриці прогресивні Равена”, яка враховує пізнавальні процеси, що мають найбільше значення для успішної професійної діяльності особового

складу, а саме: пам'яті, уваги, мислення. Зазначений показник оцінюється в балах, тому його значення приводимо до безрозмірної величини за допомогою виразу:

$$L_{nn}(t) = \frac{Q_{nn}(t)}{70}, \quad (8)$$

де $Q_{nn}(t)$ – кількість балів отримана особовим складом військової частини за результатами виконання тесту;

70 – максимальна кількість балів, яку можливо отримати за результатами виконання тесту.

Розрахунок значення показника ПІДГОТОВЛЕНІСТЬ $C_H(t)$ пропонується визначати за залежністю, яка враховує як рівень індивідуальної підготовки військовослужбовців так і колективної підготовки структурних підрозділів військової частини. Так як зазначені показники сильно корельовані, то, для визначення значення показника ПІДГОТОВЛЕНІСТЬ $C_H(t)$ пропонується використовувати нормовану мультиплікативну агрегацію [17]:

$$C_H(t) = P_{in}(t)^{q_{in}} \cdot P_{kn}(t)^{q_{kn}}, \quad (9)$$

де $P_{in}(t)$ – показник, який характеризує сукупний рівень індивідуальної підготовки (навченості) військовослужбовців військової частини на дискретний момент часу;

$P_{kn}(t)$ – показник, який характеризує сукупний рівень колективної підготовки (злагодженість) структурних підрозділів військової частини на дискретний момент часу;

q_{in}, q_{kn} – вагові коефіцієнти важливості показників $P_{in}(t), P_{kn}(t)$.

Оцінку сукупного рівня індивідуальної підготовки військовослужбовців військової частини $P_{in}(t)$ пропонується визначати за залежністю, яка враховує рівень індивідуальної підготовки кожного військовослужбовця військової частини з урахуванням його важливості:

$$P_{in}(t) = \sum_{j=1}^J P_{inj}(t) \cdot q_j, \quad (10)$$

де $P_{inj}(t)$ – рівень індивідуальної підготовки j -го військовослужбовця військової частини на дискретний момент часу.

Оцінювання рівня індивідуальної підготовки j -го військовослужбовця військової частини пропонується здійснювати за залежністю, яка враховує їх результати навчання з предметів індивідуальної підготовки з урахуванням важливості предметів:

$$P_{inj}(t) = \sum_{o=1}^O N_{jo}(t) \cdot q_o, \quad (11)$$

де $N_{jo}(t)$ – рівень індивідуальної підготовки j -го військовослужбовця військової частини з o -го предмета індивідуальної підготовки на дискретний момент часу;

q_o – ваговий коефіцієнт важливості o -го предмета індивідуальної підготовки;

O – кількість предметів індивідуальної підготовки з яких проводиться оцінювання.

Рівень індивідуальної підготовки j -го військовослужбовця військової частини з o -го предмета індивідуальної підготовки $N_{jo}(t)$ розраховується за залежністю:

$$N_{jo}(t) = \frac{A_{jo}(t)}{A_{\max}}, \quad (12)$$

де $A_{jo}(t)$ – кількість балів отримана військовослужбовцем військової частини з o -го предмета індивідуальної підготовки;

$A_{\max}$ – максимальна кількість балів, яку можливо отримати з предмету індивідуальної підготовки.

Оцінку сукупного рівня колективної підготовки структурних підрозділів військової частини $P_{\kappa n}(t)$ пропонується визначати за залежністю, яка враховує рівень злагодженості кожного структурного підрозділу військової частини з урахуванням його важливості. Так, як рівень злагодженості кожного окремого структурного підрозділу не залежить від рівня злагодженості іншого, а отже і їх показники не залежні один від одного, то для оцінювання сукупного рівня колективної підготовки $P_{\kappa n}(t)$ пропонується використовувати адитивну агрегацію:

$$P_{\kappa n}(t) = \sum_{k=1}^K T_{3k}(t) \cdot q_k, \quad (13)$$

де $T_{3k}(t)$ – показник, який характеризує рівень злагодженості k -го структурного підрозділу військової частини на дискретний момент часу;

q_k – ваговий коефіцієнт важливості k -го структурного підрозділу військової частини.

Рівень злагодженості k -го структурного підрозділу військової частини $T_{3k}(t)$ визначається за результатами відпрацювання ним стандартів колективної підготовки:

$$T_{3k}(t) = \frac{\sum_{v=1}^V K_{Cmk}(t) \cdot q_v}{V}, \quad (14)$$

де $K_{Cmk}(t)$ – показник, який характеризує оцінку за виконання стандарту колективної підготовки k -го структурного підрозділу військової частини на дискретний момент часу;

V – кількість стандартів колективної підготовки, які необхідно виконати k -му структурному підрозділу військової частини;

q_v – ваговий коефіцієнт важливості стандарту колективної підготовки.

Оцінювання стандартів колективної підготовки $K_{Cmk}(t)$ пропонується здійснювати за оцінками розділів стандарту, які характеризують спроможність структурного підрозділу виконувати певні завдання, за залежністю:

$$K_{Cmk}(t) = \frac{\sum_{s=1}^S R_{Cmks}(t) \cdot q_s}{S}; \quad R_{Cmks} = \overline{2,5}, \quad (15)$$

де $R_{Cmks}(t)$ – показник, який характеризує оцінку за результатами виконання k -им структурним підрозділом військової частини S -го розділу стандарту колективної підготовки на дискретний момент часу;

S – кількість розділів стандарту колективної підготовки;

q_s – ваговий коефіцієнт важливості розділу стандарту колективної підготовки.

Стандарт колективної підготовки оцінюється:

$$K_{Cmk}(t) = \begin{cases} \text{відмінно, якщо } \frac{\sum_{s=1}^S R_{Cmks}(t)}{S} \geq 4,5; & R_{Cmks} \geq 4; \\ \text{добре, якщо } \frac{\sum_{s=1}^S R_{Cmks}(t)}{S} \geq 3,5; & R_{Cmks} \geq 3; \\ \text{задовільно, якщо } \frac{\sum_{s=1}^S R_{Cmks}(t)}{S} < 3,5; & R_{Cmks} \geq 3; \\ \text{незадовільно, якщо } R_{Cmks}(t) = 2. \end{cases} \quad (16)$$

У свою чергу, розділи стандарту колективної підготовки складаються із елементів, які необхідно виконати k -му структурному підрозділу військової частини. Розрахунок оцінки за результатами виконання S -го розділу стандарту колективної підготовки пропонується здійснювати наступним чином:

$$R_{Cmks}(t) = \left(\frac{x + y}{x^* + y^*} \right) \cdot z_x; \quad z_x = \begin{cases} 1, & x = x^*; \\ 0, & x < x^*, \end{cases} \quad (17)$$

де x – кількість виконаних критично важливих елементів;

x^* – загальна кількість критично важливих елементів;

y – кількість виконаних інших елементів;

y^* – загальна кількість інших елементів;

z_x – індекс валідності кінцевого результату за критично важливими елементами (умова обов'язкового повного виконання).

Розділ стандарту колективної підготовки оцінюється:

$$R_{Cmks}(t) = \begin{cases} \text{відмінно, якщо } R_{Cmks}(t) \geq 0,8; \\ \text{добре, якщо } 0,7 \geq R_{Cmks}(t) < 0,8; \\ \text{задовільно, якщо } 0,6 \geq R_{Cmks}(t) < 0,7; \\ \text{незадовільно, якщо } R_{Cmks}(t) < 0,6. \end{cases} \quad (18)$$

Розрахунок значення показника “ОЗБРОЄННЯ” $C_O(t)$ пропонується визначати за залежністю, яка враховує кількість придатних до використання z -их груп (видів) зразків озброєння і військової техніки військової частини від їх загальної кількості визначеної табелем до штату з урахуванням їх важливості:

$$C_O(t) = \frac{\sum_{z=1}^{Z_n} O_z \cdot q_z}{\sum_{z=1}^{Z_{ui}} O_z \cdot q_z}, \quad (19)$$

де Z_n – кількість придатних до використання груп (видів) зразків озброєння і військової техніки військової частини;

Z_{ui} – кількість груп (видів) зразків озброєння і військової техніки визначених у таблиці до штату військової частини;

q_z – ваговий коефіцієнт важливості z -ої групи (виду) зразків озброєння і військової техніки;

Q_z – індекс наявності z -ої групи (виду) зразків озброєння і військової техніки.

$$Q_z = \begin{cases} 1, & \text{при наявності} \\ 0, & \text{відсутній} \end{cases}, \quad (20)$$

Розрахунок значення показника “ЗАПАСИ” $C_3(t)$ пропонується визначати за залежністю, яка враховує наявні матеріально-технічні засоби за класами постачання до їх штатно-табельної потреби (норми забезпечення), регламентованої нормативними документами, з урахуванням важливості u -го класу постачання матеріально-технічного засобу:

$$C_3 = \frac{\sum_{n=1}^{N_n} Q_u \cdot q_u}{\sum_{n=1}^{N_n} Q_u \cdot q_u}, \quad (21)$$

де N_n – кількість наявних у військовій частині до використання матеріально-технічних засобів за класами постачання;

N_n – кількість матеріально-технічних засобів за класами постачання регламентованих нормативними документами;

q_u – ваговий коефіцієнт важливості u -го класу постачання матеріально-технічних засобів;

Q_u – індекс наявності u -го класу постачання матеріально-технічних засобів.

$$Q_u = \begin{cases} 1, & \text{при наявності} \\ 0, & \text{відсутнє} \end{cases}, \quad (22)$$

Розрахунок вагових коефіцієнтів важливості показників усіх рівнів здійснюється методом експертного оцінювання.

Висновки та перспективи подальшого розвитку. Таким чином, у статті наведено розроблений методичний підхід до оцінювання рівня боєздатності військової частини, у якому використовуються показники: “ПЕРСОНАЛ”, який характеризує рівень укомплектованості особовим складом та їх морально-психологічний стан; “ПІДГОТОВЛЕНІСТЬ”, який характеризує рівень індивідуальної та колективної підготовки; “ОЗБРОЄННЯ”, який характеризує рівень забезпеченості військової частини справними штатними зразками озброєння і військової техніки; “ЗАПАСИ”, який характеризує рівень забезпеченості військової частини придатними до використання матеріально-технічними засобами.

Даний методичний підхід дозволяє провести кількісну оцінку рівня боєздатності військової частини до виконання завдань за призначенням. Результати проведеного дослідження можуть бути практично використані під час оцінювання боєздатності військових частин, при розробці керівних документів, що регламентують зазначене питання, а також у ході подальших досліджень з даного напрямку у наукових установах.

Перспективами подальших наукових досліджень у даному напрямі може бути обґрунтування рекомендацій з підвищення рівня боєздатності військової частини.

ЛІТЕРАТУРА:

1. Heorhadze O. Metod's for assessing the level of the organization of joint training of defence forces // Сучасні інформаційні технології у сфері безпеки та оборони. 2022. No 2 (44). С. 43–47. <https://doi.org/10.33099/2311-7249/2022-44-2-43-47>.
2. Георгадзе О.А., Пампуха І.В., Шевчук В.В., Пехота С.Г., Чайковська О.Є. Методичний підхід до оцінювання ефективності індивідуальної підготовки офіцерського складу науково-педагогічних працівників у вищих військових навчальних закладах // Збірник наукових праць військового інституту Київського Національного університету імені Тараса Шевченка. 2022. No 76. С. 130–138. <https://doi.org/10.17721/2519-481X/2022/76-11>.
3. Георгадзе О.А., Петров В.А. Часткова методика оцінювання рівня методичної діяльності кафедри військової підготовки // Сучасні інформаційні технології у сфері безпеки та оборони. 2022. No 1 (43). С. 99–104. <https://doi.org/10.33099/2311-7249/2022-43-1-99-104>.
4. Георгадзе О.А., Салаш О.А. Обґрунтування сукупності показників до комплексної методики оцінювання ефективності оперативної підготовки // Збірник наукових праць Національної академії Державної прикордонної служби України. Серія: військові та технічні науки. 2022. No 3 (88). С. 5–17. <https://doi.org/10.32453/3.v88i3>
5. Думенко М.П. Методичний підхід до оцінювання ефективності системи комплектування персоналом Збройних Сил України в умовах гібридної війни (особливого періоду) // Сучасні інформаційні технології у сфері безпеки та оборони. 2019. No 2 (35). С. 133–138. <https://doi.org/10.33099/2311-7249/2019-34-1-133-138>.
6. Маліцький Д.А. Комплексна методика оцінки ефективності мобілізації людських ресурсів на території відповідальності // Journal of Scientific Papers “Social development and security”. 2021. Vol. 11. No 4. С. 103–111. <https://doi.org/10.33445/sds.2021.11.4.8>.
7. Георгадзе О.А., Харабара В.І. Часткова методика оцінювання рівня підготовленості танкової бригади у ході відновлення боєздатності // Journal of Scientific Papers “Social development and security”. 2019. Vol. 9. No 4. С. 131–142. <https://doi.org/10.33445/sds.2019.9.4.10>.
8. Piekhota S., Heorhadze O., Kharabara V. Partial methodology for assessing the level of learning of tactical aviation brigade personnel // Political Science and Security Studies Journal. 2021. Vol. 2. No 1. P. 68–73. <https://doi.org/10.5281/zenodo.4818549>.
9. Георгадзе О.А., Макаліш О.В. Методичний підхід до оцінювання рівня навченості органів військового управління тактичного рівня // Збірник наукових праць Центру військово-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського. 2016. No 3 (58). С. 104–108. <https://doi.org/10.33099/2304-2745/2016-3-58/104-108>.
10. Vynokurov D., Heorhadze O. Partial methodology for assessing the younger specialists competence level in the training center // Journal of Scientific Papers “VUZF REVIEW”. 2020. Vol. 5. No 1. P. 50–53. <https://doi.org/10.38188/2534-9228.20.1.07>.
11. Салаш О.А., Георгадзе О.А. Часткова методика оцінювання стану індивідуальної підготовки військовослужбовців в органах військового управління // Journal of Scientific Papers “Social development and security”. 2022. Vol. 12. No 5. С. 10–20. <https://doi.org/10.33445/sds.2022.12.5.2>.
12. Георгадзе О.А., Салаш О.А. Часткова методика оцінювання стану колективної підготовки органів військового управління // Збірник наукових праць військового інституту Київського Національного університету імені Тараса Шевченка. 2022. No 77. С. 161–171. <https://doi.org/10.17721/2519-481X/2022/77-14>.
13. Vynokurov D., Heorhadze O. Comprehensive methodology for evaluating the effectiveness of training the variable composition of the training center // Political Science and Security Studies Journal. 2021. Vol. 2. № 2. P. 77 – 85. <https://doi.org/10.5281/zenodo.5071081>.
14. Heorhadze O., Kamalov Y. Methods for assessing the readiness level of an educational institution for military training of citizens according to the program of reserve officers // Political Science and Security Studies Journal. 2020. Vol. 1. № 2. P. 90–97. <https://doi.org/10.5281/zenodo.4521176>.
15. Георгадзе О.А., Репіло Ю.Є., Куртсеїтов Т.Л., Микусь С.А., Хома В.В. Методичний підхід щодо оцінювання рівня організації підготовки у Збройних Силах України // Journal of Scientific Papers “Social development and security”. 2022. Vol. 12. No 5. С. 1–9. <https://doi.org/10.33445/sds.2022.12.5.1>.
16. Георгадзе О.А., Петров В.А. Часткова методика оцінювання рівня організації вогневої підготовки на кафедрі військової підготовки // Збірник наукових праць Центру військово-

стратегічних досліджень Національного університету оборони України імені Івана Черняхівського. 2023. No 1 (77). С. 112–119. <https://doi.org/10.33099/2304-2745/2023-1-77/112-119>.

17. Heorhadze O., Barhylevych A. Separate brigade of territorial defence level of training organization assessment methodology // *Political Science and Security Studies Journal*. 2020. Vol. 1. № 1. P. 71–75. <https://doi.org/10.5281/zenodo.4399732>.

REFERENCES:

1. Heorhadze O. Metod's for assessing the level of the organization of joint training of defence forces // *Suchasni informatsiyni tehnologiyi u sferi bezpeki ta oboroni*. 2022. No 2 (44). Pp. 43–47. <https://doi.org/10.33099/2311-7249/2022-44-2-43-47>.

2. Georgadze O.A., Pampukha I.V., Shevchuk V.V., Piekhota S.G., Chaikovskaya O.E. Metodychnyi pidkhid do otsiniuvannia efektyvnosti indyvidualnoi pidhotovky ofiterskoho skladu naukovopedagogichnykh pratsivnykiv u vyshchyykh viiskovykh navchalnykh zakladakh // *Zbirnyk naukovykh prac' Vijs'kovogo instytutu Kyi'vs'kogo Nacional'nogo universytetu imeni Tarasa Shevchenka*. 2022. Kyiv. № 76. Pp. 130–138. <https://doi.org/10.17721/2519-481X/2022/76-11>.

3. Georgadze O.A., Petrov V.A. Chastkova metodyka otcinjuvannja rivnja metodychnoi' dijall'nosti kafedry vijs'kovoi' pidgotovky // *Suchasni informatsiyni tehnologiyi u sferi bezpeki ta oboroni*. 2022. Kyiv. № 1 (43). Pp. 99–104. <https://doi.org/10.33099/2311-7249/2022-43-1-99-104>.

4. Georgadze O.A., Salash O.A. Obgruntuvannja sukupnosti pokaznykiv do kompleksnoi' metodyky otcinjuvannja efektyvnosti operatyvnoi pidhotovky // *Zbirnyk naukovykh prac' Nacional'noi' akademii' Derzhavnoi' prykordonnoi' sluzhby Ukrayini*. Serija: viyskovi ta technichni nauky. 2022. No 3 (88). С. 5–17. <https://doi.org/10.32453/3.v88i3>

5. Dumenko M.P. Metodychnyi pidkhid do otsiniuvannia efektyvnosti systemy komplektuvannja personalom Zbroynykh Syl Ukrayini v umovakh gibrydnoj vijny (osoblyvogo periodu) // *Suchasni informatsiyni tehnologiyi u sferi bezpeki ta oboroni*. 2019. No 2 (35). Pp. 133–138. <https://doi.org/10.33099/2311-7249/2019-34-1-133-138>.

6. Malits'kyi D.A. Kompleksna metodyka otcinjuvannja efektyvnosti mobilizatsij lyuds'kykh resursiv na terytoriyi vidpovidal'nosti // *Journal of Scientific Papers "Social development and security"*. 2021. Vol. 11. No 4. Pp. 103–111. <https://doi.org/10.33445/sds.2021.11.4.8>

7. Georgadze O.A., Harabara V.I. Chastkova metodika otsinyuvannja rivnja pidgotovlenosti tankovoyi brigadi u hodi vidnovlennja boezdatnosti // *Journal of Scientific Papers "Social development and security"*. 2019. Vol. 9. No 4. Pp. 131 – 142. <https://doi.org/10.33445/sds.2019.9.4.10>.

8. Piekhota S., Heorhadze O., Kharabara V. Partial methodology for assessing the level of learning of tactical aviation brigade personnel // *Political Science and Security Studies Journal*. 2021. Vol. 2. No 1. Pp. 68–73. <https://doi.org/10.5281/zenodo.4818549>.

9. Georgadze O.A., Makalish O.V. Metodichnyi pidhid do otsinyuvannja rivnja navchenosti organiv viyskovogo upravlinnja taktichnogo rivnja // *Zbirnik naukovykh prats tsentru viyskovo-strategichnih doslidzhen Natsionalnogo universitetu oboroni Ukrayini imeni Ivana Chernyakovskogo*. 2016. № 3(58). – Pp. 104–108. <https://doi.org/10.33099/2304-2745/2016-3-58/104-108>.

10. Vynokurov D., Heorhadze O. Partial methodology for assessing the younger specialists competence level in the training center // *Journal of Scientific Papers "VUZF REVIEW"*. 2020. Vol. 5. No 1. Pp. 50–53. <https://doi.org/10.38188/2534-9228.20.1.07>.

11. Salash O.A., Georgadze O.A. Chastkova metodyka otsinyuvannja stanu indyvidual'noyi pidhotovky viys'kovosluzhbovtiv v orhanakh viys'kovoho upravlinnja // *Journal of Scientific Papers "Social development and security"*. 2022. Vol. 12. No 5. Pp.10–20. <https://doi.org/10.33445/sds.2022.12.5.2>.

12. Georgadze O.A., Salash O.A. Chastkova metodyka otsinyuvannja stanu kolektyvnoyi pidhotovky orhaniv viys'kovoho upravlinnja // *Zbirnyk naukovykh prac' Vijs'kovogo instytutu Kyi'vs'kogo Nacional'nogo universytetu imeni Tarasa Shevchenka*. 2022. No 77. Pp. 161–171. <https://doi.org/10.17721/2519-481X/2022/77-14>.

13. Vynokurov D., Heorhadze O. Comprehensive methodology for evaluating the effectiveness of training the variable composition of the training center // *Political Science and Security Studies Journal*. 2021. Vol. 2. № 2. Pp. 77 – 85. <https://doi.org/10.5281/zenodo.5071081>

14. Heorhadze O., Kamalov Y. Methods for assessing the readiness level of an educational institution for military training of citizens according to the program of reserve officers // *Political Science and Security Studies Journal*. 2020. Vol. 1. № 2. Pp. 90–97. <https://doi.org/10.5281/zenodo.4521176>.

15. Georgadze O.A., Repilo Y.E., Kurtseitov T.L., Mykus' S.A., Khoma V.V. Metodychnyi pidkhid shchodo otsinyuvannja rivnja orhanizatsiyi pidhotovky u Zbroynykh Sylakh Ukrayiny // *Journal of*

Scientific Papers "Social development and security". 2022. Vol. 12. No 5. Pp. 1–9. <https://doi.org/10.33445/sds.2022.12.5.1>.

16. Georgadze O.A., Petrov V.A. Chastkova metodyka otsynyuvannya rivnya orhanizatsiyi vohnevoyi pidhotovky na kafedri viys'kovoyi pidhotovky // Zbirnik naukovih prats tsentru viyskovo-strategichnih doslidzhen Natsionalnogo universitetu oboroni Ukrayini imeni Ivana Chernyakhovskogo. 2023. No 1 (77). Pp. 112–119. <https://doi.org/10.33099/2304-2745/2023-1-77/112-119>.

17. Heorhadze O., Barhylevych A. Separate brigade of territorial defence level of training organization assessment methodology // Political Science and Security Studies Journal. 2020. Vol. 1. № 1. Pp. 71–75. <https://doi.org/10.5281/zenodo.4399732>.

**PhD Heorhadze O.A., PhD Piekhota S.H., Klyuchak O.M., Chaikovska O.E., Kondratiuk S.M.,
Chornomaz O.O.**

METHODOLOGICAL APPROACH TO ASSESSING THE LEVEL OF COMBAT CAPABILITY OF A MILITARY UNIT

The need to introduce new approaches to increase the level of combat capability of military units of the Armed Forces of Ukraine is due to the armed aggression of the Russian Federation. This requires a reasonable approach to issues of improving the activities of commanders (commanders, chiefs) and their deputies in order to increase the combat capability of subordinate military units (subunits), which is not possible without the use of appropriate scientific and methodological apparatus.

On the basis of scientific and methodical approaches to the evaluation of individual components (indicators) of the combat capability of military organizational structures and the experience of conducting inspections of the combat readiness of military units, the article outlines a methodical approach to assessing the level of combat capability of a military unit. Indicators that have a direct impact on the level of combat capability of a military unit include: "PERSONNEL", which characterizes its level of staffing and their moral and psychological state; "PREPAREDNESS", which characterizes the level of individual training (training of servicemen) and the level of collective training (coherence in the composition of structural units); "WEAPONS", which characterizes the level of provision of the military unit with serviceable regular samples of weapons and military equipment; "SUPPLY", which characterizes the level of provision of the military unit with usable material and technical means.

This methodical approach makes it possible to carry out a quantitative assessment of the level of combat capability of a military unit to perform assigned tasks, as well as to identify problematic issues based on its indicators. The results of the conducted research can be practically used during the evaluation of the combat capability of military units, during the development of guiding documents regulating the specified issue, as well as in the course of further research in this direction in scientific institutions.

Keywords: *combat capability; military units; assessment indicators; personnel; preparedness; weapons; supply.*

МОДЕЛЬ ОЦІНКИ МАТЕМАТИЧНОГО СПОДІВАННЯ ШВИДКОСТІ ВИТРАТИ ПАЛЬНОГО ПІДРОЗДІЛОМ ЗБРОЙНИХ СИЛ УКРАЇНИ

Вивчення досвіду ведення антитерористичної операції та операції Об'єднаних сил у війні з Російською Федерацією дозволяє зробити висновок про те, що на сьогоднішній день застосування сучасних засобів вогневого ураження у поєднанні з новими підходами ведення розвідки істотно вплинуло на підвищення інтенсивності та швидкості переміщення військ в ході бойових дій. В таких умовах можуть з'являтися випадкові (непередбачені) витрати пального з одночасним раптовим зниженням його запасів нижче визначених (допустимих) норм. Непередбачене падіння запасів пального у військовій техніці може бути пов'язане з багатьма факторами і, як наслідок, створювати умови, що не дозволять виконувати завдання у наступі, під час розвитку успіху та при вирішенні інших бойових завдань у наступну добу бойових дій.

З метою забезпечення виконання бойових завдань частинами та підрозділами ЗСУ та недопущення обмеження їх боєздатності у зв'язку із непередбаченою нестачею пального в ході операції, виникає необхідність у розробці математичної моделі, застосування якої у подальшому дозволить розраховувати час, після якого рівень запасів пального знизиться нижче за допустиму норму, і в динаміці роботи штабів логістики сприяє своєчасному забезпеченню потреб військ.

У статті вперше отримані прості вирази для розрахунку необхідного обсягу вибірки випадкової величини швидкості витрати пального у підрозділі ЗСУ і для похибки оцінки математичного сподівання цієї величини у вибірці, що гарантує виконання вимог до точності розрахунків при обсягу вибірки істотно меншому, ніж традиційний і без використання понять "довірчий інтервал" і "довірча ймовірність", та відповідає обмеженням можливостям підрозділів ЗСУ зі збору статистики під час бойових дій.

Розроблена модель може бути використана для подальших розробок математичних інструментів прогнозування можливих витрат пального, для передбачення потреб та для своєчасного забезпечення військ паливом до встановлених норм.

Ключові слова: випадкові витрати пального, середнє арифметичне випадкової величини, число спроб, обсяг вибірки.

Вступ та постановка проблеми. Процес управління військами (силами) пов'язаний з необхідністю прийняття рішень з численних питань організації їх життєдіяльності. При цьому існують сфери діяльності, в яких рішення слід приймати на основі дослідних, у тому числі експериментальних оцінок, що мають статистичний характер. Прикладами питань у таких областях можуть бути:

- прогноз початкових та залишкових ресурсів озброєння та військової техніки;
- визначення живучості зразків озброєння та військової техніки;
- прогноз необхідної номенклатури та кількості запасних частин для зразків озброєння та військової техніки на період їх експлуатації у повсякденних та у бойових умовах;
- визначення норм витрати паливно-мастильних матеріалів автомобільної та іншої техніки при її експлуатації у мирний час та в ході бойових дій.

У зв'язку з цим, при плануванні робіт та експериментів зі статистичної оцінки параметрів зазначених та інших реальних процесів виникає необхідність визначення такого обсягу n вибірки, який з необхідною ймовірністю β забезпечує оцінку параметра X з похибкою ΔX не більш допустимої ε , тобто за умови $(|\Delta X| \leq \varepsilon)$. Зворотним є завдання визначення точності ε оцінки параметра X за вибіркою заданого обсягу n .

За результатами вивчення досвіду ведення бойових дій у війні з Російською Федерацією спостерігається зростання інтенсивності та швидкості переміщення військ (сил),

ведення бойових дій на широкому фронті, на більшу глибину та у більш високому темпі, ніж це було раніше [1].

За цих обставин, у зв'язку із зростанням інтенсивності експлуатації військової техніки, в різних умовах бойових дій з'являються позапланові (випадкові) витрати пального з одночасним раптовим зниженням запасів нижче допустимих (встановлених) норм.

Для своєчасного поповнення запасів палива органи військового управління повинні мати інструменти для прогнозу часу, після закінчення якого рівень запасів пального в підрозділах та частинах ЗСУ знизиться нижче за допустиму норму.

Однак на даний час методичний апарат, який може дозволити прогнозувати витрати пального підрозділами та частинами ЗСУ з урахуванням випадкової швидкості витрати пального, відсутній. Ключовим елементом такого апарату можуть бути засоби оцінки математичного сподівання випадкової швидкості витрат пального.

Відомі методи математичної статистики, наприклад [2 - 7], дають змогу отримувати оцінку математичного сподівання випадкової швидкості витрати пального з допустимою похибкою. Однак ці методи передбачають необхідність суттєво великого обсягу вибірки (кілька сотень значень випадкової величини), що є недосяжним у ході маневрених бойових дій підрозділів ЗСУ.

Відсутність зазначеного методичного апарату не дозволяє органам військового управління розрахувати час, після якого рівень запасів пального у підрозділах та частинах ЗСУ знизиться нижче за допустиму норму, що створює труднощі у динаміці роботи штабів логістики вирішувати завдання своєчасного поповнення запасів пального. Визначенні обставини роблять актуальною проблему розробки моделі з метою оцінки математичного очікування випадкової величини швидкості витрати пального підрозділами ЗСУ під час бойових дій.

Аналіз останніх досліджень і публікацій. Відоме вирішення цього завдання з використанням центральної граничної теореми [8], нормального закону розподілу $F(x)$ [8, С.175], інтегралу ймовірності $\Phi(x)$ та його зворотної функції $t_\beta = \arg \Phi(\beta/2)$, величини довірчого інтервалу ε , а також позначення середнього квадратичного відхилення σ , можна записати у вигляді:

$$n = \frac{t_\beta^2 \cdot \sigma^2}{\varepsilon^2}. \quad (1)$$

Теоретичні оцінки гарантованих меж зміни значень параметрів є важливою точкою опори щодо прийняття рішень, але, у більшості випадків ці оцінки є завищеними. Так, з нерівності Чебишева [8, С. 204] випливає, що гарантована ймовірність відхилення випадкової величини X від свого математичного сподівання m більш ніж на три середні квадратичні відхилення σ , обмежена і становить $P = 1/9 = 0,111$:

$$P(|X - m| \geq 3\sigma) \leq \frac{D}{(3\sigma)^2} = \frac{1}{9} \cong 0,111. \quad (2)$$

Однак відомо, що, наприклад, для нормального закону розподілу випадкової величини ця ймовірність приблизно дорівнює 0,003 [8, С. 192], тобто приблизно у 37 разів менше. Такі розбіжності можуть призводити до істотної перевитрати ресурсів на організацію вибіркового спостереження і до недооцінювання точності розрахунків за вже наявними вибірками.

Мета статті полягає у розробці моделі визначення мінімально необхідного обсягу вибірки для виконання обґрунтованих оцінок математичного сподівання випадкової величини швидкості витрати пального у підрозділі ЗСУ в ході бойових дій.

Виклад основного матеріалу. Введемо позначення кількості періодів спостереження – n та позначення випадкової швидкості ξ витрати пального в i -му періоді спостереження – " x_i ". На практиці, у якості оцінки математичного сподівання використовують середнє арифметичне значень випадкової величини ξ , процес кількісної оцінки якого розглянемо далі.

Об'єктом дослідження у статті є процес визначення мінімально необхідного обсягу вибірки для оцінки математичного сподівання швидкості витрати пального під час бойових дій (випадкової величини ξ).

Предметом дослідження є моделювання процесу визначення мінімально необхідного обсягу вибірки для виконання обґрунтованих оцінок математичного сподівання випадкової величини (ξ) – швидкості витрати пального підрозділом ЗСУ під час бойових дій.

З метою уточнення відповідних граничних співвідношень скористаємося відомим формулюванням теореми Чебишева [8, С. 204]. Якщо в n незалежних випробуваннях спостерігаються $x_1, \dots, x_n$ значень випадкової величини ξ , то при $n \rightarrow \infty$ середнє арифметичне випадкової величини ξ сходиться по ймовірності до її математичного сподівання m . Тобто, за будь-якого $\varepsilon > 0$ і $\delta > 0$ виконується нерівність:

$$\lim_{n \rightarrow \infty} P \left(\left| m - \frac{1}{n} \sum_{i=1}^n x_i \right| \geq \varepsilon \right) \leq 1 - \delta. \quad (3)$$

Розглянемо процес "збіжності за ймовірністю" середнього арифметичного випадкової величини ξ до її математичного сподівання m .

Для кількісної оцінки швидкості "збіжності за ймовірністю" з'ясуємо, як змінюється середнє арифметичне ($\bar{x}_n$) випадкової величини ξ при збільшенні числа спроб, тобто числа доданків під знаком суми у виразі (3) від значення обсягу вибірки, що дорівнює $n-1$, до значення n , отримаємо:

$$\bar{x}_{n-1} = \frac{1}{n-1} \sum_{i=1}^{n-1} x_i, \quad \text{відкіля знаходимо} \quad \sum_{i=1}^{n-1} x_i = (n-1) \cdot \bar{x}_{n-1}. \quad (4)$$

Наведемо наступне значення середнього арифметичного через його попереднє значення:

$$\bar{x}_n = \frac{1}{n} \sum_{i=1}^n x_i = \frac{1}{n} \left(\sum_{i=1}^{n-1} x_i + x_n \right) = \frac{1}{n} \left((n-1) \cdot \bar{x}_{n-1} + x_n \right) = \bar{x}_{n-1} + \frac{x_n - \bar{x}_{n-1}}{n}; \quad (5)$$

Позначимо величину збільшення попереднього середнього значення у виразі (5):

$$\Delta \bar{x}_n = \frac{x_n - \bar{x}_{n-1}}{n} \quad (6)$$

і напишемо вираз (5) коротше:

$$\bar{x}_n = \bar{x}_{n-1} + \Delta \bar{x}_n. \quad (7)$$

Таким чином, нове (наступне) значення середнього арифметичного ($\bar{x}_n$) випадкової величини ξ можна виразити (7) через попереднє значення її середнього арифметичного з урахуванням приросту $\Delta \bar{x}_n$ (6). Так як під знаком суми у виразах (4) і (5) складаються випадкові значення (x_i) величини ξ , то середнє арифметичне випадкової величини ξ , також буде величиною випадковою.

При необмеженому збільшенні обсягу вибірки величина приросту (6) в рівності (5) прагне до нуля,

$$\lim_{n \rightarrow \infty} \left(\frac{x_n - \bar{x}_{n-1}}{n} \right) = 0, \quad (8)$$

що дозволяє вважати рівності (5) і (7) варіантом моделі процесу оцінки математичного сподівання випадкової величини, вже придатної для якісної оцінки динаміки цього процесу.

Змінні, що стоять у чисельнику виразу (6), є величинами випадковими. Врахуємо діапазон можливих значень ($x_{\max} \leq x_i \leq x_{\min}$) випадкової величини ξ і спробуємо з'ясувати, як змінюється абсолютна величина збільшення $\Delta \bar{x}_n$ (6) зі збільшенням обсягу вибірки (числа спроб) n . Для цього перейдемо до оцінок за модулем виразів у правій і в лівій частині (6) і замінимо вираз у чисельнику формули (6) значеннями максимальної ($x_{\max}$) і мінімальної ($x_{\min}$)

меж діапазону зміни випадкової величини ξ , що призведе до свідомо більшого значення чисельника в (6), отримаємо нерівність:

$$\left| \Delta \bar{x}_n \right| \leq \left| \frac{x_{\max} - x_{\min}}{n} \right|. \quad (9)$$

Отже, після першого дослідження ($n=1$) величина приросту може дорівнювати величині всього діапазону можливих значень (x_i), після другого дослідження ($n=2$) – величина приросту може дорівнювати половині діапазону, після третього ($n=3$) – третій частині діапазону можливих значень, і так далі відбувається ділення діапазону можливих значень на більш дрібні частини.

Сукупність випадкових доданок (6) являє собою знаковмінний ряд з монотонно спадаючими членами ряду. Загальний член ряду (6), при необмеженому зростанні обсягу n вибірки, дорівнює нулю (8). Тому, відповідно до ознаки Лейбніца, наприклад у [9 - 12], ряд сходиться. В даному випадку, «сходиться за ймовірністю» до математичного сподівання випадкової величини ξ .

Часткова сума ряду не перевищує величини модуля першого з відкинутих членів ряду. Отже, можлива похибка (6) оцінок середнього арифметичного при збільшенні обсягу вибірки (числа спроб) n буде зменшуватися за законом (6), який мажоредується величиною, що стоїть у правій частині нерівності (9).

Знак різниці випадкових величин, що стоять у дужках (6) може бути як позитивним, так і негативним, тому можна стверджувати, що абсолютне значення похибки розрахунків не перевищує величини, що стоїть у правій частині нерівності (9) для будь-якого конкретного обсягу вибірки n .

Таким чином, при необмеженому збільшенні числа спроб n значення величини (6) збільшення $\Delta \bar{x}_n$ середнього арифметичного, залишаючись випадковою величиною, буде прагнути до нуля:

$$\lim_{n \rightarrow \infty} \Delta \bar{x}_n = \lim_{n \rightarrow \infty} \frac{x_n - \bar{x}_{n-1}}{n} = 0. \quad (10)$$

Отже, середнє арифметичне $\bar{x}_n$ (4), (5) випадкової величини ξ буде величиною випадковою за будь-якої кінцевої кількості доданків ($n < \infty$). Однак, при необмеженому збільшенні числа доданків ($n \rightarrow \infty$) величина $\Delta \bar{x}_n$ додаткової випадкової складової (6) зменшується (10) аж до нуля.

Таким чином, вирази (5), (6), (7), (9) та (10) є варіантом моделі процесу "збіжності за ймовірністю" середнього арифметичного випадкової величини ξ до її математичного сподівання m .

Для оцінки швидкості (V) "збіжності за ймовірністю" візьмемо похідну по n від лівої та від правої частини нерівності (9), отримаємо:

$$V = \left| \frac{d \Delta \bar{x}}{dn} \right| \leq \frac{-|x_{\max} - x_{\min}|}{n^2}. \quad (11)$$

З нерівності (11) випливає висновок про те, що швидкість (V) "збіжності за ймовірністю" негативна, тобто величина збільшення зменшується зі зростанням обсягу вибірки, і є обернено пропорційною квадрату обсягу n вибірки. Такий результат дозволяє стверджувати суттєвий вплив перших 10 доданків у розрахунковому виразі (5) для середнього арифметичного випадкової величини ξ і різке (у десятки разів) зниження впливу на величину середнього арифметичного з боку наступних доданків.

Таким чином, враховуючи знаковмінний характер випадкової добавки (6) в моделі (7), можна стверджувати, що основний внесок у визначення значення середнього арифметичного $\bar{x}_n$ випадкової величини ξ вносять перші доданки в сумі (5).

Для загального випадку вибірки довільної випадкової величини виконаємо лінійне перетворення вибірки, яке змінює початок відліку та одиницю масштабу вимірювання членів вибірки – змістимо початок відліку величини членів вибірки на початок координат і змінимо масштаб вимірювання членів вибірки:

$$u_i = (x_i - x_{\min}) / (x_{\max} - x_{\min}), \quad i = 1, \dots, n. \quad (12)$$

У такому разі граничні значення діапазону еквівалентної вибірки виявляться рівними:

$$\left. \begin{aligned} u_{\min} &= (x_{\min} - x_{\min}) / (x_{\max} - x_{\min}) = 0 \\ u_{\max} &= (x_{\max} - x_{\min}) / (x_{\max} - x_{\min}) = 1 \end{aligned} \right\} \quad (13)$$

$$u_{\max} = 1; \quad u_{\min} = 0. \quad (14)$$

При цьому вирази для діапазону значень похибки розрахунків оцінки середнього арифметичного вже випадкової величини u_i у вибірці обсягом n для нормованих членів вибірки набудуть вигляду:

$$\bar{u}_n = \frac{1}{n} \sum_{i=1}^n u_i = \bar{u}_{n-1} + \frac{u_n - \bar{u}_{n-1}}{n}; \quad (15)$$

$$|\Delta \bar{u}_n| \leq \left| \frac{u_{\max} - u_{\min}}{n} \right| = \left| \frac{1 - 0}{n} \right| = \left| \frac{1}{n} \right|; \quad (16)$$

$$|\Delta \bar{u}_n| \leq \frac{1}{n}. \quad (17)$$

Межі зміни похибки розрахунків середнього арифметичного еквівалентної нормованої випадкової величини u_i та початкової випадкової величини x_i у такій вибірці обсягом n можна представити у явному вигляді:

$$\left. \begin{aligned} \Delta_{\max, u} &= \frac{1}{n}; \quad \Delta_{\min, u} = -\frac{1}{n}; \quad \Delta_x = x_{\max} - x_{\min}; \\ \Delta_{\max, x} &= \frac{1}{n} \cdot \Delta_x; \quad \Delta_{\min, x} = -\frac{1}{n} \cdot \Delta_x; \\ \Delta_{\min, u} &\leq \Delta \bar{u}_n \leq \Delta_{\max, u}; \quad \Delta_{\min, x} \leq \Delta \bar{x}_n \leq \Delta_{\max, x}. \end{aligned} \right\} \quad (18)$$

З нерівності (17) можна знайти обсяг вибірки n_b , необхідний для отримання оцінок середнього арифметичного нормованої випадкової величини u_i з похибкою не більшою за допустиму $|\Delta \bar{u}_n|$:

$$n_b \geq \frac{1}{|\Delta \bar{u}_n|}. \quad (19)$$

Абсолютне значення оцінки середнього арифметичного початкової випадкової величини ξ і модуля похибки $\Delta \bar{x}_n$ такої оцінки можна покроково знайти з виразу (15) шляхом підстановки в цей вираз рівності (12):

$$\bar{x}_n = \bar{u}_n \cdot (x_{\max} - x_{\min}) + x_{\min}, \quad (20)$$

$$|\Delta \bar{x}_n| = |\Delta \bar{u}_n| \cdot (x_{\max} - x_{\min}), \quad (21)$$

$$\frac{x_n - \bar{x}_{n-1}}{n \cdot (x_{\max} - x_{\min})} = \frac{(u_n - \bar{u}_{n-1})}{n}. \quad (22)$$

При цьому відносне значення похибки оцінки середнього арифметичного $\bar{x}_n$ початкової випадкової величини ξ можна представити в явному вигляді:

$$\frac{|\Delta \bar{x}_n|}{(x_{\max} - x_{\min})} = |\Delta \bar{u}_n|. \quad (23)$$

Для додаткової оцінки можливих чисельних значень похибки розрахунків середнього арифметичного еквівалентної випадкової величини u_i в межах інтервалу значень (18) введемо позначення для відношення величини похибки до розміру цього інтервалу:

$$D_{u,\Delta} = \frac{|\Delta \bar{u}_n|}{\Delta_{\max,u} - \Delta_{\min,u}}. \quad (24)$$

Приклад зміни величини збільшення $\Delta \bar{u}_n$ оцінок середнього арифметичного $\bar{u}_n$ випадкової величини, яка змінюється в межах $u_i \in [0; 1]$, що відповідає початковій рівномірно розподіленій [4] випадковій величині ξ , при зміні кількості спроб n (числа елементів у вибірці) для умов $u_{\min} = 0$; $u_{\max} = 1$, представлений у таблиці 1 і наведено на рис. 1. Лінії обмежень на рис. 1 отримані відповідно до формули (17):

$$\Delta_{\max,u} = \frac{1}{n}; \quad \Delta_{\min,u} = -\frac{1}{n}. \quad (25)$$

Наведений приклад (табл.1, колонка 11) демонструє часткову закономірність, відповідно до якої похибка $D_{u,\Delta}$ (24) оцінки вибіркового середнього еквівалентної рівномірно розподіленої випадкової величини u_i , у вибірці виявляється в три рази менше ширини інтервалу гарантованих значень похибки:

$$\max(D_{u,\Delta}) = 32 [\%]. \quad (26)$$

Нерівність (19) дозволяє стверджувати, що з оцінки вибіркового середнього з похибкою не більш ніж $\pm 5\%$ ($|\Delta \bar{u}_n| = \varepsilon = 0,05$) достатнім може бути обсяг вибірки $n_b \geq 20$.

При цьому, у практичних розрахунках може бути врахована часткова закономірність (26), відповідно до якої похибка розрахунків виявляється приблизно в 2-3 рази меншою за діапазон обмежень розміру похибки розрахунків (25). Отже, шукане значення похибки $\varepsilon = 0,05$ може бути досягнуто при значеннях допустимої похибки $|\Delta \bar{u}_n|$ в два рази більших, ніж необхідні, що може відповідати меншому обсягу вибірки:

$$n_b \geq \frac{1}{2 \cdot |\Delta \bar{u}_n|}. \quad (27)$$

У наведеному вище прикладі для досягнення оцінки вибіркового середнього з похибкою не більше $\pm 5\%$ ($|\Delta \bar{u}_n| = \varepsilon = 0,05$) достатнім може виявитися обсяг вибірки $n_b = 10$.

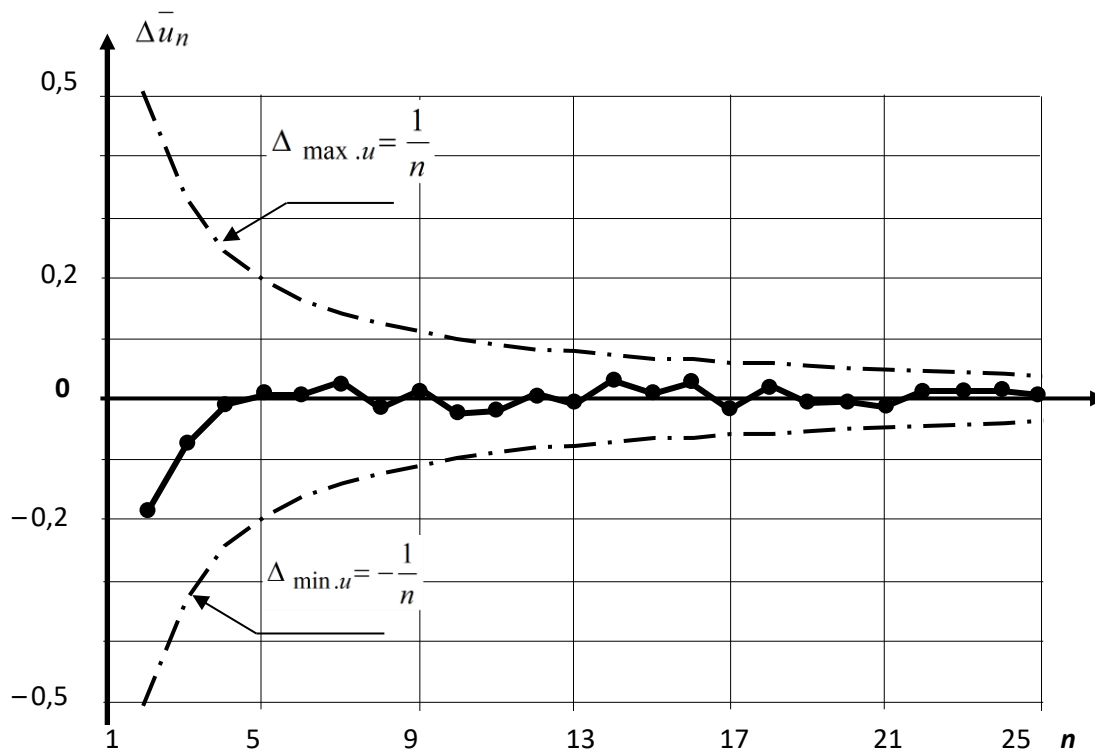


Рисунок 1 - Приклад залежності відносного значення довільної похибки $\Delta \bar{u}_n$ оцінки вибіркового середнього від обсягу вибірки n

Оцінку абсолютного значення похибки розрахунків $\Delta \bar{x}_n$ середнього арифметичного випадкової величини ξ можна також знайти, помноживши оцінку вибіркового середнього нормованої випадкової величини u_i на величину діапазону значень початкової випадкової величини x_i (21).

У свою чергу, якщо за вибіркою обсягу n_b вже отримані значення $\bar{x}_n$ – вибіркового середнього (середнього арифметичного), то відносна похибка, що виникає при цьому, може бути оцінена відповідно до нерівності (17):

$$\frac{|\Delta \bar{x}_n|}{(x_{\max} - x_{\min})} = |\Delta \bar{u}_n| \leq \frac{1}{n_b} \dots \quad (28)$$

Таблиця 1.

Оцінка процесу збіжності середнього арифметичного $\bar{x}_n$ значень рівномірно розподіленої $x_i \in [0;100]$ випадкової величини ξ та еквівалентних величин $u_i \in [0;1]$

n_b	x_i	$\bar{x}_n$	$\Delta \bar{x}_n$	$\bar{x}_{n, \text{отн}}$	u_i	$\bar{u}_n$	$\Delta_{\max, u}$	$\Delta \bar{u}_n$	$\Delta_{\min, u}$	$D_{u\Delta}, \%$	$\Delta_{\max, x}$
1	2	3	4	5	6	7	8	9	10	11	12
1	73	73	–	–	0,73	0,73	1	–	1	–	1
2	9	41	-32	0,562	0,09	0,41	0,500	-0,3200	-0,500	32,00	50,00
3	10	30,67	-10,33	0,748	0,1	0,3067	0,333	-0,1033	-0,333	15,50	33,33
4	25	29,25	-1,42	0,954	0,25	0,2925	0,250	-0,0142	-0,250	2,83	25,00
5	33	30	0,75	1,026	0,33	0,3	0,200	0,0075	-0,200	1,88	20,00

6	37	31,17	1,17	1,039	0,37	0,3117	0,167	0,0117	-0,167	3,50	16,67
7	54	34,43	3,26	1,105	0,54	0,3443	0,143	0,0326	-0,143	11,42	14,29
8	20	32,63	-1,80	0,948	0,2	0,3263	0,125	-0,0180	-0,125	7,21	12,50
9	48	34,33	1,71	1,052	0,48	0,3433	0,111	0,0171	-0,111	7,69	11,11
10	5	31,4	-2,93	0,915	0,05	0,314	0,100	-0,0293	-0,100	14,67	10,00
11	8	29,27	-2,13	0,932	0,08	0,2927	0,091	-0,0213	-0,091	11,70	9,09
12	42	30,33	1,06	1,036	0,42	0,3033	0,083	0,0106	-0,083	6,36	8,33
13	26	30	-0,33	0,989	0,26	0,3	0,077	-0,0033	-0,077	2,17	7,69
14	89	34,21	4,21	1,140	0,89	0,3421	0,071	0,0421	-0,071	29,50	7,14
15	53	35,47	1,25	1,037	0,53	0,3547	0,067	0,0125	-0,067	9,39	6,67
16	99	39,44	3,97	1,112	0,99	0,3944	0,063	0,0397	-0,063	31,77	6,25
17	1	37,18	-2,26	0,943	0,01	0,3718	0,059	-0,0226	-0,059	19,22	5,88
18	90	40,11	2,93	1,079	0,9	0,4011	0,056	0,0293	-0,056	26,41	5,56
19	25	39,32	-0,80	0,980	0,25	0,3932	0,053	-0,0080	-0,053	7,56	5,26
20	29	38,8	-0,52	0,987	0,29	0,388	0,050	-0,0052	-0,050	5,16	5,00
21	12	37,52	-1,28	0,967	0,12	0,3752	0,048	-0,0128	-0,048	13,40	4,76
22	80	39,45	1,93	1,051	0,8	0,3945	0,045	0,0193	-0,045	21,24	4,55
23	79	41,17	1,72	1,044	0,79	0,4117	0,043	0,0172	-0,043	19,77	4,35
24	99	43,58	2,41	1,059	0,99	0,4358	0,042	0,0241	-0,042	28,91	4,17
25	70	44,64	1,06	1,024	0,7	0,4464	0,040	0,0106	-0,040	13,21	4,00
384	93	49,11	0,11	1,002	0,93	0,4911	0,003	0,0011	-0,003	22,00	0,26

Для визначення зв'язку абсолютної похибки (ε_A), що відрізняє оцінку $\bar{x}_n$ від істинного значення математичного сподівання m , і для визначення необхідної кількості елементів у вибірці (обсягу вибірки n_B) можна скористатися виразом (9). Тоді отримаємо:

$$\varepsilon_A \leq \left| \frac{x_{\max} - x_{\min}}{n_B} \right|; \quad n_B \geq \left| \frac{x_{\max} - x_{\min}}{\varepsilon_A} \right|. \quad (29)$$

Зазначимо, що в розробленій моделі самі межі (13), (17), (18), (25) оцінки похибки розрахунків (мажоранти) не потребують використання категорій "довірча ймовірність" і "довірчий інтервал", прийнятих у математичній статистиці [2 - 7].

Розглянемо приклад, що ілюструє традиційний і розроблений варіанти оцінки обсягу вибірки. Знайдемо обсяг вибірки n для оцінки ймовірності виникнення деякої події A (наприклад, попадання в ціль при одному пострілі), яке в результаті однієї спроби може відбутися або не відбутися приблизно з однаковою ймовірністю $p = q = 0,5$. У цьому випадку $\sigma^2 = p \cdot q = 0,25$.

Використовуючи традиційний підхід, вираз (1) для прийнятого в математичній статистиці [2 - 7] рівня довірчої ймовірності $\beta = 0,95$ та довірчого інтервалу $\varepsilon = 0,05$, величину $t_\beta = 1,96$, отримаємо оцінку необхідного обсягу вибірки для оцінки ймовірності появи події A з похибкою не більше $\pm 0,05$:

$$n = \frac{t_\beta^2 \cdot \sigma^2}{\varepsilon^2} = \frac{1,96^2 \cdot 0,25}{0,05^2} = 384,16.$$

Для розглянутого варіанта, використовуючи (16) при $\varepsilon = 0,05$, знаходимо:

$$n_B \geq \frac{1}{\varepsilon} = \frac{1}{0,05} = 20.$$

Таким чином, одержуване при традиційному підході значення числа елементів n у вибірці в 19,2 рази перевищує реально необхідне, що може мати істотне значення для визначення витрат на проведення експерименту з набору статистики. Зазначимо також, що при $n = 384$ величина відносної похибки розрахунків буде відрізнятися від передбачуваних п'яти відсотків і складе $\varepsilon \leq 1/384 = 0,0026$, тобто не більше 0,26%. (див. табл. 1, останній рядок).

Висновки. Мета статті полягала в розробленні моделі визначення мінімально необхідного обсягу вибірки для виконання обґрунтованих оцінок математичного сподівання випадкової величини (ξ) швидкості витрати пального у підрозділі ЗСУ з метою його своєчасного поповнення в ході бойових дій.

У статі вперше отримані прості вирази для розрахунку необхідного обсягу вибірки випадкової величини (ξ) швидкості витрати пального у підрозділі ЗСУ і для похибки оцінки математичного сподівання цієї величини у вибірці. Визначені вирази гарантують виконання вимог до точності розрахунків при обсягу вибірки істотно меншою, ніж традиційний обсяг, не застосовуючи поняття "довірчий інтервал" і "довірча ймовірність".

Використання розробленої моделі відкриває можливості для розробки математичних інструментів, які можуть дозволити органам управління служби пального прогнозувати значення часу до моменту вичерпання запасів палива в підрозділах ЗСУ до встановленого рівня з урахуванням планової та випадкової витрати пального.

У результаті, з'являється можливість оперативного вживання заходів із своєчасного поповнення запасів пального, що сприяє підвищенню ефективності функціонування системи забезпечення військ паливом та підтриманню боєздатності частин та підрозділів ЗСУ в ході ведення бойових дій.

Напрямок подальшого дослідження може бути розробка відповідної математичної моделі для прогнозу часу, після якого обсяг пального, яке залишилося в підрозділі ЗСУ, знизиться нижче критичного (допустимого) рівня, з урахуванням планової та випадкової витрати пального в ході ведення бойових дій.

ЛІТЕРАТУРА:

1. Тимчасовий бойовий статут "Механізованих військ Сухопутних військ Збройних сил України" частина 1 (бригада)/ Командування СВ ЗС України. – Київ: МОУ, 2021. – 116 с.
2. Ефимова М.Р., Петрова Е.В., Румянцев В.Н. Общая теория статистики: учебник. – М.: ИНФРА-М, 1998. – 416 с.
3. Блягоз З.У. Теория вероятностей и математическая статистика. Курс лекций: учебное пособие. – СПб.: Лань, 2018. – 224 с.
4. Гмурман В.Е. Руководство к решению задач по теории вероятностей и математической статистике: учебное пособие, 3-е изд., перераб. и доп. – М.: Высшая школа, 1979. – 400 с.
5. Балдин К.В. Теория вероятностей и математическая статистика: учебник / К.В. Балдин, В.Н. Башлыков. – М.: Дашков и К, 2016. – 472 с.
6. Ивченко Г.И., Медведев Ю.И. Математическая статистика: учебник. – М.: Книжный дом «ЛИБРОКОМ», 2014. – 352 с.
7. Сидняев Н. И. Теория вероятностей и математическая статистика: учебник для ср. проф.обр. – М.: Юрайт, 2023. – 219 с.
8. Городнов В.П. Вища математика (популярно, із прикладами): підручник для студ. екон. спец. вищ. навч. закл. Видання 3-є / В.П. Городнов. – Х.: Вид-во АБВ МВС України, 2013. – 372 с.
9. Гредасова Н.В., Желонкина Н. И., Корешникова М.А., Полищук Е.Г., Андреева И.Ю. Ряды: учебное пособие. – Екатеринбург: Урал, 2016. – 116 с.
10. Прусова И. В., Кондратьева Н. А., Прихач Н. К. Высшая математика. Ряды, теория функций комплексного переменного, операционное исчисление: учебное пособие – Минск: БНТУ, 2017. – 154 с.
11. Панкратова Л.В. Числовые ряды: учебное пособие – Красноярск: Научно-инновационный центр, 2020. – 126 с.
12. Рудой Е.М. Математический анализ. Числовые и функциональные ряды: учебное пособие – Новосибирск: Изд. НГПУ, 2010. – 95 с.

REFERENCES:

1. Timchasovij bojovij statut "Mehanizovanih vijsk Suhoputnih vijsk Zbrojnih sil Ukrayini" chastina 1 (brigada) / Komanduvannya SV ZS Ukrayini. [Temporary combat charter of the «Mechanized Ground Forces of Ukraine» part 1 (Brigade)/ Command of the Armed Forces of Ukraine], Kyiv, MOU, 2021. 116 p.
2. Efimova, M.R., Petrova, E.V., Rumyantsev, V.N. "Obshaya teoriya statistiki" [General theory of statistics], uchebnik. M.: INFRA-M, 1998. 416 p.
3. Blyagoz, Z.U. "Teoriya veroyatnostej i matematicheskaya statistika" [Probability theory and mathematical statistics], Kurs lekcij: uchebnoe posobie. SPb.: Lan, 2018. 224 p.
4. Gmurman, V.E. "Rukovodstvo k resheniyu zadach po teorii veroyatnostej i matematicheskoy statistike" [Guide to problem solving in probability theory and mathematical statistics], uchebnoe posobie, 3-e izd., pererab. i dop. M.: Vysshaya shkola, 1979. 400 p.
5. Baldin, K.V. "Teoriya veroyatnostej i matematicheskaya statistika" [Probability theory and mathematical statistics], uchebnik / K.V. Baldin, V.N. Bashlykov. M.: Dashkov i K, 2016. 472 p.
6. Ivchenko, G.I., Medvedev, Yu.I. "Matematicheskaya statistika" [Mathematical statistics], uchebnik. M.: Knizhnyj dom «LIBROKOM», 2014. 352 p.
7. Sidnyaev, N. I. "Teoriya veroyatnostej i matematicheskaya statistika" [Probability theory and mathematical statistics], uchebnik dlya sr. prof. obr. M.: Yurajt, 2023. 219 p.
8. Gorodnov, V.P. "Visha matematika" (populyarno, iz prikladami) [Higher mathematics (popular, with examples)], pidruchnik dlya stud. ekon. spec. vish. navch. zakl. Vidannya 3-e / V.P. Gorodnov. H.: Vidvo AVV MVS Ukrayini, 2013. 372 p.
9. Gredasova, N.V., Zhelonkina, N. I., Koreschnikova, M.A., Polishuk, E.G., Andreeva, I.Yu. "Ryady": uchebnoe posobie. Ekaterinburg: Ural, 2016. 116 p.
10. Prusova, I. V., Kondrateva, N. A., Prihach, N. K. "Vysshaya matematika. Ryady, teoriya funkciy kompleksnogo peremennogo, operacionnoe ischislenie" [Higher mathematics. Rows, theory of a complex variable, operational calculus], uchebnoe posobie. Minsk: BNTU, 2017. 154 p.
11. Pankratova, L.V. "Chislovye ryady" [Number series], uchebnoe posobie, Krasnoyarsk: Nauchno-innovacionnyj centr, 2020. 126 p.
12. Rudoj, E.M. "Matematicheskij analiz. Chislovye i funkcionalnye ryady" [Mathematical analysis. Numerical and functional series], uchebnoe posobie. Novosibirsk: Izd. NGPU, 2010. 95 p.

D. of Mil. S., Prof. Gorodnov V.P., Cand. of Mil. S., As. Prof. Kovalev I.V., Druzhinin V.S.

MODEL FOR ASSESSMENT THE MATHEMATICAL EXPECTATION SPEED OF FUEL CONSUMPTION BY MILITARY SUBUNITS OF THE ARMED FORCES OF UKRAINE

The study of the experience of conducting an anti-terrorist operation (ATO) and an operation of the United Forces (OUF) in the war against the Russian Federation allows us to conclude that today the use of modern means of fire damage in combination with new approaches to intelligence conducting has had a significant effect on increasing the intensity and speed of troops movement during hostilities.

In such conditions, random (unforeseen) consumption of fuel may appear with a simultaneous sudden decrease in its reserves below the specified (acceptable) norms. An unexpected drop in fuel reserves in military equipment can be related to many factors and, as a result, create conditions that will not allow to perform tasks in the offensive, during the development of success and when solving other combat tasks in the next day of hostilities.

In order to ensure the fulfillment of combat missions by units and subunits of the Armed Forces and to prevent the limitation of their combat capability in connection with an unforeseen shortage of fuel during the operation, there is a need to develop a mathematical model, the use of which in the future will allow to calculate the time after which the level of fuel reserves will decrease below the permissible norm, and in the dynamics of the work of the logistics headquarters, it contributes to the timely provision of the troops needs.

In the article, for the first time, simple expressions were obtained for calculating the required sample volume of a random fuel consumption value in the UAF subunits and for the error of estimating the mathematical expectation of this value in the sample, which guarantees the fulfillment of the requirements for the accuracy of calculations with a sample size significantly smaller than the traditional one and without using the concepts of "confidence interval" and "confidence probability", and

corresponds to the limited capabilities of the Ukraine Armed Forces subunits to collect statistics during hostilities.

The developed model can be used for further development of mathematical tools for predicting possible fuel consumption, for predicting needs and for providing the troops with fuel up to the established standards in a timely manner.

Keywords: random fuel consumption, arithmetic mean of a random variable, number of attempts, sample size.

д.т.н., с.н.с. **Купріненко О.М.** (НАСВ, м. Львів)
к.т.н., доц. **Нагачевський В.Й.** (НАСВ, м. Львів)
к.т.н., с.н.с. **Кривцун В.І.** (НАСВ, м. Львів)
к.т.н., с.н.с. **Фтемов Ю.О.** (НАСВ, м. Львів)
к.т.н., доц. **Мищенко Я.С.** (НАСВ, м. Львів)
Заверуха Г.В. (ХІТВ, м. Харків)

DOI: <http://doi.org/10.17721/2519-481X/2023/80-04>

МЕТОДИКА ВИЗНАЧЕННЯ ПОТРЕБИ В НАЗЕМНИХ РОБОТИЗОВАНИХ КОМПЛЕКСАХ ПІДРОЗДІЛІВ СУХОПУТНИХ ВІЙСЬК

В роботі наведено результати теоретичних досліджень щодо визначення потреби в наземних роботизованих комплексах підрозділів Сухопутних військ. Проведено аналіз характеру ведення сучасної збройної боротьби. Обґрунтовано необхідність пошуку шляхів зменшення втрат особового складу та актуальність розвитку наземних роботизованих комплексів. Проведено порівняльний аналіз стану розвитку наземних роботизованих комплексів в провідних країнах світу та в Україні. За результатами проведеного порівняльного аналізу встановлено проблемні питання, що стримують розвиток і постачання наземних роботизованих комплексів для потреб Сухопутних військ. Встановлено одним з важливих проблемних питань – недостатню ефективність воєнно-наукових досліджень з визначення потреби в наземних роботизованих комплексах.

Встановлено фактори, які впливають на процес визначення потреби підрозділів Сухопутних військ в наземних роботизованих комплексах. Запропоновано науково-методичний апарат, який враховує досвід бойового застосування підрозділів Сухопутних військ, умови, характер виконання завдань, рівень розвитку технологій з області робототехніки та дозволяє визначати перелік завдань, для яких доцільно використовувати наземні роботизовані комплекси, та потребу підрозділів Сухопутних військ.

З урахуванням досвіду бойового застосування підрозділів Сухопутних військ в російсько-українській війні визначено основні завдання, для вирішення яких доцільно використовувати наземні роботизовані комплекси. Обґрунтовано доцільність використання імітаційної системи JCATS для моделювання типових ситуацій застосування наземних роботизованих комплексів. Критерієм ефективності виконання покладених на наземні роботизовані комплекси завдань запропоновано мінімальні втрати за умови забезпечення виконання завдань.

Із використанням запропонованого науково-методичного апарату визначено зразки, ефективність застосування яких відповідає прийнятому критерію. З урахуванням отриманих результатів для проведення подальших випробувань в бойових умовах обґрунтовано пропозиції щодо організаційної структури експериментально-бойового підрозділу у складі окремої механізованої (мотопіхотної) бригади.

Ключові слова: наземні роботизовані комплекси, потреба, сухопутні війська, моделювання, імітаційна система JCATS.

Вступ. Десятирічний досвід війни росії проти України та воєнних конфліктів останніх десятиріч свідчить про суттєве зростання можливостей сучасних систем озброєння, яке є результатом широкого застосування у військовій сфері досягнень в області інформаційних технологій.

Суттєве збільшення дальності, швидкості, точності та вибіркової впливу сучасних систем озброєння обумовило розширення просторових, скорочення часових показників вирішення завдань і гостру необхідність пошуку шляхів зменшення втрат особового складу і створення зразків (комплексів, систем) озброєння та військової техніки (ОВТ), що дозволяють уникнути безпосереднього контакту з противником [1]. Одним з таких шляхів є створення безпілотних систем, до яких відносяться наземні роботизовані комплекси (НРК).

Дослідження з розвитку НРК сьогодні активно проводяться в провідних країнах світу для потреб власних збройних сил [2 - 5]. Фахівці провідних країн вважають, що раціональне поєднання екіпажних та безпілотних систем зменшить втрати особового складу, розширить

можливості підрозділів і дозволить досягнути рівня ситуаційної обізнаності, якого неможливо досягнути існуючими екіпажними зразками ОВТ.

Але в Україні на десятий рік війни процес розвитку НРК не має системного характеру, підрозділи Сухопутних військ (СВ) не оснащуються НРК незважаючи на наявність пропозицій вітчизняних виробників. Серед багатьох існуючих проблем, що стримують розвиток і постачання НРК у війська, основними є:

1. Відсутність єдиних поглядів на місце і роль НРК в організаційно-штатній структурі підрозділів СВ України та способи їх бойового застосування. Сьогодні в Україні відсутні державні програми, концепції (чи стратегії) розвитку та застосування НРК.

2. Відсутність нормативного забезпечення розроблення НРК. Це відсутність національних стандартів, нормативно-технічних документів, які регламентують терміни та визначення, класифікацію НРК, показники оцінки їх технічного рівня, методи випробувань НРК і т.і.

3. Недостатня ефективність воєнно-наукових досліджень з визначення нагальної потреби в НРК. Відповідно до [6] нагальна потреба у зразках ОВТ – потреба в ОВТ, яка визначена командуванням виду, родом військ (сил) Збройних Сил України для термінового забезпечення (підтримання, нарощування) необхідного рівня боєздатності (виконання завдань за призначенням) Збройних Сил України в умовах правового режиму воєнного стану та не може бути покрита державними програмами розвитку, планами закупівель та ремонту у відповідний період. Але загальноприйнятого механізму реалізації цього процесу сьогодні не існує.

4. Недостатня ефективність механізму постачання НРК в умовах правового режиму воєнного стану, встановленого в [6]. Причинами цього є великі витрати часу на створення, організацію роботи комісій з перевірки достатності проведених розробником випробувань для підтвердження заявлених тактико-технічних характеристик (ТТХ), а також недостатня кількість фахівців, компетентних в питаннях розвитку НРК.

5. Нерозвиненість системи управління розвитком НРК. Причиною цього є низький рівень укомплектованості компетентними фахівцями новостворених структурних підрозділів органів управління, уповноважених в питаннях визначення пріоритетів розвитку НРК, планування заходів, спрямованих на розвиток НРК, взаємодії під час проведення досліджень і розробок з виробниками, науковими установами, закладами вищої освіти, організації підготовки фахівців з експлуатації НРК, координації, всебічного забезпечення розвитку НРК та контролю за виконанням завдань.

Серед перерахованих проблем, важливою є проблема недостатньої ефективності воєнно-наукових досліджень з визначення нагальної потреби в НРК. В роботі розглядається науково-методичний підхід щодо вирішення цієї проблеми.

Аналіз останніх досліджень та постановка задачі. В СВ, сьогодні, на жаль, існує суттєве протиріччя між виробниками (розробниками) НРК та споживачами НРК (Командуванням СВ, Командуванням Сил підтримки ЗС України, які одночасно є замовниками), що пов'язані з нерозумінням того, які ж НРК потрібні СВ [7]. Споживач, зазвичай, скептично відноситься до можливостей НРК ефективно вирішувати завдання в реальних бойових умовах, а вітчизняні виробники, які розробляють НРК, як правило, за своєю ініціативою, намагаються довести споживачу, що запропоновані ними зразки дозволять підвищити ефективність дій підрозділів СВ. У військах, навіть в бойових умовах [8], на виконання вимог [6] за ініціативою виробників відбувається випробування дослідних зразків НРК для подальшої підтримки проєктів у кластері Brave1 [9].

Але відповідно до пп. 2.5 [6] командування видів, родів військ (сил) Збройних Сил України визначають потребу у зразку НРК. Водночас сьогодні, на жаль, не існує загальноприйнятого науково-методичного підходу щодо визначення потреби в НРК.

Отже, **метою статті** є обґрунтування методики визначення потреби в НРК підрозділів СВ.

Виклад основного матеріалу. Під час визначення нагальної потреби в НРК необхідно враховувати такі аспекти:

1. По-перше, у найближчій перспективі НРК не замінять солдата та існуючі екіпажні зразки ОВТ, а доповнять їх для вирішення окремих завдань де існує дефіцит боєздатності (недостатня ефективність виконання завдань, великий ризик втрат особового складу) та необхідність розширення можливостей дій підрозділів.

2. По-друге, необхідно враховувати згадане вище протиріччя між виробниками (розробниками) НРК та споживачем НРК, яке пов'язане з нерозумінням того, які ж НРК потрібні СВ?

3. По-третє, під час визначення потреби необхідно обов'язково враховувати рівень розвитку технологій в області робототехніки та штучного інтелекту.

Сьогодні рівень розвитку технологій в області штучного інтелекту та робототехніки поки що не дозволяють створити НРК, які б були спроможні адекватно діяти, самостійно приймати рішення в бойових умовах. Це мова про бойові автономні НРК, розвиток яких сьогодні стримують проблемні питання пов'язані з навігацією, виявленням, розпізнаванням об'єктів в недетермінованих (бойових) умовах. Бойові НРК на відміну від НРК, що виконують завдання забезпечення (бойового, логістичного), можуть бути оснащені різноманітним озброєнням, але їх застосування, як дистанційно-керованих машин, за досвідом, як правило, обмежується завданнями охорони об'єктів та патрулювання. Підтвердженням цього є результати аналізу інформаційних джерел [10-11] та незадовільні результати бойового застосування російського бойового робототехнічного комплексу Уран-9 в Сирії [12].

4. По-четверте, варто усвідомлювати, що основний ефект від використання НРК полягає у зменшенні втрат особового складу, підвищенні рівня ситуаційної обізнаності, а також у меншій вартості у порівнянні з екіпажними машинами (менше витрат на вирішення завдань).

Враховуючи зазначені аспекти пропонується методика визначення потреби СВ в НРК.

Вона складається з двох етапів і полягає в наступному.

На першому етапі (рис. 1) визначається перелік завдань, для яких доцільно використовувати НРК.

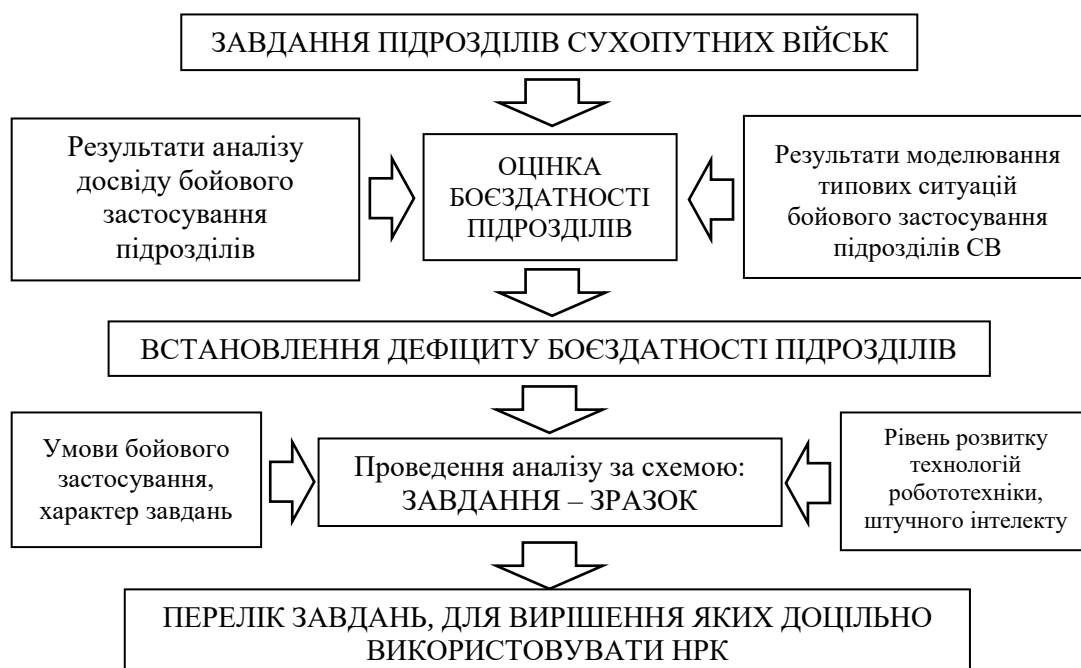


Рисунок 1 - Визначення переліку завдань для вирішення яких доцільно використовувати НРК

На підставі результатів досвіду бойового застосування підрозділів СВ та результатів моделювання типових ситуацій їх бойового застосування оцінюється боєздатність підрозділів.

За результатами проведеної оцінки встановлюється дефіцит боєздатності, під яким розуміється те, чого не вистачає для ефективного вирішення завдань підрозділами СВ. Наприклад, не вистачає засобів для підвезення боєприпасів, евакуації поранених.

На підставі результатів оцінки дефіциту боєздатності підрозділів СВ проводиться аналіз за схемою “ЗАВДАННЯ–ЗАСІБ”, який полягає у визначенні для кожного завдання, встановленого як дефіцит боєздатності, засобу, спроможного найбільш ефективно його виконати. Зазначений аналіз проводиться з урахуванням місця, характеру виконання завдань, а також досягнутого рівня розвитку технологій в галузі робототехніки.

За результатами такого аналізу визначається перелік завдань, для яких доцільно використовувати НРК.

З урахуванням досвіду бойового застосування підрозділів СВ в російсько-українській війні проведені дослідження за результатами яких визначено основні завдання, для вирішення яких доцільно використовувати НРК. Це:

1. Евакуація поранених з місця, де їх було поранено (“червоної зони”), до місць надання долікарської медичної допомоги.

2. Підвезення до ротного (взводного) опорного пункту боєприпасів, продовольства, іншого майна, необхідного для забезпечення ефективного ведення оборонних дій.

3. Перевезення боєприпасів, продовольства, особистого майна військовослужбовців, що діють у пішому порядку під час проведення наступальних, стабілізаційних дій (патрулювання).

4. Виконання окремих завдань інженерної розвідки противника і місцевості, подолання мінно-вибухових загороджень (МВЗ), влаштування інженерних загороджень, пошук та знищення вибухонебезпечних пристроїв (ВНП).

5. Ведення розвідки (приховане спостереження на загрозованих (небезпечних) напрямках) для підвищення ситуаційної обізнаності командирів підрозділів.

На другому етапі (рис. - 2) проводиться оцінка ефективності виконання завдань НРК.

Для визначеного переліку завдань проводиться вибір НРК серед існуючих (перспективних) зразків за результатами моделювання процесу застосування НРК.

Моделювання типових ситуацій застосування НРК пропонується проводити з використанням імітаційної системи JCATS (Joint Conflict and Tactical Simulation) – єдиної моделюючої системи тактичної обстановки та збройних конфліктів різної інтенсивності.

Зазначена імітаційна система дозволяє створювати імітаційні моделі типових ситуацій бойового застосування НРК з відомими ТТХ [13].

Адекватність імітаційної системи JCATS підтверджується успішним її використанням під час бойових дій в Югославії, Сомалі, Іраку [14] та позитивними результатами проведених перевірок, звіти про які наведені в [15 - 16]. Ця система широко використовується для моделювання бойових дій в 23 країнах, в тому числі країнах-членах НАТО.

З точки зору використання математичного апарату для формалізованого опису процесів ведення збройної боротьби імітаційна система JCATS представляє ієрархічну модель [15 - 17], яка наведена на рис. 3.

Критерієм ефективності виконання покладених на НРК завдань прийнято мінімальні втрати за умови забезпечення виконання завдань.

Якщо за результатами моделювання підтверджена достатня ефективність зразка НРК – обґрунтовуються пропозиції щодо потреби в НРК, які, відповідно до [6], подаються до командування СВ. В такий спосіб формується потреба підрозділів СВ в НРК. У випадку встановлення за результатами моделювання недостатньої ефективності виконання завдань проводиться корегування ТТХ НРК (або вибір іншого НРК серед існуючих зразків) і процес оцінки ефективності виконання завдань НРК повторюється.

Для побудови імітаційних моделей було обрано такі типові ситуації бойового застосування НРК:

1. Оборонний бій механізованого взводу у складі механізованої роти.

Завдання НРК: підвезення до взводного опорного пункту боєприпасів, евакуація поранених на зворотному шляху; ведення розвідки – приховане спостереження на загрозливих (небезпечних) напрямках.

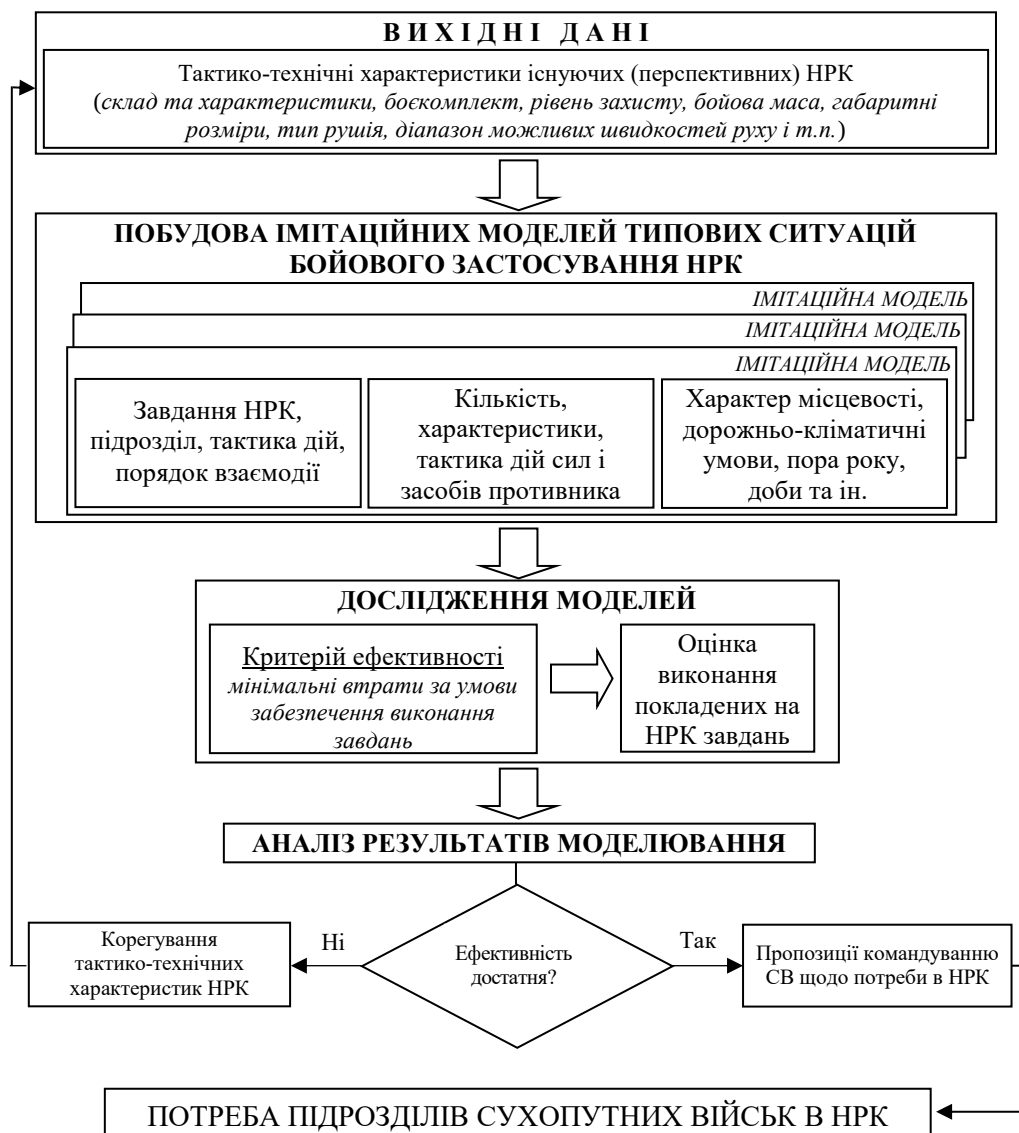


Рисунок 2 - Оцінка ефективності виконання завдань НРК

2. Наступальний бій механізованого взводу у складі механізованої роти. Завдання НРК – перевезення майна військовослужбовців, що діють у пішому порядку.

Серед існуючих зразків оцінка ефективності яких проводилась були НРК: “Sirko-S” (TOB Skylab), “БРП-3” (TOB “КБ Роботікс”), “Camel” (TOB “GlobalDynamics”), “ROBOTRACK” (ФОП “Панченко”), “Миротворець” (TOB “КВП СИНЕРГІЯ”).

За результатами моделювання визначено зразки, ефективність застосування яких відповідала прийнятому критерію. Найменування цих зразків не оприлюднюються, щоб це не було сприйнято, як зацікавленість в просуванні продукції цих компаній. Достовірність результатів, отриманих із застосуванням запропонованого науково-методичного апарату підтверджується результатами математичного моделювання, а також тим, отримані результати не суперечать відомим даним.

Враховуючи отримані результати для проведення подальших дослідницьких випробувань розробника в бойових умовах, пропозицією до створення експериментально-бойового підрозділу, передбаченого в [6] є введення до складу підрозділів забезпечення окремої механізованої (мотопіхотної) бригади окремої роти НРК, варіант організаційної структури якої наведено на рис. 4.

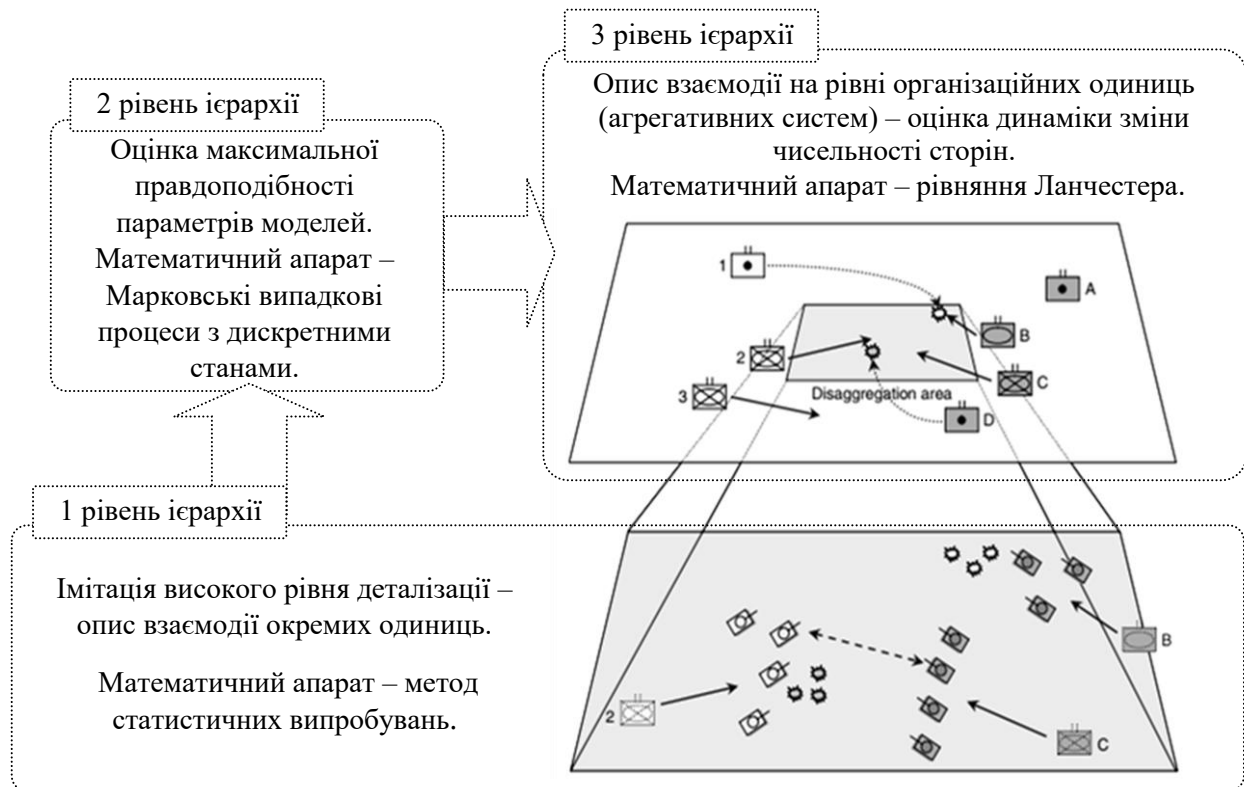


Рисунок 3 - Ієрархічна модель імітаційної системи JCATS

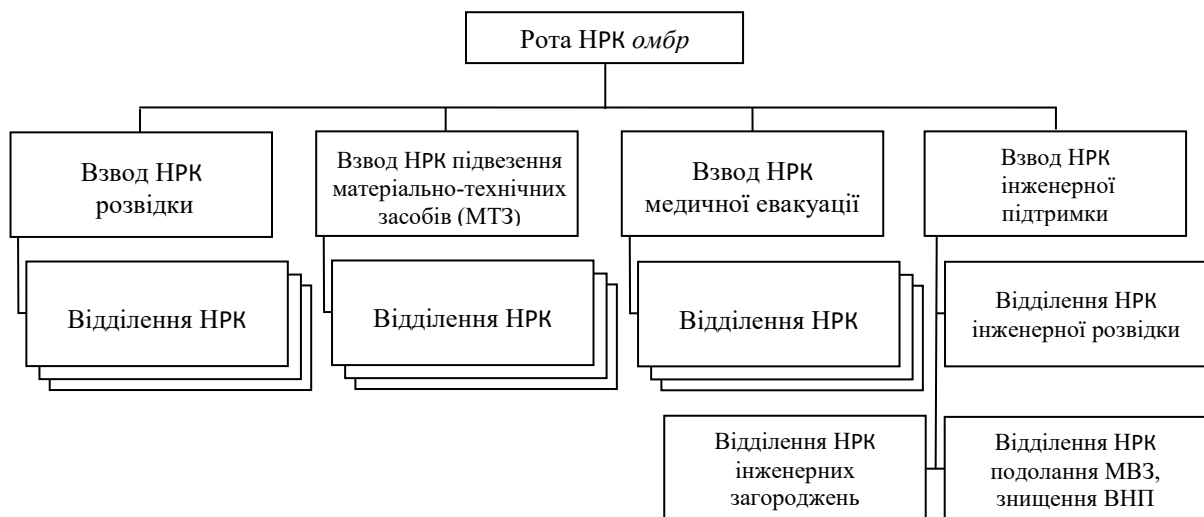


Рисунок 4 - Організаційна структура окремої роти НРК омбр (варіант)

Пропозиції щодо кількості НРК, особового складу та іншої техніки наведено в таблиці.

Висновки. В умовах суттєвого збільшення дальності, швидкості, точності та вибіркової впливу сучасних систем озброєння НРК поряд з іншими безпілотними системами сьогодні є пріоритетним шляхом зменшення втрат особового складу та

підвищення рівня ситуаційної обізнаності командирів підрозділів, якого неможливо (економічно недоцільно) досягнути існуючими екіпажними зразками ОБТ.

Таблиця

Кількість особового складу та військової техніки окремої роти НРК

Підрозділ	Особовий склад	Найменування військової техніки					
		Кількість зразків НРК				Вантажні автомобілі з причепом	Автомобіль HMMWV M1114
		Типи (типорозміри)* НРК					
		I	II	III	IV		
Управління	4						1
Взвод НРК розвідки	21	9 (3х3)				3	
Взвод НРК підвезення МТЗ	21	9 (3х3)				3	
Взвод НРК медичної евакуації	21	9 (3х3)				3	
Взвод НРК інженерної підтримки, в тому числі:	21						
- відділення НРК інженерної розвідки;	7		4			2	
- відділення НРК інженерних загороджень;	7			4		2	
- відділення НРК подолання МВЗ, знищення ВВП.	7				3	2	
Всього	88	27	4	4	3	15	1

* – тип (типорозмір) НРК - умовне позначення зразка НРК з притаманними йому ТТХ. Наприклад, НРК “Sirko-S”.

Враховуючи недостатню ефективність воєнно-наукових досліджень з визначення потреби в НРК, що проводяться в Україні, запропоновано науково-методичний апарат, який враховує досвід бойового застосування підрозділів СВ, умови, характер виконання завдань, рівень розвитку технологій з області робототехніки та дозволяє визначати перелік завдань, для яких доцільно використовувати НРК, та потребу підрозділів СВ. Запропонована методика може бути типовою для інших видів (родів військ) Збройних Сил України.

ЛІТЕРАТУРА:

1. Горбулін В. Як перемогти Росію у війні майбутнього. Київ: Брайт Букс. 2021. 248 с.
2. Unmanned Ground Vehicles (Defense) – Thematic Research. GlobalData, July 2023. URL: <https://www.globaldata.com/store/report/unmanned-ground-vehicles-theme-analysis/>. (дата звернення: 17.09.2023).
3. Unmanned Systems Integrated Roadmap FY 2017-2042. Office of the Under Secretary of Defense for Acquisition and Sustainment. URL: <https://apps.dtic.mil/sti/citations/AD1059546>. (дата звернення: 17.09.2023).
4. The U.S. Army Robotic and Autonomous Systems Strategy. U.S. Army Training and Doctrine Command, Fort Eustis, March 2017. 31 p. URL: <https://www.ndia.org/-/media/sites/ndia/meetings-and-events/divisions/robotics/4dvorakrd12815.pdf>. (дата звернення: 17.09.2023).
5. British Army unveils plans to make greater use of RAS in future. URL: <https://www.army-technology.com/news/british-army-plans-greater-use-ras-future/>. (дата звернення: 17.09.2023).
6. Тимчасовий порядок постачання озброєння, військової і спеціальної техніки та боєприпасів для потреб Збройних Сил України під час воєнного стану, затверджений Головнокомандувачем Збройних Сил України 1 лютого 2023 року. 7 с.
7. Роботизація, безпілотні авіакомплекси та бойова цифра: про інноваційні рішення для Збройних сил - від ключових гравців і без прикрас. URL: <https://defence->

ua.com/people_and_company/robotizatsija_bezpilotni_aviakompleksi_ta_bojova_tsifra_pro_inovatsijni_rishennja_dlja_zbrojnih_sil_vid_kljuchovih_gravtsiv_i_bez_prikas-4985.html. (дата звернення: 17.09.2023).

8. ЗСУ потрібно 10 000 роботів для боротьби з Росією: Міноборони налагоджує виробництво. URL: <https://focus.ua/uk/digital/582051-zsu-potribno-10-000-robotiv-dlya-borotbi-z-rosiyeyu-minoboroni-nalagodzhuje-virobnictvo>. (дата звернення: 17.09.2023).

9. Brave1 – кластер підтримки defense Tech розробок в Україні. URL: <https://brave1.gov.ua/>. (дата звернення: 17.09.2023).

10. U.S. Ground Forces Robotics and Autonomous Systems and Artificial Intelligence: Considerations for Congress. URL: <https://www.everycrsreport.com/reports/R45392.html#Content> (дата звернення: 17.09.2023).

11. Matejka, Jaroslav. "Robot As a Member of Combat Unit – An Utopia or Reality for Ground Forces?". *Advances in Military Technology*, 2020, Vol. 15, No. 1, pp. 7-24. URL: <https://aimt.cz/index.php/aimt/article/view/1332>. DOI: <https://doi.org/10.3849/aimt.01332>. (дата звернення: 17.09.2023).

12. Проблемы и вопросы применения военных робототехнических комплексов URL: <https://robocraft.ru/news/3825>. (дата звернення: 17.09.2023).

13. Engineering principles of combat modeling and distributed simulation / [Edited by Andreas Tolk]. Published by John Wiley & Sons, Inc., Hoboken, New Jersey, 2012. 906 p.

14. Shimamoto F. Simulating warfare is no video game. *Science&Technology Review*. 2000. January/February. P. 4-11.

15. Taylor James G., Beny Neta. Support of JCATS Limited Verification and Validation : report. California : Naval postgraduate school, September 2001. 51 p.

16. Christenson W.M., Catherine Mary, Walsh Terri J., Zirkle Robert A. JCATS Verification and Validation Report. Alexandria, Virginia : Institute for Defense Analyses, October 2002. 230 p.

17. Taylor J., Yildirim U., Murphy W. Hierarhy-of-Models Approach for Aggregated-Force Attrition / Proceeding of the 2000 Winter Simulation Conference. Orlando, 2000. P. 925-932.

REFERENCES:

1. Gorbulin, V. (2021), "Kak pobedit Rossiyu v vojne budushhego" [How to defeat Russia in the war of the future]: Brajt Buks, Kyiv, 248 p. [in Ukrainian].

2. Unmanned Ground Vehicles (Defense) – Thematic Research. GlobalData, July 2023. URL: <https://www.globaldata.com/store/report/unmanned-ground-vehicles-theme-analysis/>. (дата звернення: 17.09.2023).

3. Unmanned Systems Integrated Roadmap FY 2017-2042. Office of the Under Secretary of Defense for Acquisition and Sustainment. URL: <https://apps.dtic.mil/sti/citations/AD1059546>. (дата звернення: 17.09.2023).

4. The U.S. Army Robotic and Autonomous Systems Strategy. U.S. Army Training and Doctrine Command, Fort Eustis, March 2017. 31 p. URL: <https://www.ndia.org/-/media/sites/ndia/meetings-and-events/divisions/robotics/4dvorakrd12815.pdf>. (дата звернення: 17.09.2023).

5. British Army unveils plans to make greater use of RAS in future. URL: <https://www.army-technology.com/news/british-army-plans-greater-use-ras-future/>. (дата звернення: 17.09.2023).

6. "Tymchasovyy poriadok postachannya ozbroynennya, viys'kovoyi i spetsial'noyi tekhniky ta boyeprypasyv dlya potreb Zbroynykh Syl Ukrayiny pid chas voyennoho stanu, zatverdzhenny Holovnokomanduvachem Zbroynykh Syl Ukrayiny 1 lyutoho 2023 roku". [Temporary procedure for the supply of weapons, military and special equipment and ammunition for the needs of the Armed Forces of Ukraine during martial law, approved by the Commander-in-Chief of the Armed Forces of Ukraine] (2023). [in Ukrainian].

7. "Robotizatsija bezpilotni aviakompleksi ta bojova tsifra pro inovatsijni rishennja dlja zbrojnih sil vid kljuhovih gravtsiv I bez prikras" [Robotization, unmanned aerial vehicles, and combat numbers: innovative solutions for the Armed Forces from key players and without embellishment]. (2021) : https://defence-ua.com/people_and_company/robotizatsija_bezpilotni_aviakompleksi_ta_bojova_tsifra_pro_inovatsijni_rishennja_dlja_zbrojnih_sil_vid_kljuchovih_gravtsiv_i_bez_prikas-4985.html. [in Ukrainian].

8. "ZSU potribno 10000 robotiv dlya borotbi z rosiyeyu minoboroni nalagodzhuye virobnictvo" [Ukraine's Armed Forces need 10,000 robots to fight Russia: Defense Ministry sets up production]. (2023) : <https://focus.ua/uk/digital/582051-zsu-potribno-10-000-robotiv-dlya-borotbi-z-rosiyeyu-minoboroni-nalagodzhuye-virobnictvo>. [in Ukrainian].
9. Brave1 is a defense tech development support cluster in Ukraine URL: <https://brave1.gov.ua/>
10. U.S. Ground Forces Robotics and Autonomous Systems and Artificial Intelligence: Considerations for Congress. URL: <https://www.everycrsreport.com/reports/R45392.html#Content> (дата звернення: 17.09.2023).
11. Matejka, Jaroslav. "Robot As a Member of Combat Unit – An Utopia or Reality for Ground Forces?". *Advances in Military Technology*, 2020, Vol. 15, No. 1, pp. 7-24. URL: <https://aimt.cz/index.php/aimt/article/view/1332>. DOI: <https://doi.org/10.3849/aimt.01332>. (дата звернення: 17.09.2023).
12. Problems and issues in the application of military robotic systems URL: <https://robocraft.ru/news/3825>.
13. Engineering principles of combat modeling and distributed simulation / [Edited by Andreas Tolk]. Published by John Wiley & Sons, Inc., Hoboken, New Jersey, 2012. 906 p.
14. Shimamoto F. Simulating warfare is no video game. *Science&Technology Review*. 2000. January/February. P. 4-11.
15. Taylor James G., Beny Neta. Support of JCATS Limited Verification and Validation : report. California : Naval postgraduate school, September 2001. 51 p.
16. Christenson W.M., Catherine Mary, Walsh Terri J., Zirkle Robert A. JCATS Verification and Validation Report. Alexandria, Virginia : Institute for Defense Analyses, October 2002. 230 p.
17. Taylor J., Yildirim U., Murphy W. Hierarhy-of-Models Approach for Aggregated-Force Attrition / Proceeding of the 2000 Winter Simulation Conference. Orlando, 2000. P. 925-932.

D.Sci.Tech. Kuprinenko O., Ph.D. Nagachevskyi V., Ph.D. Kryvtsun V., Ph.D. Ftemov Y., Ph.D. Mishchenko Y., Zaverukha H.

METHODOLOGY FOR DETERMINING THE NEED FOR GROUND COMBAT VEHICLES OF THE ARMY UNITS

The paper presents the results of theoretical research on determining the need for ground combat vehicles of the Army units. The nature of modern armed struggle is analyzed. The necessity of finding ways to reduce personnel losses and the relevance of the development of ground combat vehicles are substantiated. A comparative analysis of the state of development of ground combat vehicles in the leading countries of the world and in Ukraine is carried out. Based on the results of the comparative analysis, the problematic issues that hinder the development and supply of ground combat vehicles for the needs of the Army are identified. One of the most important problematic issues is the insufficient effectiveness of military scientific research to determine the need for ground combat vehicles.

The factors that influence the process of determining the need for ground combat vehicles for the Army units are determined. The article proposes a scientific and methodological apparatus that takes into account the experience of combat use of the Army units, conditions, nature of tasks, the level of development of robotics technologies and allows determining the list of tasks for which it is advisable to use ground combat vehicles and the needs of the Army units.

Taking into account the experience of combat use of the Army units in the Russian-Ukrainian war, the main tasks for which it is advisable to use ground combat vehicles are identified. The expediency of using the JCATS simulation system for modeling typical situations of use of ground combat vehicles is substantiated. The criterion for the efficiency of performing the tasks assigned to ground combat vehicles is the minimum losses, provided that the tasks are completed.

Using the proposed scientific and methodological apparatus, samples were identified whose effectiveness met the adopted criterion. Taking into account the obtained results, proposals for the organizational structure of an experimental combat unit as part of a separate mechanized (motorized infantry) brigade are substantiated for further testing in combat conditions.

Keywords: ground combat vehicles, need, Army, modeling, simulation system JCATS.

к.т.н., доц. Маміч В. В. (ВА м. Одеса)
к.т.н., доц. Максименко Ю. А. (ВА м. Одеса)
Шаршаткін Д. Ю. (ВА м. Одеса)
Маляганов В. В. (ВА м. Одеса)
Кароль Д. А. (ВА м. Одеса)

DOI: <http://doi.org/10.17721/2519-481X/2023/80-05>

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ВІЙСЬК РОЗВІДУВАЛЬНОЮ ІНФОРМАЦІЄЮ

В даній роботі проаналізовані особливості забезпечення військ розвідувальною інформацією, відмічено, що для успішного ведення сучасного бою необхідно, насамперед, знати противника, його сили, засоби і характер дій. Для забезпечення цими даними командирів і штабів усіх ступенів існує вид бойового забезпечення дій військ – розвідка та її важливіша складова - розвідувально-інформаційна робота. Досвід ведення бойових дій свідчить, що тільки там, де розвідка ведеться активно і цілеспрямовано, бойові завдання вирішуються успішно і з найменшими втратами. Навпаки, погано організована розвідка завжди була головною причиною невдалого виконання бойових завдань. Сучасний бойовий досвід військ свідчить, що у теперішній час значно виріс обсяг завдань, які вирішує розвідка. Натомість, терміни їх виконання суттєво скоротилися. Підвищилися вимоги щодо часу передавання даних і точності визначення координат об'єктів противника. В роботі відмічено, що розвідувально-інформаційна робота включає в себе організацію, збір, обробку розвідувальних відомостей, своєчасну доповідь їх командирів, старшому начальнику і доведення необхідних даних до начальників родів військ і служб, командирів (штабів) підлеглих, взаємодіючих підрозділів і сусідів. Для прийняття рішення командирами підрозділів на ведення бойових дій їм потрібно мати розвідувальне донесення, де сформульовані висновки з оцінювання сучасного противника в реальному часі. Відмічено, що сьогодні саме організація розвідувально-інформаційної роботи стає найвагомішою складовою в розвідувальному забезпеченні підрозділів у сучасному бою, тому розвідники первинної ланки повинні мати високий рівень знань та навичок сучасної методики організації розвідувально-інформаційної роботи в підрозділах. Аналіз бойових дій на Сході України свідчить, що на успіх у бою впливає перш за все ступінь точності та достовірності інформації про противника, а також своєчасна доповідь про ймовірності прогнозованих його дій.

Ключові слова: розвідувальна інформація, сучасний бій, прогнозовані дії, методика, розвідники, координати, роди військ, досвід, достовірність, бойові дії.

Вступ. На теперішній час розвідка являє собою чи не найважливіший елемент державного функціонування, що дозволяє керівництву країни отримати інформацію найвищої цінності та обрати найбільш вдалий вектор подальших дій. Дивлячись на найпотужніших гравців світової арени сучасності, можна із впевненістю сказати, що потужна і авторитетна розвідка є сталим і незмінним атрибутом розвинених держав [1]. Не є винятком і країни європейського континенту, чиї розвідки мають коріння ще з часів Середньовіччя та на сьогодні мають доволі розгалужену структуру та різноманітний функціонал. Говорячи про країни, що стабільно посідають найвищі щаблі у світових рейтингах з економічного розвитку, з європейських держав на думку одразу спадає Німеччина, що є одним з безапеляційних лідерів у міжнародному політикумі. Проте, говорячи про причини такого небувалого розвитку, варто відзначити не лише такі фактори успіху, як освіту, дієві органи державної влади та згуртованість суспільства, а й надзвичайно ефективні розвідувальні органи, що виконують свої функції одразу на кількох невидимих фронтах. У Збройних силах, як відомо, органи розвідки відомості про противника добувають по крихтах, частинах, у різний час і в найрізноманітніших обставинах [2]. Нерідко інформація про один й той самий об'єкт, що добута різними органами розвідки або отримана з різних джерел одночасно, є суперечливою. Командирів ж завжди необхідно мати повну уяву про силу противника, його реальне положення, стан і наміри. Для цього необхідно всю інформацію, яка добута розвідкою й отримана від різних джерел (підлеглих командирів,

штабів, сусідів тощо), зібрати, вивчити, проаналізувати й узагальнити. Тільки на підставі всебічного аналізу всіх відомостей можна зробити обґрунтовані висновки про противника і забезпечити вірне прийняття рішення командиром на ведення бойових дій, які гарантують успіх у сучасному бою. Таким чином, для наукової організації розвідувально-інформаційної роботи в підрозділах необхідно: мати знання з фундаментальних основ інформаційної роботи та її складових; знання щодо організації інформаційної роботи в підрозділі; знання основ інформаційної роботи в загальновійськовому підрозділі; знання порядку і правил збору, обробки, аналізу розвідувальних відомостей та розробки звітних інформаційних документів із розвідки; знання методики з оцінювання противника [3].

Аналіз останніх досліджень. Аналіз публікацій в області організації розвідувально-інформаційної діяльності, методики оцінки противника у сучасному бою викладено у багатьох літературних джерелах [1 - 3]. Розкриття основ та особливостей забезпечення військ розвідувальною інформацією викладено у Військовому стандарті 01.101.001. Видання 2. Воєнна розвідка. Терміни та визначення. – К.: Міністерство оборони України. [8 - 9] Основні положення про організацію розвідувально-інформаційної роботи в підрозділах та військових частинах викладені у низки керівних документів, а саме у Бойовому статуті механізованих і танкових військ Сухопутних військ Збройних Сил України. Ч. II (батальйон, рота)/ затвердженого наказом командувача СВ ЗС України від 30.12. 2016 № 605. – 315 с.; Бойовому статуті механізованих і танкових військ Сухопутних військ Збройних Сил України. Ч. III (взвод, відділення, екіпаж)/ затвердженого наказом командувача СВ ЗС України від 25.05.2016 № 238. – 296 с.; Настанові з тактичної розвідки/ Командування СВ ЗС України. – Київ : МОУ, 2017. – 127 с. Все це дає можливість оволодіння фундаментальними основами забезпечення військ розвідувальною інформацією та дозволяє розвідникам первинної ланки оволодіти сучасною методикою збору, обробки та підготовки розвідувальної інформації для командирів та штабів [4 - 7].

Мета статті. Метою роботи є аналіз особливостей забезпечення військ розвідувальною інформацією для удосконалення порядку організації розвідувально-інформаційної роботи командирами військових частин і підрозділів в сучасному бою, проведення її у відповідності до вимог керівних документів. Тому, що на сьогоднішній день перемога у сучасному бою неможлива без правильної організації розвідки, особливо з використанням новітніх технологій, безпілотних літальних апаратів та інших технічних засобів розвідки. [4]

Виклад основного матеріалу. На думку військових фахівців, сутність інформаційної роботи полягає у опрацюванні та своєчасному наданні інформації про противника та місцевість командирам. Від правильної організації інформаційної роботи багато в чому залежить об'єктивність оцінювання противника і місцевості в районі майбутніх дій. Оперативно зібрана, оброблена і доведена інформація про противника та місцевість дозволяють командирові приймати правильні рішення та ефективно використовувати наявні сили та засоби. Інформаційний документ є кінцевим результатом інформаційної роботи, він містить проаналізовані та узагальнені дані щодо поставленого розвідувального завдання, викладені за визначений термін часу, в установлених обсязі та формі. Інформаційний документ у визначеній формі доводиться до споживача [5]. Споживач (розвідувальної інформації) – визначена законом, нормативно-правовим актом посадова особа, підрозділ, частина, установа, орган державного або військового управління, який використовує розвідувальну інформацію для прийняття управлінських рішень або виконання поставлених перед ним завдань в інтересах забезпечення національної безпеки держави. Іншими словами, інформаційна робота полягає у зборі, обробці розвідувальних відомостей та своєчасній доповіді їх командирові, старшому начальнику, а також доведенні необхідних даних до начальників родів військ і служб, командирів (штабів) підлеглих, взаємодіючих підрозділів і сусідів [6.] Основними принципами інформаційної роботи є: принцип конкретності, який означає, що інформаційна робота ведеться суто на основі розвідувальних завдань, які поставлені певним виконавцям, кожний інформаційний документ висвітлює конкретну тему; принцип реальності означає, що інформаційна робота будується відповідно до розумно вибраних напрямків, вони повністю забезпечені ресурсами, а цілі є досяжними; принцип

контрольованості означає, що хід обробки інформації, а значить і процес реалізації поставлених цілей інформаційної роботи, повинен постійно знаходитись у полі зору як керівників, так і безпосередньо виконавців на всіх етапах. Загальні вимоги до інформаційної роботи формуються на основі таких принципів як: цілеспрямованість інформаційної роботи, що полягає в першочерговому зборі, опрацюванні і доповіді (доведенні) тих розвідувальних відомостей, які в даній обстановці є найбільш важливими; активність інформаційної роботи, що полягає в наполегливому прагненні всіх посадових осіб у будь-якій обстановці зібрати необхідні розвідувальні відомості, обробити їх, доповісти командуванню (у вищий штаб), а також довести до всіх зацікавлених посадових осіб; об'єктивність інформаційної роботи, що полягає в ретельному і всебічному вивченні змісту всіх розвідувальних відомостей, а також обставин, джерел і часу їх добування, для того щоб виявити правильне положення, стан і характер дій противника [7].

Органи розвідки добувають необхідну команду інформацію про противника, яка повинна пройти певну обробку та перевірку до моменту прийняття рішення командиром на ведення бойових дій. Розвідувальним підрозділам досить рідко вдається одержати повні відомості про склад противника, його засоби масового ураження, елементи високоточної зброї, замисли застосування засобів ураження, морально-психологічний стан його особового складу, боєздатність його підрозділів (військових частин, з'єднань) тощо. Таким чином, на даному етапі циклу інформаційної роботи від органу розвідки до командира підрозділу надходять розвідувальні матеріали [8]. Розвідувальні матеріали – необроблені, але документально зафіксовані первинні результати добування розвідувальної інформації, що містять розвідувальні ознаки, як правило, в неявному вигляді і тому не можуть бути використані без первинної обробки. Розвідувальна ознака – характеристика (параметр) об'єкта розвідки, яку (який) можна визначити (виміряти) і використовувати для розпізнавання об'єкта розвідки, визначення його стану, характеру діяльності, а також прогнозування напрямку розвитку подій (явищ). Їх прийнято ділити на розпізнавальні й тактичні. Розпізнавальні ознаки це тип, призначення об'єкта розвідки його належність. Тактичні ознаки це зовнішній вигляд, конструктивні особливості, кольори, форма об'єктів розвідки. Розвідники повинні добре знати і швидко розрізняти саме розпізнавальні ознаки. Особливістю якісної організації розвідувально-інформаційної роботи є безпомилкове визначення тактичних розвідувальних ознак противника, таких як бойовий склад, організація, тактика дій і намір противника все це використовується командирами при аналізі розвідувальних відомостей. При цьому слід мати на увазі, що противник буде прагнути маскуванню, дезінформацією, оманними діями приховати дійсне положення своїх об'єктів (цілей), свою діяльність і наміри. Тільки наявність декількох ознак дає можливість зробити правильний висновок про об'єкт розвідки і дозволить командирам прийняти правильне рішення на ведення сучасного бою. До об'єктів розвідки належать: війська у районах розташування (зосередження, під час пересування, на вихідних, стартових, вогневих позиціях); аеродроми, військово-морські та військово-повітряні бази, військові кораблі; пункти управління, вузли зв'язку; радіотехнічні системи виявлення, наведення та управління зброєю; органи тилу; вузли шляхів, мости та гідротехнічні споруди, трубопроводи; підприємства, які пов'язані з виробництвом військової продукції [9]. Об'єкти розвідки класифікуються так: за роллю у збройній боротьбі; за ступенем впливу на хід бойових дій; за структурою і кількістю елементів; за характером виявлення; за належністю; за характером розташування; за розміром; за ступенем рухомості. Розвідувальна інформація до командирів доходить у формі усної доповіді, донесення по радіо, письмово або графічного матеріалу, за допомогою всіх можливих засобів зв'язку, головне щоб вона була повною, вірною і своєчасною, за допомогою якої можна визначити склад об'єкта розвідки, його стан, місце знаходження та характеристики його діяльності. Джерелом розвідки прийнято називати особовий склад військ противника і його дії, що можуть спостерігатися нашими органами розвідки, а також полонені, перебіжчики, захоплені документи; працюючі радіоелектронні засоби; предмети озброєння і бойової техніки противника, осколки снарядів, бомб та ракет; райони, заражені радіоактивними й отруйними речовинами, а також органи розвідки,

підлеглі, взаємодіючі і сусідні командири підрозділів (штаби) і вищий штаб, від яких інформація про противника надходить командирові (до штабу) підрозділу, а також місцеві жителі й особовий склад своїх військ, що знаходився на території противника, бачив його своїми очима або чув про нього [10, 14]. За ступенем надійності джерело розвідувальної інформації прийнято поділяти як: надійне; достатньо надійне; сумнівне; ненадійне; з невизначеною надійністю. Надійне джерело розвідувальної інформації – перевірене джерело, яке неодноразово використовувалось, а інформація, яка від нього надходила, за ступенем достовірності була не нижче, ніж достовірною. Достатньо надійне джерело розвідувальної інформації – перевірене джерело, яке неодноразово використовувалось, а інформація, яка від нього надходила, за ступенем достовірності була не нижче, ніж ймовірна. Сумнівне джерело розвідувальної інформації – джерело, яке використовувалось раніше, але інформація, яка від нього надходила, за ступенем достовірності була сумнівною, а інколи й недостовірною. Ненадійне джерело розвідувальної інформації – джерело, інформація від якого в значній кількості випадків за ступенем достовірності була недостовірною або містила дезінформацію. Джерело розвідувальної інформації з невизначеною надійністю – джерело, яке раніше не використовувалось і надійність якого не може бути визначена до перевірки інформації, що від нього надійшла. Розвідувальна інформація складається з розвідувальних відомостей та розвідувальних даних [11, 15]. Для перетворення розвідувальної інформації в розвідувальні відомості проводиться первинна обробка цієї інформації, перевірка на відповідність визначеним вимогам та придатність для подальшого використання. Для перетворення розвідувальних відомостей у розвідувальні дані вони підлягають додатковій обробці обов'язково старшим командиром, з подальшим додатковим аналізом у вищому штабі.

Висновки та напрямки подальших досліджень. Таким чином, в результаті аналізу організації розвідувально-інформаційної роботи підрозділів у сучасному бою при веденні повномасштабної війни Росії в Україні і збройних конфліктів сучасності, встановлено, що одним із ключових моментів в обробці розвідувальних відомостей (матеріалів) є їх аналіз. В інформаційній роботі під аналізом (грец. analysis – розкладання, розчленування, розбір) розуміється метод дослідження, сутність якого полягає в тому, що досліджуваний предмет подумки або практично розчленовується на елементи, кожний із яких потім досліджується окремо як частина цього цілого. Призначення аналізу полягає в тому, щоб відокремити суттєве від несуттєвого, звести складне до більш простого [12]. За результатами проведеного аналізу розвідувальні відомості перетворюються в розвідувальні дані та класифікуються: за достовірністю, важливістю, терміновістю, повнотою та за ступенем достовірності. Вони поділяються на достовірні, ймовірні, сумнівні і недостовірні. Отже, задача всіх офіцерів, що обробляють (узагальнюють) розвідувальні відомості, полягає в тім, щоб шляхом вивчення, аналізу і зіставлення окремих, розрізнених, неповних, нерідко суперечливих даних (фактів) робити обґрунтовані висновки, що розкривають реальну картину сучасної обстановки, з визначенням змісту проведених противником заходів і його замислу [13]. Оброблені розвідувальні відомості з висновками (прийнятими інформаційними рішеннями) щодо даного питання чи об'єкта та оформлені певним документом прийнято використовувати командирами для прийняття рішення на ведення сучасного бою. Для підвищення ефективності в організації розвідувально-інформаційної роботи підрозділів необхідно виключити прояви суб'єктивізму, ігнорування уривчастих або навіть самих незначних розвідувальних відомостей, що може призвести до прорахунків під час оцінювання противника, звести нанівець успішну діяльність розвідувальних підрозділів (органів) й ускладнити виконання бойового завдання. Таким чином, розвідувально-інформаційна робота в тактичній розвідці – це діяльність органів розвідки щодо забезпечення посадових осіб даними, які необхідні для вирішення покладених на них завдань. Збір, обробка, використання та доведення інформації про противника є невід'ємним елементом успішного ведення сучасного бою.

ЛІТЕРАТУРА:

1. Війна в Україні: розвідка Британії розкрила ключовий у найближчий час фактор. <https://www.unian.ua/war/viyna-rosiji-proti-ukrajini>
2. Тактика в бойових прикладах навч.-метод. посіб./колектив авторів; за заг. ред. А. М. Сиротенка. – К. : НУОУ ім. І. Черняхівського, 2017. – 140 с.
3. "Ситуація бентежна": у ГУР назвали єдиний безпечний варіант для росіян в Криму. Анжеліка Байбак 17:29, 27 вересня 2023 р. https://24tv.ua/chornomorskiy-flot-sevastopoli-vibuhi-rozvidtsi-dali-poradu-rosiyanam_n2400724.
4. Левченко О. В. Методика оцінки противника у бою : навчальний посібник/ О. В. Левченко. – К. : НАОУ, 2021. – 76 с.
5. Війна Росії проти України. 27.09.2023 р. <https://www.dw.com/uk/viina-rosii-proty-ukrainy/t-608993214>.
6. Тактична розвідка в бойових прикладах за досвідом проведення АТО: посібник. – Київ : МОУ ГУР, 2017. – 160 с.
7. Війна Росії з України з Україною. Матеріали по темі. https://lb.ua/tag/13406_viyna_z_rosiieyu
8. Методичні рекомендації з розробки розвідувальних оцінок (за стандартами провідних країн-членів НАТО). – К. : ГУР МО України, 2018. – 118 с.
9. Варенко В. М. Інформаційно-аналітична діяльність : навчальний посібник. – К. : Університет "Україна", 2014. – 417 с.
10. Процеси розвідувальної діяльності. Стандарт НАТО. Союзницька об'єднана настанова АJP–2.1 (видання В, варіант 1)/ Управління стандартизації НАТО, 2016. – 80 с.
11. Російське вторгнення в Україну (з 2022). <https://uk.wikipedia.org/wiki>
12. Бойовий статут механізованих і танкових військ Сухопутних військ Збройних Сил України. Ч. II (батальйон, рота)/ затверджений наказом командувача СВ ЗС України від 30.12. 2016 № 605. – 315 с.
13. Бойовий статут механізованих і танкових військ Сухопутних військ Збройних Сил України. Ч. III (взвод, відділення, екіпаж)/ затверджений наказом командувача СВ ЗС України від 25.05.2016 № 238. – 296 с.
14. Настанова з тактичної розвідки/ Командування СВ ЗС України. – Київ : МОУ, 2017. – 127 с.
15. Левченко О.В., Віннік В.В., Устименко О.В. Розвідка та іноземні армії. Навчальний посібник. – Житомир, ЖВІ, 2019.- 126 с.
16. Військовий стандарт 01.101.004. Видання 2. Воєнна розвідка. Розвідувально-інформаційна діяльність. Терміни та визначення. – К. : Міністерство оборони України, 2015. – 26 с.

REFERENCES:

1. The war in Ukraine: British intelligence revealed a key factor in the near future. <https://www.unian.ua/war/viyna-rosiji-proti-ukrajini>
2. Tactics in combat examples of training methods. manual/team of authors; in general ed. A. M. Syrotenko. – K.: NUOU named after I. Chernyakhovsky, 2017. – 140 p.
3. "The situation is embarrassing": the GUR named the only safe option for Russians in Crimea. Anzhelika Baibak 17:29, September 27, 2023 https://24tv.ua/chornomorskiy-flot-sevastopoli-vibuhi-rozvidtsi-dali-poradu-rosiyanam_n2400724
4. O. V. Levchenko. Techniques for assessing the enemy in battle: study guide/ O. V. Levchenko. - K.: NAOU, 2021. - 76 p.
5. Russia's war against Ukraine. 09/27/2023 <https://www.dw.com/uk/viina-rosii-proty-ukrainy/t-608993214>.
6. Tactical reconnaissance in combat examples based on the experience of ATO: manual – Kyiv: MOU HUR, 2017. – 160 p.
7. Russia's war with Ukraine against Ukraine. Materials on the topic. https://lb.ua/tag/13406_viyna_z_rosiieyu
8. Methodological recommendations for the development of intelligence assessments (according to the standards of leading NATO member countries). - K.: GUR Ministry of Defense of Ukraine, 2018. - 118 p.
9. Varenko V. M. Information and analytical activity: study guide. - K.: "Ukraine" University, 2014. - 417 p.
10. Intelligence activity processes. NATO standard. Allied Joint Instruction AJP–2.1 (edition B, version 1)/ NATO Standardization Office, 2016. – 80 p.

11. Russian invasion of Ukraine (from 2022). <https://uk.wikipedia.org/wiki>
12. Combat statute of the mechanized and tank troops of the Ground Forces of the Armed Forces of Ukraine. Part II (battalion, company)/ approved by the order of the Commander of the Armed Forces of Ukraine dated 30.12. 2016 No. 605. – 315 p.
13. Combat statute of the mechanized and tank troops of the Ground Forces of the Armed Forces of Ukraine. Part III (platoon, detachment, crew)/ approved by the order of the Commander of the Armed Forces of Ukraine dated 05.25.2016 No. 238. – 296 p.
14. Instruction on tactical intelligence/ Command of the Defense Forces of Ukraine. - Kyiv: MOU, 2017. - 127 p.
15. Levchenko O.V., Vinnik V.V., Ustymenko O.V. Intelligence and foreign armies. Tutorial. - Zhytomyr, ZVI, 2019. - 126 p.

Ph.D. Mamich V.V. Ph.D. Maksimenko Yu.A., Sharshatkin D.Y., Malyaganov V.V., Karol D. A.

FEATURES OF PROVIDING TROOPS WITH INTELLIGENCE INFORMATION

This paper analyzes the features of providing troops with intelligence information, it is noted that for the successful conduct of a modern battle, it is necessary, first of all, to know the enemy, his forces, means and nature of actions. In order to provide commanders and staffs of all levels with this data, there is a type of combat support for military actions - intelligence and its most important component - intelligence and information work. The experience of conducting military operations shows that only where reconnaissance is conducted actively and purposefully, combat tasks are solved successfully and with the least losses. On the contrary, poorly organized intelligence has always been the main reason for the failure of combat missions. The modern combat experience of the troops shows that nowadays the volume of tasks solved by intelligence has grown significantly. On the other hand, the terms of their implementation have significantly shortened. The requirements for the time of data transmission and the accuracy of determining the coordinates of enemy objects have increased. It is noted in the work that intelligence and information work includes the organization, collection, processing of intelligence information, timely reporting to the commander, senior commander, and delivery of the necessary data to the heads of military branches and services, commanders (staffs) of subordinate, interacting units and neighbors. In order for unit commanders to make a decision on the conduct of hostilities, they need to have an intelligence report, which formulates conclusions based on the assessment of the modern enemy in real time. It was noted that today it is the organization of intelligence and information work that is becoming the most important component in the intelligence support of units in a modern battle, therefore primary-level scouts must have a high level of knowledge and skills of modern methods of organization of intelligence and information work in units. The analysis of hostilities in the East of Ukraine shows that success in battle is primarily influenced by the degree of accuracy and reliability of information about the enemy, as well as a timely report on the probabilities of his predicted actions.

Key words: *intelligence information, modern combat, predicted actions, technique, scouts, coordinates, types of troops, experience, reliability, combat operations.*

Стаття не містить відомостей, що розкривають державну таємницю та службову інформацію. Автори надають дозвіл на перевірку праці відповідальними особами, призначеними для перевірки праць на оригінальність і відсутність неправомірних запозичень. Автори гарантують, що ними одержано всі необхідні дозволи на використання у цій статті матеріалів, що охороняються авторським правом. Автори гарантують, що ця стаття раніше не публікувалась і не подавалась до інших видань”.

МЕТОД АНТИКРИЗОВОГО УПРАВЛІННЯ В СИСТЕМІ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ЩОДО ПОСЛАБЛЕННЯ ВПЛИВУ НЕГАТИВНИХ ТЕНДЕНЦІЙ БЕЗПЕКОВОГО СЕРЕДОВИЩА НА ПРОЦЕСИ РЕАЛІЗАЦІЇ НАЦІОНАЛЬНИХ ІНТЕРЕСІВ ДЕРЖАВИ

У XXI столітті збройні конфлікти та війни все частіше ведуться в “сірій зоні”, тобто поза межами міжнародного права, як у фізичному просторі, так і в інших вимірах – інформаційному, кібернетичному, культурному, когнітивному, переважно гібридними способами, із залученням іррегулярних формувань (приватних військових компаній, повстанців, терористів і т. ін.). Як наслідок – сьогоденніс міждержавне протистояння стає все більш складним, охоплює різні сфери національної безпеки, характеризується широким діапазоном негативних для населення держави наслідків.

Пріоритетними завданнями правоохоронних, спеціальних, розвідувальних та інших державних органів сектору безпеки і оборони України відповідно до їх компетенції визначено активну та ефективну протидію розвідувально-підривній діяльності, спеціальним інформаційним операціям та кібератакам, ворожій пропаганді, протидію зовнішнім загрозам національній безпеці України, сприяння реалізації національних інтересів тощо.

Сталий розвиток держави потребує своєчасного кількісно-якісного оцінювання негативних тенденцій розвитку (загроз) з метою недопущення кризових ситуацій у забезпеченні національної безпеки.

Запропонований метод дозволяє розробляти концептуальні підходи до обґрунтування відповідних антикризових стратегій і програм, а також рекомендації щодо критеріїв оцінювання ефективності усунення (нейтралізації) негативних тенденцій розвитку геополітичної та воєнно-політичної обстановки (загроз) в умовах обмеженості ресурсів.

В основу методу закладається обґрунтування критичних значень ризиків реалізації деструктивних факторів в окремих сферах національної безпеки, на основі порівняння яких з оціненими поточними ризиками, розробляються антикризові заходи для визначених сфер національної безпеки стосовно кожної виявленої негативної тенденції. Метод передбачає організацію системного моніторингу ефективності антикризового управління з визначенням критеріїв для прийняття рішень щодо порядку виконання антикризових заходів.

Ключові слова: національна безпека, антикризове управління, негативна тенденція, загроза, ризик, пороговий рівень ризику, безпекове середовище.

Вступ і постановка завдання. Стаття присвячена проблемі підвищення ефективності антикризового управління у системі забезпечення національної безпеки (СЗНБ) держави в умовах застосування (виявлення) комбінованих загроз. Успішне розв’язання цієї проблеми потребує кількісно-якісного оцінювання негативних тенденцій (НТ) розвитку з метою недопущення кризових ситуацій у забезпеченні національної безпеки держави [1]. Для цього пропонується вирішити низку наукових та практичних завдань, зокрема обґрунтувати критичні значення ризиків реалізації деструктивних факторів у визначених сферах національної безпеки, провести оцінювання поточних ризиків та на основі їх порівняння розробити антикризові заходи для кожної сфери національної безпеки стосовно виявлених НТ, а також визначити критерії для прийняття рішень щодо порядку виконання таких заходів.

Аналіз останніх досліджень і публікацій. У монографіях [2 – 5] автори розглядають гібридну війну як інтеграцію різних реальних і віртуальних загроз (військових, дипломатичних, економічних, інформаційних тощо) з метою негативного впливу на державу-жертву (мішень), занурення її в ситуацію невизначеності, послаблень та руйнування без оголошення війни, а також на створення навколо відповідного інформаційного поля, яке має сформувати у світової спільноти такий образ цієї держави, який виправдовував би будь-які

недружні, навіть агресивні дії на її адресу. Однак, питання оцінювання та аналізу НТ розвитку геополітичної та воєнно-політичної обстановки авторами не розглянуті.

У монографії [6] розглянуто методологічний апарат організації комплексної, зокрема асиметричної протидії загрозам воєнного характеру з боку сильнішого у військовому відношенні противника. Антикризове управління розглянуте лише як необхідність порушення цього питання.

У публікаціях [7, 8] наводиться загальна характеристика гібридних загроз, аналізується їх вплив на забезпечення національної безпеки, однак методичні підходи до оцінювання їх впливу на визначальні сфери національної безпеки (НБ) не розглядаються.

У статті [9] розглянуто комплексний підхід до формування стратегії вирішення проблем розвитку соціально-економічних об'єктів на основі структуризації знань про їх розвиток у вигляді когнітивних карт. Він є інструментальним комплексом підтримки діяльності щодо розв'язання проблем управління. Загрози об'єктам у статті детально не розглядаються.

У статті [10] з теоретичного погляду розглянуто когнітивний підхід в моделюванні та управлінні. Виділено клас управлінських задач, для вирішення яких доцільне когнітивне моделювання. Детально розглянута когнітивна модель соціально-економічного розвитку окремого регіону, однак загрози розвитку регіону не розглянуті.

У зазначених та інших публікаціях, з якими могли ознайомитися автори, не наводиться методичний апарат оцінювання рівня гібридних загроз та їх деструктивного впливу на визначальні сфери НБ, а також їхнього впливу на ризики забезпечення НБ держави.

Формулювання мети статті. Метою статті є розроблення методу антикризового управління у СЗНБ щодо послаблення впливу НТ безпекового середовища на процеси реалізації національних інтересів (НІ) держави.

Виклад основного матеріалу дослідження. Стратегія національної безпеки України визначає людину, її життя і здоров'я, честь і гідність, недоторканність і безпеку найвищою соціальною цінністю в Україні. Реалізація цієї норми Конституції України – головна ціль державної політики національної безпеки [1].

Державний суверенітет, територіальна цілісність, демократичний конституційний лад та інші фундаментальні НІ мають реалізовуватися в умовах наявності загроз як воєнного, так і невоєнного характеру з боку недружніх держав. Найбільш небезпечними загрозами є спроби порушити соціально-політичну стабільність та сталий розвиток держави, спровокувати громадянську війну, внутрішні конфлікти, здійснити державний переворот тощо.

Пріоритетними завданнями правоохоронних, спеціальних розвідувальних та інших державних органів сектору безпеки і оборони України (СБОУ) відповідно до їх компетенції визначено активну та ефективну протидію розвідувально-підбивній діяльності, спеціальним інформаційним операціям та кібератакам, ворожій пропаганді, протидію зовнішнім загрозам НБ України, сприяння реалізації НІ України тощо. Звісно, що для запобігання й реагування на ці деструктивні явища та загрози в умовах обмеженості ресурсів потрібна чітка координація та взаємодія органів СБОУ, інших державних органів, територіальних громад, бізнесу, громадянського суспільства і населення, для чого необхідно розробити науково обґрунтовані відповідні антикризові стратегії, програми та рекомендації [2]. Однак в Стратегії національної безпеки України не розглянуті концептуальні підходи до їх обґрунтування, критерії ефективності усунення (нейтралізації) деструктивних явищ (загроз) в умовах обмеженості ресурсів, фактори, що спричиняють ризики забезпечення НБ у її пріоритетних сферах і, що вкрай важливо, їх порогові значення (рівні). Тому авторами статті запропоновано метод антикризового управління у СЗНБ щодо послаблення впливу НТ на процеси реалізації НІ держави (далі метод).

Суть методу полягає в обґрунтуванні критичних значень (порогових рівнів) ризиків реалізації деструктивних факторів в окремих сферах національної безпеки, оцінюванні поточних ризиків та розроблення на основі їх порівняння антикризових заходів для кожної сфери національної безпеки, а також визначення критеріїв для прийняття рішень щодо

порядку виконання антикризових заходів. Залежно від результату виконання розроблених заходів щодо послаблення впливу негативних тенденцій може бути прийнято одне з таких рішень: продовжувати виконання заходів без змін, провести коригування заходів або, якщо усунуті (послаблені) фактори негативного впливу, закінчити їх виконання.

Метод передбачає організацію системного моніторингу виконання заходів антикризового управління з можливістю постійного оцінювання поточного рівня виявлених ризиків.

Узагальнена блок-схема методу, який передбачає одинадцять основних етапів, наведена на рис. 1.

На *першому етапі* здійснюється моніторинг безпекового середовища з метою виявлення НТ розвитку геополітичної та воєнно-політичної обстановки в регіонах, які впливають на НІ держави.

Слід зазначити, що проблемні питання у сфері національної безпеки досліджують державні науково-дослідні установи та низка навчальних закладів, незалежні громадські організації держави, вітчизняні та закордонні фахівці з питань оборони, але дефініція безпекового середовища на цей час у нормативно-правових документах не визначена.

У цій публікації під *безпековим середовищем* будемо розглядати геополітичну, політико-дипломатичну, воєнну, економічну, інформаційну та інші сфери, де зароджуються, існують, накопичуються або проявляються сприятливі або небезпечні явища, негативні тенденції розвитку, потенційні та реальні загрози реалізації національних інтересів, та у яких держава реалізує політику національної безпеки, взаємодіє з міжнародними структурами безпеки, стратегічними партнерами, союзниками, військово-політичними та іншими інститутами й організаціями в інтересах забезпечення свого сталого розвитку на певному часовому інтервалі [3].

В ході моніторингу безпекового середовища для кожної сфери НБ з урахуванням виявлених НТ розробляються найбільш небажані сценарії та визначаються фактори, які їх провокують.

На *другому етапі* проводиться експертна фільтрація НТ (T_s) по сферах НБ (S) та їх паспортизація. Паспортизація дає можливість фіксувати у часі та просторі виявлену НТ (T_s), її основні ознаки, характер, масштаб, джерело, спрямування, можливі наслідки, можливі деструктивні прояви в інших сферах тощо. Більш детально паспорт загрози розглянуто в [4]. Бажаною умовою є те, щоб кількість таких НТ не перевищувала дев'яти у кожній сфері.

На *третьому етапі* за технологією експертного оцінювання, наведеною в [2], визначаються пріоритети ("важливості") кожної i -ї ($i=1, I$) НТ (T_{si}) у кожній s -й ($s=1, S$) сфері НБ.

На *четвертому етапі* шляхом експертного опитування для кожної i -ї ($i=1, I$) НТ (T_{si}) здійснюється формування пріоритетного ряду факторів ризику F_{sik} ($k=1, K$), що посилюють НТ (T_{si}) розвитку геополітичної та воєнно-політичної обстановки на визначену перспективу. При цьому важливо враховувати вплив як прямих, так і опосередкованих факторів ризику [8].

Визначення пріоритетів НТ та факторів ризику здійснюється методом ранжирування за 9-бальною шкалою, де 9-й ранг відповідає найбільшому впливу, а 1-й ранг – найменшому. Для цього доцільно залучати 7-9 експертів – фахівців у сфері, що розглядається.

Враховуючи тенденцію до ускладнення загроз, появи так званих гібридних загроз, труднощі їх виявлення, оцінювання та прогнозування їх рівня і руйнівного потенціалу, припускаємо, що на стратегічному рівні державного управління є достатня кількість підготовлених експертів (аналітиків) для оцінювання деструктивного впливу факторів ризику на посилення негативних тенденцій у визначених сферах НБ.

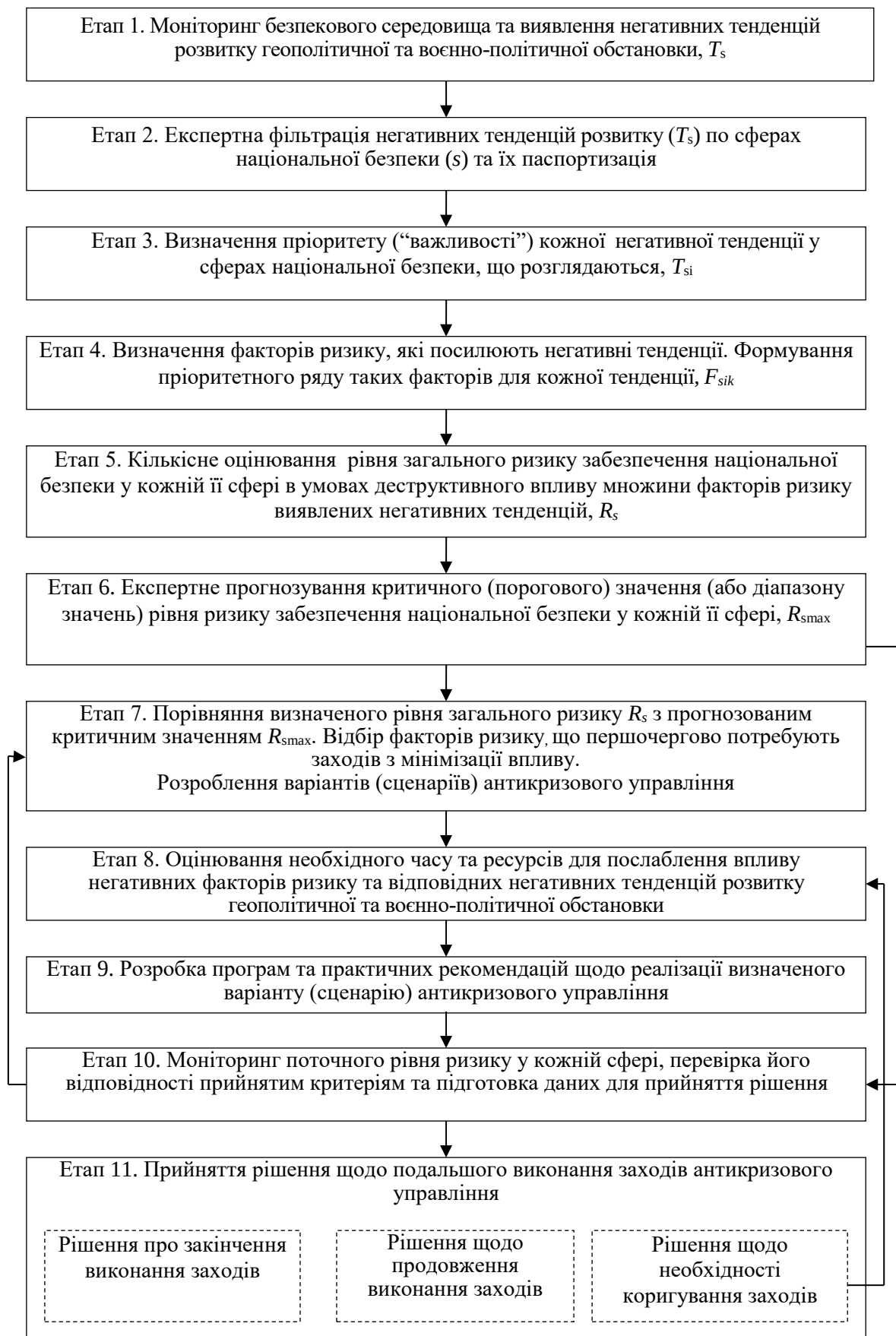


Рисунок 1 – Узагальнена блок-схема методу антикризового управління у СЗНБ щодо послаблення впливу НТ безпекового середовища на процеси реалізації НІ у визначених сферах НБ

програма спеціального призначення "Модель ситуаційного управління ризиком М7", яка дозволяє визначити числове значення загального ризику забезпечення НБ як інтегрального показника впливу негативних факторів ризику на кожну сферу НБ, що розглядається [11, 12].

На шостому етапі проводиться аналіз результатів, отриманих на попередньому етапі. Аналіз пропонується проводити на підставі орієнтовної шкали оцінювання впливу негативних факторів ризику (табл. 1).

Таблиця 1

Орієнтовна шкала оцінювання впливу негативних факторів ризику на s -ту сферу ($s=1, S$) НБ

Інтервал оцінок (критичне значення рівня ризику, R_{smax})	0 – 0,24 (R_{smax1})	0,25 – 0,49 (R_{smax2})	0,5 – 0,74 (R_{smax3})	0,75 – 1,0 (R_{smax4})
Характеристика впливу	Незнач ний вплив	Помірний вплив	Значний вплив	Дуже значний вплив

Також на цьому етапі здійснюється експертне прогнозування критичного (порогового) значення (або діапазону значень) рівня ризику R_{smax} , за якого, на думку експертів, у СЗНБ може виникати кризовий стан, що утруднить (або навіть унеможливить) стає функціонування системи та, відповідно, сталий розвиток держави (реалізацію НІ) [9], [10], і що потребуватиме впровадження антикризових заходів.

Як варіант, пропонується встановлення критичних значень рівня ризику R_{smax4} та R_{smax3} , що можуть бути використані в якості показників зниження впливу з дуже значного на значний та із значного на помірний відповідно (табл. 1).

Такий підхід дозволяє конкретизувати мету антикризового управління, оцінювати його поточні результати та приймати відповідні рішення з урахуванням можливого ресурсного забезпечення.

На сьомому етапі здійснюється порівняння визначеного рівня загального ризику R_s з прогнозованим критичним значенням (або діапазоном значень) рівня ризику R_{smax} забезпечення НБ у кожній s -й сфері. У разі виявлення необхідності послаблення впливу НТ T_{si} на процеси забезпечення НБ розробляються варіанти (сценарії) антикризового управління, проводиться відбір факторів ризику F_{sik} , що потребують першочергового нетривіального впливу [6].

На восьмому етапі проводиться експертне оцінювання часу та ресурсів, що потрібні для розробки і впровадження заходів з мінімізації впливу негативних факторів ризику F_{sik} та відповідних НТ T_{si} з урахуванням прогнозних змін геополітичної та воєнно-політичної обстановки на визначену перспективу. Графічне пояснення процедури експертного оцінювання потрібного часу наведено на рис. 2.

На дев'ятому етапі розробляються програми та практичні рекомендації щодо реалізації визначеного варіанту (сценарію) антикризового управління.

На десятому етапі здійснюється моніторинг виконання заходів антикризового управління у заданому проміжку часу t з визначенням поточного рівня ризику R_{spot} у кожній s -й сфері ($s=1, S$), перевіряється його відповідність прийнятим критеріям (R_{smax}) та готуються рекомендації для оцінювання результатів антикризового управління та прийняття відповідного рішення.

На одинадцятому етапі, залежно від результату виконання розроблених заходів, спрямованих на послаблення впливу НТ, приймається рішення щодо подальшого виконання заходів антикризового управління, а саме:

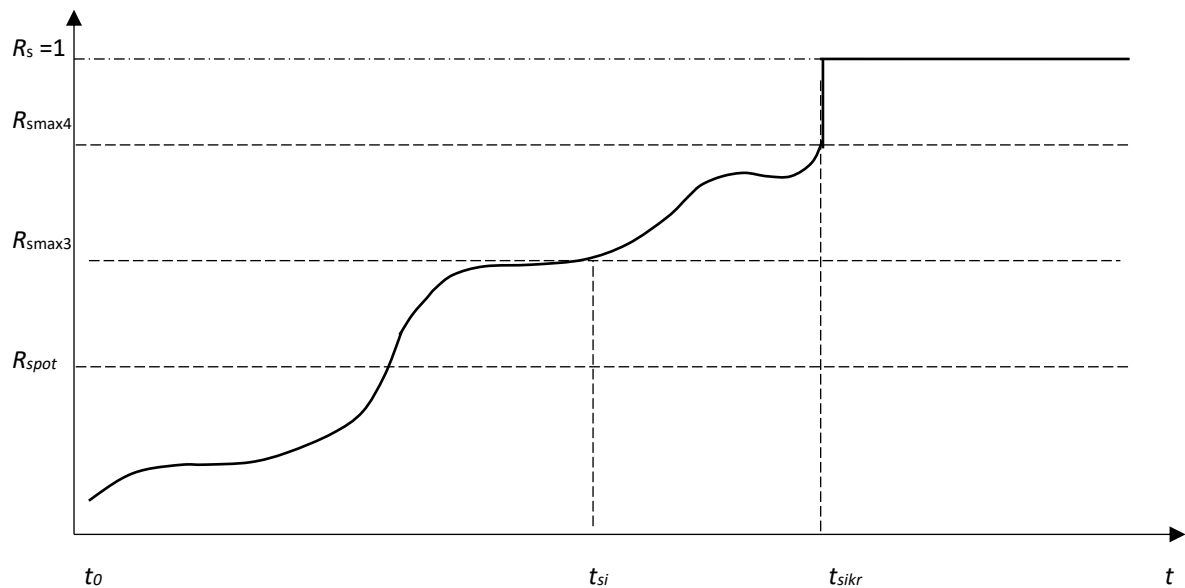


Рисунок 2 – Процедура експертного оцінювання часу, потрібного для нейтралізації впливу множини негативних факторів ризику i -ї НТ у s -й сфері:

R_{smax4} – криза у забезпеченні НБ у s -й сфері (рівень ризику, при якому вводиться в СЗНБ антикризове управління);

R_{smax3} – рівень ризику, при якому здійснюється прогнозування динаміки поточного рівня ризику i -ї НТ у s -й сфері;

R_{spot} – поточний рівень ризику i -ї НТ у s -й сфері;

t_0 – час виявлення i -ї НТ у s -й сфері;

якщо $R_{smax3} < R_{spot} < R_{smax4}$, то приймається рішення на продовження виконання заходів антикризового управління;

якщо $R_{spot} \geq R_{smax4}$, то приймається рішення на коригування таких заходів (уточнюються час та/або ресурси, необхідні для мінімізації впливу негативних факторів ризику та відповідних негативних тенденцій розвитку).

Висновки. Запропонований метод антикризового управління в системі забезпечення НБ щодо послаблення впливу НТ на процеси реалізації НІ держави дає змогу підвищити ефективність антикризового управління в умовах застосування проти неї комбінованих загроз шляхом кількісно-якісного оцінювання ризиків НТ розвитку (загроз) та попереджати кризові ситуації у забезпеченні НБ держави.

Метод забезпечує визначення критичних значень ризиків реалізації деструктивних факторів в окремих сферах НБ, на основі порівняння яких з оціненими поточними ризиками розробляються антикризові заходи (програми та рекомендації) для кожної сфери НБ стосовно послаблення впливу виявлених в процесі моніторингу безпекового середовища НТ на принципах комплексності, системної узгодженості між собою для мирного та воєнного часу, ресурсозабезпеченості на достатньому рівні, професіоналізму аналітиків, надійного кіберзахисту та незалежної експертизи на вищому державному рівні.

Розроблений метод передбачає підвищення ефективності антикризового управління на підставі прийняття обґрунтованих рішень щодо порядку виконання антикризових заходів.

У подальших публікаціях авторами планується розробити прикладну методiku антикризового управління.

ЛІТЕРАТУРА:

1. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року “Про Стратегію воєнної безпеки України”: Указ Президента України від 25.03.2021 року № 121/2021. URL: <http://www.president.gov.ua/documents/1212021-37661> (дата звернення: 10.08.2023).
2. Богданович В. Ю., Свида І. Ю., Скулиш Є. Д. Теоретико-методологічні основи забезпечення національної безпеки України. Монографія. У 7 т. Т. 1. Теоретичні основи, методи й технології забезпечення національної безпеки України. За заг. ред. Є. Д. Скулиша. Київ: Наук.-вид. відділ НА СБ України, 2012. 548 с.
3. Богданович В. Ю., Свида І. Ю., Романченко І. С., Сиротенко А. М., Дублян О. В. Методологія комплексного використання військових і невійськових сил та засобів сектору безпеки і оборони для протидії сучасним загрозам воєнній безпеці України. Моногр. Вид. 2-ге, розшир. та доповн. Київ. НУОУ. 2021. 364 с.
4. Богданович В. Ю., Свида І. Ю., Скулиш Є. Д. Теоретико-методологічні основи забезпечення національної безпеки України. Монографія. У 7 т. Т. 4. Воєнна безпека держави і шляхи її забезпечення. За заг. ред. Є. Д. Скулиша. Київ. Наук.-вид. відділ НА СБ України. 2012. 464 с.
5. Арзуманян Р. Кромка Хаоса. Сложное мышление и сеть: парадигма нелинейности и среда безопасности XXI века. Москва: Изд. дом “Регнум”. 2012. 600 с.
6. Семенченко А. І. Стратегічне планування у сфері державного управління забезпеченням національної безпеки. Монографія. Київ. НАДУ при Президентові України. 2007. 260 с.
7. Висідалко А. Л., Богданович В. Ю. Аналіз можливостей системи забезпечення національної безпеки України щодо всебічної підтримки безпекового супроводу реалізації національних інтересів. Наука і техніка Повітряних сил ЗС України. Наук.-тех. журнал. Харків: ХНУПС. 2013. № 3 (12). С. 5–12.
8. Приміренко В. М., Грицай М. П. Способи ведення гібридної війни та роль збройної боротьби у ній. Труды ун-ту. Зб. наук. пр. НУО України. Київ. 2016. № 5 (138). С. 104–109.
9. Горбулін В. П., Качинський А. Б. Стратегічне планування: вирішення проблем національної безпеки. Монографія. Київ. НІСД. 2010. 288 с.
10. Висідалко А. Л., Богданович В. Ю. Забезпечення безпеки інформаційних процесів безпекового супроводу реалізації національних інтересів. Сучасний захист інформації. Київ. ДУТ. 2013. № 3. С. 60–66.
11. Богданович В. Ю. Воєнна безпека України: методологія дослідження та шляхи забезпечення. Київ. 2003. С. 291–297.
12. Саати Т. Принятие решений при зависимостях и обратных связях: Аналитические сети. Москва: Издательство ЛКИ. 2008. 360 с.

REFERENCES:

1. Pro rishennja Rady natsionalnoyi bezpeky i oborony Ukrainy vid 25.03.2021 “Pro Strategiyu voyennoyi bezpeky Ukrainy”: Ukaz Prezidenta Ukrainy vid 25.03.2021 № 121/2021. URL: <http://www.president.gov.ua/documents/1212021-37661>.
2. Bogdanovych, V.Yu., Svyda, I. Yu. and Skulysh, Ye.D. Teoretyko-metodologichni osnovy zabezpechennya natsionalnoyi bezpeky Ukrainy. Monograf. T. 1. // Za zag. red. Ye.D. Skullysha. K.: Nauk.-vyd. viddil NA SB Ukrainy. 2012. 548 p.
3. Bogdanovych, V.Yu., Svyda, I.Yu., Romanchenko, I.S., Syrotenko, A.M. and Dublyan, O. V. Metodologiya kompleksnogo vykorystannya viyskovykh i neviyskovykh syl ta zasobiv sectoru bezpeky i oborony dlya protydyi suchasnym zagrozam voyenniy bezpetsi Ukrainy. Monograf. Vyd. 2-ge. K.: NUOU. 2021. 364 p.
4. Bogdanovych, V.Yu., Svyda, I. Yu. and Skulysh, Ye.D. Teoretyko-metodologichni osnovy zabezpechennya natsionalnoyi bezpeky Ukrainy. Monograf. T. 4. // Za zag. red. Ye.D. Skullysha. K.: Nauk.-vyd. viddil NA SB Ukrainy. 2012. 464 p.
5. Arzumyan, R. Kromka Haosa. Slozhnoje myshlenije i set: paradigma nelinejnosti i sreda bezopasnosti XXI veka. M.: Izd. dom “Regnum”. 2012. 600 p.
6. Semenchenko, A.I. Strategichne planuvannja u sferi derzhavnogo upravlinnja zabezpechennjam natsionalnoyi bezpeky. Monograf. K.: NADU pry Prezidentovi Ukrainy. 2007. 260 p.
7. Vysidalko, A.L and Bogdanovych, V.Yu. Analiz mozhlyvostey systemy zabezpechennya natsionalnoyi bezpeky Ukrainy schodo vsebichnoyi pidtrymky bezpekovoogo suprovodu realizatsiyii

natsionalnyx interesiv. Nauka i texnika Povitryanyx Syl ZS Ukrainy. Nauk.-tex. zhurnal. X.:XNUPS. 2013. № 3 (12). P. 5–12.

8. Prymirenko, V.M. and Gritsay, M.P. Sposoby vedennya gibrydnoyi viyny ta rol zbroynoyi borotby u niy. Trudy un-tuТруды ун-ту. Zb. nauk. pr. NUO Ukrainy. K. 2016. № 5 (138). P. 104–109.

9. Gorbunin, V.P. and Kachinskiy, A.B. Strategichne planuvannya: vyrishennya problem natsionalnoyi bezpeky. Monograf. K.: NISD. 2010. 288 p.

10. Vysidalko, A.L. and Bogdanovych, V.Yu. Zabezpechennya bezpeky informatsiynykh protsesiv bezpekovogo suprovodu realizatsiyi natsionalnyx interesiv. Suchasnyy zaxyst informatsiy. K.: DUT. 2013. № 3. P. 60–66.

11. Bogdanovych, V.Yu. Voyenna bezpeka Ukrainy: metodologiya doslidzhennya ta shlyaxy zabezpechennya. K. 2003. P. 291–297.

12. Saati, T. Prinyatiye resheniy pri zavisimostyax i obratnyx svyazyax: Analiticheskiye seti. M.: Izdatelstvo LKI. 2008. 360 p.

Ph.D. Muzhenko V.M., Ph.D. Tsybizov A.L., Ph.D. Pekuliak R.O.

METHOD OF ANTI-CRISIS MANAGEMENT IN THE NATIONAL SECURITY SUPPORT SYSTEM CONCERNING IMPACT REDUCING OF THE SAFE ENVIRONMENT NEGATIVE TRENDS ON THE STATE NATIONAL INTERESTS REALIZATION PROCESSES

In the 21st century, armed conflicts and wars are increasingly being waged in the "Gray zone", that is, outside the boundaries of international law, both in physical space and in other dimensions – informational, cybernetic, cultural, cognitive – mainly by hybrid methods with involvement of irregular formations (private military companies, rebels, terrorists, etc.). As a result, today's interstate confrontation is becoming more and more complex, covering various spheres of national security, characterized by a wide range of negative consequences for the population of the state.

The priority tasks of the law enforcement, special, intelligence and other state bodies of the security and defence sector of Ukraine in accordance with their competence are defined as active and effective countering intelligence and subversive activities, special information operations and cyber-attacks, enemy propaganda, countering external threats to the national security of Ukraine, promoting implementation of national interests, etc.

Sustainable development of the state requires timely a quantitative and qualitative assessment of negative development trends (threats) in order to prevent crisis situations in ensuring the national security of the state.

The proposed method allows for the development of conceptual approaches to the justification of appropriate anti-crisis strategies and programs, as well as recommendations for evaluating the effectiveness of the elimination (neutralization) of negative trends in the development of the geopolitical and military-political situation (threats) in conditions of limited resources.

The basis of the method is the justification of the critical values of the risks of the implementation of destructive factors in certain areas of national security, based on a comparison of which with the assessed current risks, anti-crisis measures are developed: strategies, programs and recommendations for each area of national security in relation to each negative trend identified in the process of monitoring the security environment. The method provides the organization of: systematic monitoring of the effectiveness of anti-crisis management with the definition of criteria for making decisions on the order of anti-crisis measures carrying out.

Key words: national security, anti-crisis management, negative trend, threat, risk, threshold level of risk, security environment.

МОДЕЛЮВАННЯ РОЗПОДІЛЕНОГО НЕЛІНІЙНО-ОПТИЧНОГО ПІДСИЛЕННЯ У ТЕЛЕКОМУНІКАЦІЙНИХ ВОЛОКНАХ TRUEWAVE^{RS} ТА G.652

Загальноприйняті методики моделювання нелінійно-оптичного підсилювача, а саме на основі ефекту вимушеного комбінаційного розсіяння (ВКР), що в англomовній літературі має назву Raman effect, незважаючи на простоту його технічної реалізації, є доволі ускладненими і громіздкими через необхідністю теоретичного описання нелінійної взаємодії багатьох світлових хвиль накачки та сигналів за допомогою відповідних систем диференціальних рівнянь високого порядку. Принципові обмеження таких методик полягають не тільки у кількості рівнянь, а й у наявності особливих точок у кожному рівнянні динаміки хвиль сигналів (такі точки відповідають пороговим значенням потужності помпування). За цих умов нестійкість розв'язків диференціальних рівнянь та їхня неоднозначність мають іноді руйнівний вплив на результати моделювання. Альтернативна методика моделювання з використанням наближення заданої накачки потребує окремих досліджень своєї практичної застосовності до аналізу динаміки розподіленого оптичного підсилення в телекомунікаційних волокнах.

Тому має місце задача визначення критерію застосовності наближення заданої накачки для розробки спрощеної моделі нелінійного оптичного підсилення сигналів в умовах їхнього розповсюдження вздовж стандартних кварцових волокон. Серед незаперечних переваг аналітичних розв'язків, які отримано на основі спрощеної моделі, є усунення зазначених обмежень методики розв'язку систем багатьох диференціальних рівнянь

Стаття присвячена моделюванню динаміки розподіленого оптичного підсилення на основі ефекту вимушеного комбінаційного розсіяння (ВКР) залежно від довжини стандартного одномодового волокна (ОМВ) та потужності помпування. В обґрунтуванні методики моделювання, яка пропонується, показано відповідність параметрів активних волокон та схем підсилювачів на основі ефекту вимушеного комбінаційного розсіяння (далі за текстом – ВКР підсилювачів) критерію застосовності наближення заданої накачки.

У роботі наведено аналітичний вираз критерію застосовності наближення заданої накачки у вигляді верхньої межі потужності сигналу, який не може перевищувати підсилений сигнал. Представлені результати порівняльного аналізу параметрів розподіленого ВКР підсилення залежно від довжини таких активних волокон як G.652 та TrueWave^{RS}.

Ключові слова: ВКР підсилювач, підсилення оптичних сигналів, потужність накачки, потужність помпування, телекомунікаційні системи

Вступ. Застосування високих технологій, серед яких виділяються пристрої нелінійної фотоніки – оптичні підсилювачі та лазери, що побудовані на основі ефекту вимушеного комбінаційного розсіяння [1 - 5], забезпечує рекордні швидкості інформаційного обміну [6 - 8] в оптоволоконних телекомунікаційних системах. Широке застосування ВКР фотоніки в сучасних телекомунікаціях обумовлене простотою технічної реалізації пристроїв нелінійного підсилення світла [2 - 4] і лежить в основі єдиної технології, що здатна до освоєння повного вікна прозорості кварцового волокна із шириною смуги ~60 ТГц [3-5,9]. Однак, згідно із останньою редакцією стандарту ITU-T G.652 [10], у цьому документі ще відсутні дані про нелінійні властивості транспортних телекомунікаційних волокон, оскільки вони залишаються предметом інтенсивних світових досліджень, що саме по собі є свідченням актуальності вивчення фізичних принципів та фундаментальних особливостей розробки фотонних пристроїв. Зокрема, проблема оптимізації ефективності та робочої смуги ВКР підсилювачів, зважаючи на досить значний потік наукових публікацій [11 - 22] в останні два десятиліття, з одного боку зустрічає фундаментальні ускладнення в процесі свого

вирішення, а з іншого – вказує на важливість цього етапу моделювання для модернізації існуючих телекомунікаційних систем до сучасних і перспективних потреб.

З метою моделювання параметрів волоконних ВКР підсилювачів раніше [25 - 29] була розроблена і апробована методика аналітичної апроксимації профілів ВКР підсилення складного континуального типу. Проте дослідження динаміки розподіленого комбінаційного підсилення залишається недостатньо вивченою навіть у типових телекомунікаційних волокнах [30 - 31]. У роботі, що пропонується, досліджено основні характеристики ВКР підсилення у волокні типу TrueWave^{RS} порівняно з такими ж характеристиками ВКР підсилення у стандартному кварцовому волокні G.652 і надано результати моделювання.

Постановка задачі. Провести моделювання динаміки розподіленого ВКР підсилення в залежності від довжини активного волокна ми проводимо за допомогою спрощеної моделі та з використанням реальних параметрів стандартних ОМВ.

Розглянемо багатоканальну оптоволоконну систему з розділенням за довжинами хвилі, модернізацію якої здійснено за допомогою розподілених ВКР підсилювачів. На рис. 1 зображено узагальнену схему такої системи.

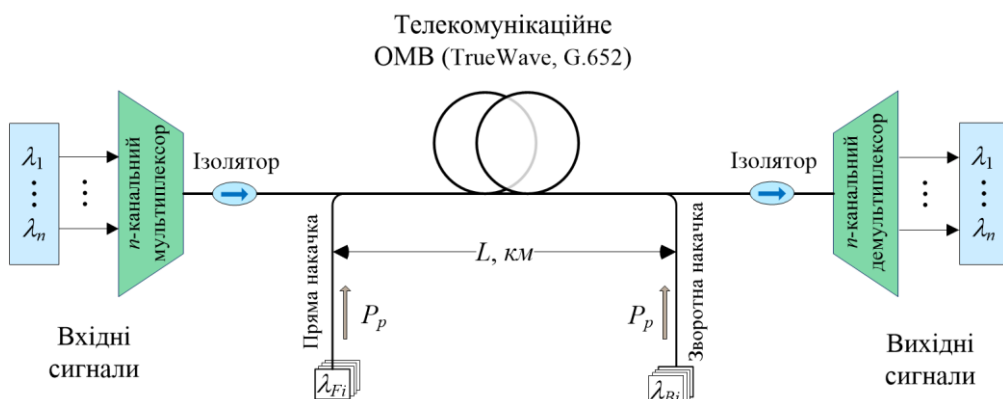


Рисунок 1 - Узагальнена схема багатоканальної оптоволоконної системи з розділенням за довжинами хвилі, в якій застосовуються розподілені ВКР підсилювачі із двосторонньою накачкою.

З технічної точки зору розподілене ВКР підсилення (див. рис.1) реалізується за допомогою простого введення до волокна випромінювання накачки середньої потужності ($0,1 \div 1 \text{ Вт}$) у прямому та/або зустрічному напрямку до сигнала, причому ефект можливий у будь-якому волокні. ВКР підсилювач, особливо в разі застосування двосторонньої накачки, радикально збільшує відстань L між ретрансляторами, а мультихвильове джерело помпування дозволяє розширити смугу підсилення аж до 13 ТГц, причому у будь-якій частині повного вікна прозорості телекомунікаційного волокна. Однак, незважаючи на граничну простоту практичної реалізації ВКР підсилювачів за схемою на рис.1, моделювання динамічних параметрів підсилювачів залишається актуальною задачею, що вкрай ускладнюється необхідністю теоретичного описання фундаментальних процесів нелінійної взаємодії багатьох хвиль як накачки, так і сигналів.

Спрощення узагальненої схеми, що представлена на рис.1, полягає у розгляді одноканальної системи, в якій груповий цифровий сигнал із часовим ущільненням передається через одномодове волокно на відстань $L, [\text{км}^{-1}]$ з використанням однієї несучої оптичної частоти ω_s , що знаходиться у вікні прозорості волокон на основі кварцового скла (С-вікно, $\lambda_s = 1,55 \text{ мкм}$). Для ВКР підсилення такого сигналу у процесі його розповсюдження вздовж одномодового кварцового волокна досить використати монохроматичне джерело помпування на довжині хвилі $\lambda_p = 1,425 \text{ мкм}$. За таких умов кількісний аналіз динаміки розподіленого ВКР підсилення залежно від довжини оптичного волокна можна проводити за допомогою системи двох диференціальних рівнянь для нелінійної ВКР взаємодії двох хвиль – стоксової хвилі (на частоті корисного сигналу ω_s) та хвилі накачки ω_p .

Метою статті є розробка критерію застосовності спрощеної моделі нелінійного оптичного підсилення для стандартних волокон на основі кварцового скла, моделювання динаміки та порівняльний аналіз параметрів розподіленого ВКР підсилення залежно від довжини таких активних волокон.

Зазначимо, що активним середовищем для моделювання розподіленого ВКР підсилювача вибрано стандартні ОМВ, які досить давно були розроблені і вже тривалий час використовуються як дуже прозорий носій оптичних сигналів (ОМВ із «чистого» кварцового скла стандарту G.652) та потім вдосконалювали системи дальнього зв'язку шляхом одночасного зменшення шкідливого впливу дисперсії на швидкісні параметри систем інформаційного обміну (кварцове ОМВ типу TrueWave^{RS}).

Незабаром з'ясувалось, що для будь-якого ОМВ нелінійний коефіцієнт ВКР підсилення g_R , $[(Вт \cdot км)^{-1}]$ відмінний від нуля, однак він має досить складну залежність від частоти стоксового зсуву Ω і в цьому випадку функція $g_R = g_R(\Omega)$ отримала назву *профілю ВКР підсилення*. Реальні профілі ВКР підсилення всіх кварцових волокон, незважаючи на досить значимі відмінності для різних типів волокна, забезпечують на практиці можливість спільного використання таких волокон не тільки для передачі оптичних імпульсів на великі відстані, а й для одночасного їх підсилення для компенсації неминучих втрат потужності світлових сигналів.

На рис.2 представлено профілі ВКР підсилення $g_R(\Omega)$ в абсолютних одиницях, $[(Вт \cdot км)^{-1}]$ для обох типів ОМВ, що були прийняті для моделювання. На осі абсцис подано незалежну змінну - частоту стоксового зсуву Ω , яка для зручності представлена як у спектроскопічних одиницях, $[см^{-1}]$ на нижній осі, так і в $[ТГц]$ – на верхній осі.

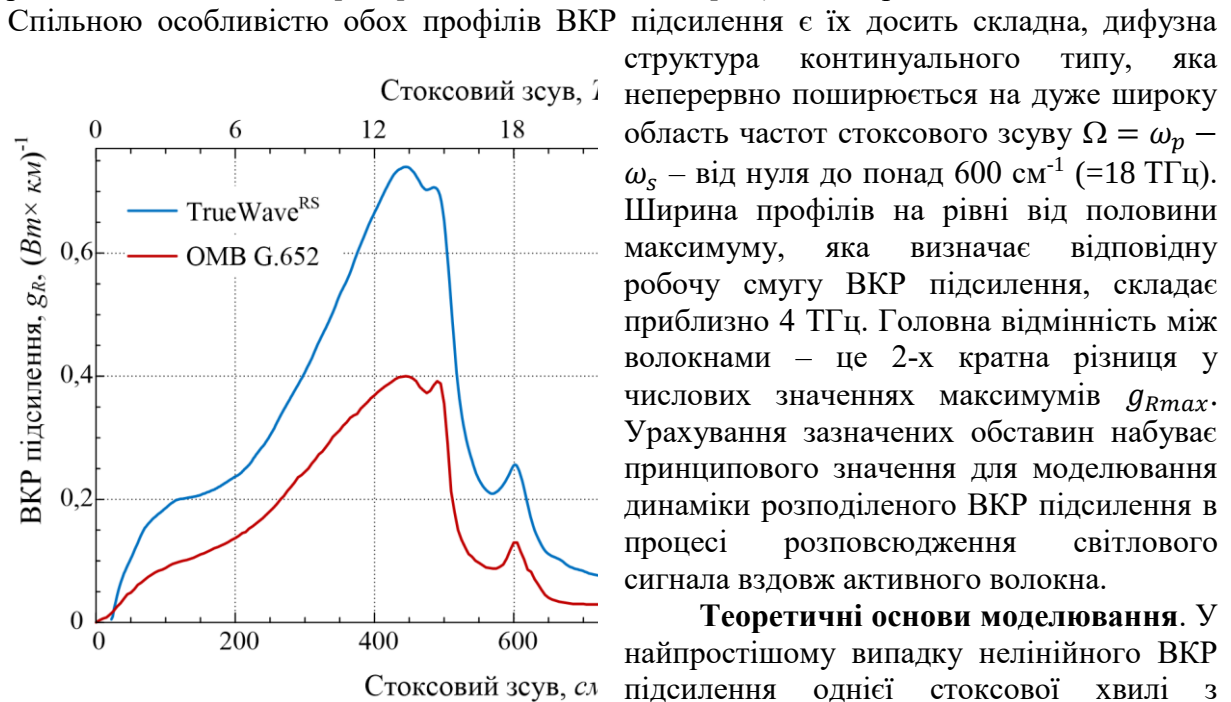


Рисунок - 2 Профілі ВКР підсилення двох стандартних одномодових волокон на основі кварцового скла

Спільною особливістю обох профілів ВКР підсилення є їх досить складна, дифузна структура континуального типу, яка неперервно поширюється на дуже широку область частот стоксового зсуву $\Omega = \omega_p - \omega_s$ – від нуля до понад 600 см^{-1} ($=18 \text{ ТГц}$). Ширина профілів на рівні від половини максимуму, яка визначає відповідну робочу смугу ВКР підсилення, складає приблизно 4 ТГц. Головна відмінність між волокнами – це 2-х кратна різниця у числових значеннях максимумів g_{Rmax} . Урахування зазначених обставин набуває принципового значення для моделювання динаміки розподіленого ВКР підсилення в процесі розповсюдження світлового сигналу вздовж активного волокна.

Теоретичні основи моделювання. У найпростішому випадку нелінійного ВКР підсилення однієї стоксової хвилі з потужністю P_s за рахунок високої інтенсивної хвилі накачування з потужністю P_p динаміка зміни обох потужностей у процесі їх спільного

розповсюдження в одному напрямку, а саме вздовж z – координати ($z \in [0, L]$) оптичного волокна, описується системою зв'язаних диференціальних рівнянь [32]:

$$\begin{cases} \frac{dP_s}{dz} = g_R P_p P_s - \alpha_s P_s & (a), \\ \frac{dP_p}{dz} = -\frac{\omega_p}{\omega_s} g_R P_p P_s - \alpha_p P_p & (b), \end{cases} \quad (1)$$

де α_s, α_p , $[км^{-1}]$ – коефіцієнти поглинання світла відповідно на стоксовій частоті ω_s і частоті накачування ω_p . Формальний зв'язок рівнянь між собою забезпечує нелінійний

коефіцієнт ВКР підсилення g_R , $[(\text{Вт} \cdot \text{км})^{-1}]$, частотний спектр якого відповідає *профілю* ВКР підсилення $g_R = g_R(\Omega)$.

Зазначимо, що в загальному випадку аналітичні розв'язки навіть найпростішої системи (1) зараз не відомі і це суттєво ускладнює моделювання практичних ВКР підсилювачів для багатоканальних оптоволоконних систем, що показані на рис.1. Розрахунки багатократно ускладнюються у випадку моделювання реальних систем, в яких зараз можуть міститися кількасот стоксових хвиль (по числу каналів) та близько десятка довжин хвилі помпуювання, а їх сума буде визначати кількість зв'язаних диференціальних рівнянь, які підлягають числовим розв'язкам.

Однак, головна проблема моделювання полягає не у застосуванні більш ефективних алгоритмів розв'язку складних систем диференціальних рівнянь дуже високого рангу, а у наявності особливих точок для кожної сигнальної хвилі. З практичної точки зору особлива точка - це порогові значення потужності накачок, визначення яких відноситься до основних задач моделювання. Але поблизу від цих особливих точок розв'язки системи рівнянь стають нестійкими, тобто отримані числові результати надто сильно відхиляються одне від іншого за малих відхилень у заданих значеннях коефіцієнтів кожного рівняння.

Це обмеження методики диференціальних рівнянь має принциповий характер в задачах моделювання ВКР підсилення та може приводити до неоднозначних результатів. Негативний вплив нестійкості розв'язків на результати моделювання, однак, можна дещо зменшити шляхом забезпечення максимальної точності визначення всіх коефіцієнтів g_R в межах робочої смуги частот ВКР підсилювача. Експериментальні залежності $g_R(\Omega)$ показано на рис.2. Обидва профілі, як і для багатьох інших волокон із аморфного кварцового скла, мають вигляд нерівномірного континууму із терагерцовою шириною спектру, що сильно ускладнює проблему їх точного відтворення при моделюванні. Крім того, профіль ВКР підсилення є індивідуальним для кожного типу волокна і методи його максимально точної апроксимації являють собою окрему задачу. У підсумку, зважаючи на досить велику кількість досліджень, присвячених моделюванню динаміки ВКР підсилення для багатоканальних систем методом зв'язаних диференціальних рівнянь, що опубліковані за останні два десятиліття [4,5,11], проблема залишається ще дуже далекою від свого остаточного вирішення.

Альтернативно, в даній роботі використовувалась модель заданої накачки, фундаментальні основи якої ми ілюструємо за допомогою наближеного розв'язку базової системи рівнянь (1). Наближення, як відомо [32], полягає у тому, що розгляд обмежується випадком, коли першим членом у правій частині рівняння (1b) можна знехтувати, тобто при:

$$\frac{\omega_p}{\omega_s} g_R P_s \ll \alpha_p \quad (2)$$

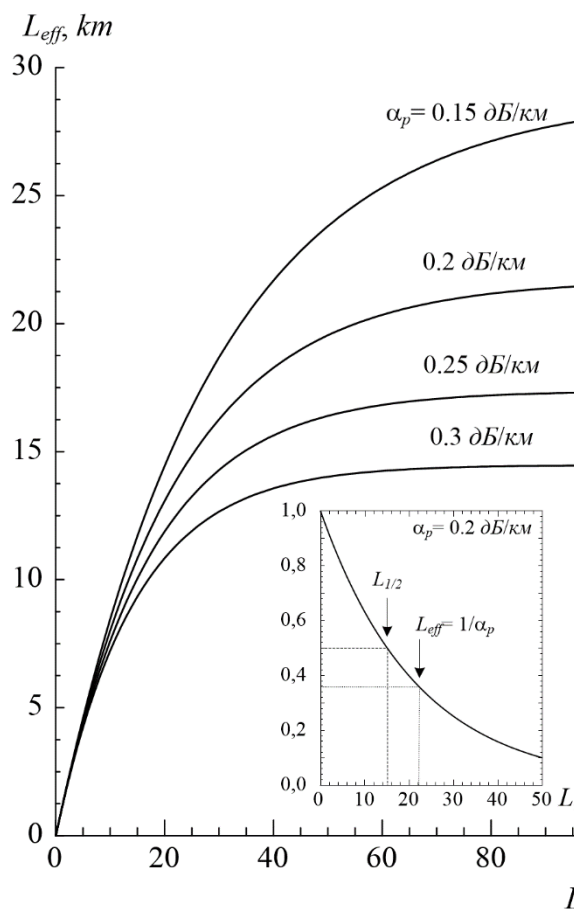


Рисунок - 3 Ефективна довжина взаємодії стоксової хвилі та накачки вздовж волокна довжиною L . На вставці показано співвідношення між характеристичними довжинами загасання $L_{1/2}$ та L_{eff} без ВКР підсилення

виснаження потужності накачування шляхом прямого її використання тільки на підсилення сигналу стає зневажливо малим у порівнянні із власним загасанням α_p для поточного значення потужності P_p . Без першого доданку у правій частині рівняння (1b) спрощене рівняння вже не зв'язане із рівнянням (1a). В результаті рівняння (1b) стає еквівалентним випадку вільного розповсюдження накачки у дисипативному середовищі із загасанням α_p , тобто накачка залишається заданою і не залежною від наявності нелінійної взаємодії. Розв'язок спрощеного рівняння є добре відомим і має вигляд: $P_p(z) = P_0 e^{-\alpha_p z}$, де $P_0 = P_p(z=0)$, $[Bm]$ - початкове значення потужності помпування у точці введення його до волокна. Підставляючи цей розв'язок у рівняння (1a), одержуємо шукане рівняння динаміки зміни потужності сигналу вздовж довжини волокна L :

$$P_s(L) = P_s(0) \exp(g_R P_0 L_{eff} - \alpha_s L), \quad (3)$$

де $L_{eff} = [1 - \exp(-\alpha_p L)] / \alpha_p$ - ефективна довжина взаємодії стоксової хвилі та накачки, [км], яка на початку волокна (при $\alpha_p L \ll 1$) дорівнює його фактичній довжині $L_{eff} \cong L$ (рис.3), але не перевищує асимптотичного значення $L_{eff} = 1/\alpha_p$ при $L \rightarrow \infty$. Отже, при великих $L \rightarrow \infty$ значення L_{eff} співпадає із довжиною, на якій потужність помпування зменшується в e разів. Тоді довжина $L_{1/2}$, на якій потужність накачки зменшується у 2 рази дорівнює $L_{1/2} = \ln(2) L_{eff} = 0,69 L_{eff}$. Співвідношення між характеристичними довжинами загасання $L_{1/2}$ та L_{eff} без ВКР підсилення ми показуємо на вставці рис.3. Слід зазначити, що в (3) $P_s(0)$ та $P_s(L)$ - це відповідні потужності сигналу на вході (при $z = 0$) та підсиленого на довжині L вихідного (при $z = L$) сигналу. Тоді, з урахуванням виразу (3), безрозмірний коефіцієнт підсилення стоксової хвилі $G_{on/off}(L) = P_s(L)/P_s(0)$ можна представити в аналітичному вигляді, як:

$$G_{on/off}(L) = \exp \left\{ \frac{g_R}{\alpha_p} P_0 [1 - \exp(-\alpha_p L)] - \alpha_s L \right\}, \quad (4)$$

що в межах зроблених наближень (застосовність яких ми аналізуємо нижче) дозволяє отримати досить точні результати при моделюванні процесів нелінійного оптичного підсилення шляхом вимушеного комбінаційного розсіяння в поширених одномодових волокнах, таких як TrueWave^{RS} та кварцове волокно G.652.

В логарифмічному масштабі вираз (4) для підсилення $G_{on/off}$ в [dB] прийме вигляд:

$$G_{on/off}[dB] = 4,343 \cdot \left\{ \frac{g_R}{\alpha_p} P_0 [1 - \exp(-\alpha_p L)] - \alpha_s L \right\}, \quad (5)$$

де числовий коефіцієнт - це $10 \log_{10} e = 4,343$. Аналітичні вирази (4) і (5) покладені в основу нашої спрощеної моделі для описання динаміки ВКР підсилення залежно від довжини волокна L . Моделювання враховує наявність оптичних втрат електромагнітного випромінювання у реальних волокнах як для накачки з коефіцієнтом загасання α_p , так і для сигналу із коефіцієнтом загасання α_s , а потужність накачки P_0 на вході до активного волокна є параметром моделі, що дозволяє налаштовувати величину $G_{on/off}$ підсилення у реальному пристрої.

Параметри моделювання. Числові параметри волокон, для яких проводилось моделювання зведено до Табл. 1.

Таблиця 1.

Параметри волокон, що були використані для моделювання динаміки розподіленого ВКР підсилення монохроматичного сигналу з $\lambda_s = 1,55$ мкм при помпуванні на довжині хвилі $\lambda_p = 1,425$ мкм.

Параметр	Тип волокна	
	G.652	TrueWave ^{RS}
1	2	3
1. Вхідна потужність сигналу, P_p , мВт	1	1
дБм	0	0
2. Частота сигналу, ω_s , ТГц	193,5	193,5
3. Загасання сигналу, α_s , дБ/км	0,2	0,2
км^{-1}	0,046	0,046
4. Частота накачки, ω_p , ТГц	210,5	210,5
5. Загасання накачки, α_p , дБ/км	0,25	0,3
км^{-1}	0,058	0,069
6. Довжина вільного загасання накачки, L_{eff} , км	17,4	14,5
$L_{1/2}$, км	12,0	10,0
7. Максимум профілю ВКР підсилення, g_{Rmax} , (Вт·км) ⁻¹	0,4	0,74
8. Порогова потужність накачки для ВКР підсилення, P_{th} , мВт	115,1	62,2
дБм	20,6	17,9
9. Критична потужність сигналу, P_s^{cr} , мВт	132,3	85,8
дБм	21,2	19,3

Критерій застосовності моделі. Однак, при цілком очевидних перевагах аналітичного моделювання, що проявляються, зокрема, при порівняльному аналізі різних волокон в якості активного середовища нелінійного оптичного підсилювача, слід враховувати обмеження, тобто виконання нерівності (2), яка має сенс критерію застосовності самої моделі. Якщо ввести значення критичної потужності сигналу P_s^{cr} :

$$P_s^{cr} = \frac{\omega_s}{\omega_p} \frac{\alpha_p}{g_{Rmax}}, \quad (6)$$

то нерівність

$$P_s \leq P_s^{cr} \quad (7)$$

можна розглядати як критерій застосовності аналітичної моделі. За своїм фізичним змістом потужність стоксової хвилі P_s^{cr} , згідно з (2) та (6), відповідає граничному значенню сигналу у підсилювачі, починаючи від якого підсилення сигналу набуває домінуючого характеру, оскільки відбір потужності сигналом [ліва частина (2)] починає перевищувати дисипативні втрати у волокні із сталою загасання α_p . Якщо зростання P_s приводить до обернення знаку нерівності (7), тобто при $P_s \gg P_s^{cr}$, то настає режим генерації, за якого в результаті конкуренції мод практично вся потужність помпування перетікає лише у вузький діапазон частот на максимумі профілю ВКР підсилення. Оскільки генерація в середині смуги частот будь-якого підсилювача (самозбудження) є вкрай небажаним режимом роботи, то можна сподіватись, що для забезпечення робочих режимів широкосмугових ВКР підсилювачів значення P_s і в загальному випадку (див. рис.1) повинно задовольняти нерівності типу (7).

Введену критичну потужність сигналу P_s^{cr} слід віднести до характеристикних параметрів волокна, яке буде використовуватись в якості активного середовища для нелінійного оптичного підсилення сигналу. Дійсно, оскільки $\omega_s/\omega_p \cong 1$, тобто майже не залежить від параметрів та схеми помпування, то числове значення P_s^{cr} на практиці є індивідуальним для кожного волокна. Воно визначається відношенням лінійного параметра

загасання α_p до нелінійного коефіцієнта ВКР підсилення $g_{R_{max}}$, де $g_{R_{max}}$ - максимум на профілі ВКР підсилення $g_R = g_R(\Omega)$. Згідно до співвідношень (2) та (6) виконання нерівності (7) при $g_R = g_{R_{max}}$ гарантовано виконується для всіх інших частот із смуги ВКР підсилення, тобто для всіх $g_R = g_R(\Omega)$.

Слід зазначити, що згідно із критерієм (7) порівнянню підлягають значення потужності сигналу P_s після підсилення на довжині L , а результати вважаються достовірними тільки за умови виконання цієї нерівності. Характеристичні параметри P_s^{cr} для досліджуваних волокон визначаються на попередньому етапі моделювання з урахуванням відповідних констант загасання α_p на довжині хвилі помпування. Числові значення цих параметрів наведено у Таблиці 1 для зручності перевірки виконання критерію (7) щодо підтвердження застосовності запропонованої моделі до кожного волокна. Зокрема, тверде виконання нерівності (7) в умовах нашого моделювання, коли потужність P_s виявляється практично на 2 порядки меншою за P_s^{cr} в обох волокнах, є незаперечним фактором на користь правомірності застосування наближеної моделі із гарантією достатньої точності представлених числових обчислень.

Результати моделювання та їх обговорення. Моделювання проводилось за схемою розподіленого підсилення із прямою накачкою, коли сигнал з $\lambda_s = 1,55$ мкм та потужністю $P_s = 1$ мВт розповсюджувався вздовж волокна разом із хвилею помпування з $\lambda_p = 1,425$ мкм значно більшої потужності. Обидві хвилі розповсюджувались в одному напрямі, а потужність накачки могла збільшуватись, починаючи від $P_p = 100$ мВт. Вхідні дані, що використані для нашого моделювання динаміки розподіленого ВКР підсилення, зведено до таблиці 1, які з метою порівняльного аналізу представлені для двох модельних волокон, а саме для волокон типу TrueWave^{RS} та чистого кварцового волокна стандарту G.652.

На попередньому етапі ми провели оцінку допустимого рівня збільшення підсилення в межах застосовності нашої аналітичної моделі. У результаті, згідно із (7), модель заданої накачки, при розрахунку параметрів схеми із прямою накачкою на основі (4) та (5), є придатною для моделювання, якщо коефіцієнт підсилення $G_{on/off}$ сигналу потужністю 1 мВт не перевищує ~ 120 (21 дБ) у стандартному волокні G.652, а для волокна типу TrueWave^{RS} - не перевищує ~ 70 (18 дБ). Зазначимо також, що для накачки потужністю $P_p = 100$ мВт поріг ВКР підсилення досягається тільки у волокні типу TrueWave^{RS} ($P_{th} = 62$ мВт), але не досягається у волокні G.652, оскільки $P_p < P_{th} = 109$ мВт і тоді $G_{on/off} < 1$ по всій довжині волокна, тобто нелінійність ефекту ВКР у допороговому режимі накачки приводить не до підсилення сигналу, а лише до зменшення його загасання у процесі розповсюдження вздовж волокна.

Результати моделювання динаміки розподіленого ВКР підсилення у волокнах типу TrueWave^{RS} та G.652 при розповсюдженні сигналу вздовж довжини L волокна для різних значень потужності накачування ілюструє рис. 4. Відповідні залежності коефіцієнтів $G_{on/off}(L)$ оптичного підсилення від довжини волокна лінії зв'язку зображено на рис. 4 для трьох значень $P_0 = 100; 200$ та 300 мВт: (a) – за лінійною шкалою, (b) – за логарифмічною шкалою, [у дБ].

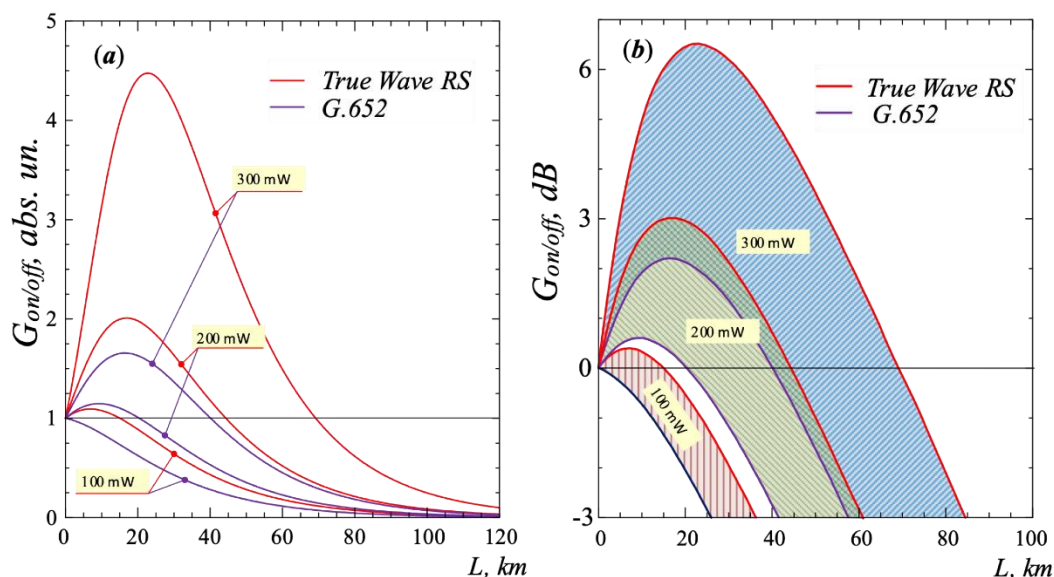


Рисунок - 4. Залежність розподіленого ВКР підсилення від довжини розповсюдження сигналу для трьох потужностей помпування, які генерує єдине джерело на $\lambda_p = 1425$ нм в ОМВ стандарту G.652 та у волокні типу TrueWave^{RS}: (a) – за лінійною шкалою, (b) – за логарифмічною шкалою

За виключенням допорогового режиму накачки при $P_0 = 100$ мВт у волокні G.652, альтернативно в обох волокнах накачка утворює області підсилення (рис.4), які залежно від потужності помпування займають довжину волокна L_0 , яку ми називаємо *довжиною повної прозорості* волокна. Дійсно, оскільки $G_{on/off}(L_0) = G_{on/off}(0) = 1$, то сигнал після проходження довжини L_0 буде мати свою початкову потужність, а ділянка транспортного волокна довжиною L_0 буде виглядати абсолютно прозорою, без загасання сигналу. Реально повну прозорість волокна забезпечує ВКР підсилення, причому для повної компенсації власних втрат волокна потужності накачки вистачає тільки на довжині L_0 . Потім при $L > L_0$ вплив помпування досить швидко зникає, а розповсюдження сигналу мало відрізняється від вільного поширення вздовж волокна без ВКР підсилення. Про це свідчить рис.4б, на якому логарифмічна залежність $G_{on/off}(L)$ має вигляд паралельних прямих в області $L > L_0$. Прямолінійний хід кривої $G_{on/off}(L)$ на логарифмічній шкалі відповідає звичайному експоненціальному закону загасання сигналу у волокні, а паралельність всіх прямих при $L > L_0$ свідчить про рівність всіх коефіцієнтів у показнику експоненти. Отже, на великій довжині від джерела помпування сталі загасання сигналу повертаються до своїх значень, які були без ВКР підсилення.

Динаміка компенсації власних втрат на довжині повної прозорості, як бачимо на рис.4, має нерівномірний характер із яскраво вираженим максимумом, що розташований на довжині волокна, яку ми позначаємо L_{max} . Значення L_{max} , як і характеристична довжина $L_{1/2}$, що відмічає точку половинного загасання сигналу після підсилювача, залежать від потужності помпування та параметрів активного волокна. В результаті моделювання ми отримали числові дані для цих характеристичних довжин волокна, які разом із коефіцієнтами підсилення G_{max} наведені у Таблиці 2.

Розподілене ВКР підсилення в обох типах волокон, як свідчать дані нашого моделювання із таблиці 2, дозволяють розширити область повної прозорості волокон на понад 150 км, якщо підсилювач використовується у режимі підсилення потужності вхідних сигналів, яка дорівнює 1 мВт. За майже однакових максимально досяжних значеннях L_0 в обох волокнах, волокно TrueWave^{RS} типу майже вдвічі більш ефективно дозволяє використати потужність помпування, ніж ОМВ стандарту G.652. Однак існує суттєва різниця критичних потужностей, а саме $P_s^{cr} = 86$ мВт для TrueWave^{RS} та $P_s^{cr} = 132$ мВт для ОМВ G.652, перевищення яких вкрай не бажано для підтримання робочих режимів ВКР підсилення.

Таблиця 2.

Динаміка *on/off* коефіцієнтів ВКР підсилення в залежності від зміни потужності помпування та характеристичні відстані максимального підсилення сигналу L_{max} , повної прозорості L_0 і половинного загасання потужності сигналу $L_{1/2}$ у волокні TrueWave RS порівняно із такими ж даними для стандартного волокна G.652.

P_0 , mW	$True\ Wave\ RS\ \text{волокно}$ $\alpha_p = 0,3\ \text{дБ/км}; \alpha_s = 0,2\ \text{дБ/км}$					$OMB\ \text{стандарту}\ G.652$ $\alpha_p = 0,25\ \text{дБ/км}; \alpha_s = 0,2\ \text{дБ/км}$								
	G_{max}	$G_{max},$ dB	$L_{max},$ km	$L_0,$ km	$L_{1/2},$ km	G_{max}	$G_{max},$ dB	$L_{max},$ km	$L_0,$ km	$L_{1/2},$ km				
1	2	3	4	5	6	7	8	9	10	11				
100	1,1	0,4	7	15	36,5	1	0	-	-	27				
200	2	3	17	44,5	61	1,16	0,6	9,5	21,5	42,5				
300	4,5	6,5	23	69	84,5	1,68	2,2	16,5	41	59				
500	27,1	14,3	30	116,5	131,5	4,48	6,5	25,5	74,5	90				
600	70,1	18,5	33	139,5	154,5	7,76	8,9	28,5	90	105,5				
700	184,7	22,7	35	163	178	13,7	11,4	31,5	105,5	120,5				
1000	$P_s > P_s^{cr}=86\ mBm$ – модель не застосовна					83	19,2	37,5	151	166				
1100	$P_s^{cr}=86\ mBm$ досягають при $P_0=614\ mBm$					154,2	21,9	39	166	181				
						$P_s > P_s^{cr}=132\ mBm$ – модель не застосовна								
						$P_s^{cr}=132\ mBm$ досягають при $P_0=1075\ mBm$								
Примітка: Використано розрахункові параметри: $\lambda_p = 1425\ nm, \lambda_s = 1550\ nm$														

Загалом дані Табл. 2 підтверджують застосовність нашої моделі для опису динаміки розподіленого ВКР підсилення у досить широкому діапазоні зміни потужностей помпування в обох типах волокон. Зазначимо, що розглянутий випадок підсилення потужності сигналу на вході лінії передачі є найбільш складним для моделювання, оскільки обмеження моделі полягають у не перевищенні критичної потужності P_s^{cr} сигналу. Тому умови застосовності моделі, очевидно, більш строго виконуються при зустрічному помпуванні сигналу з боку фотоприймача, коли підсилюються сигнали значно послаблені у процесі їх розповсюдження.

Висновки. В роботі представлено результати моделювання динаміки розподіленого ВКР підсилення за різних потужностей помпування та паралельного його розповсюдження із сигналом вздовж довжини двох типів кварцових волокон – TrueWave^{RS} та стандартного G.652. Обґрунтовано можливість використання спрощеної аналітичної моделі нелінійного ВКР підсилення оптичних сигналів, як ефективної альтернативи більш поширеній моделі прямого числового розв'язку складних систем диференціальних рівнянь із загальної теорії нелінійної взаємодії довільної кількості хвиль сигналів та накачки.

Вперше проаналізовано придатність наближення заданої накачки із теорії ВКР взаємодії в умовах практичної реалізації нелінійного підсилення оптичного сигналу в системах далекого зв'язку. Шляхом ведення критичної потужності сигналу P_s^{cr} , як нового характеристичного параметра активного волокна, запропоновано кількісний критерій застосовності моделі для описання динаміки нелінійного оптичного підсилення сигналу. Показано, що критерій застосовності моделі строго виконується для модельних волокон, причому в обох волоконних конфігураціях ВКР підсилювача – як із прямою, так і зустрічною накачкою.

Отримані результати моделювання динаміки нелінійного підсилення однозначно підтверджують значний ріст ефективності підсилення ВКР в активному волокні TrueWave^{RS} у порівнянні зі стандартним ОМВ із чистого кварцового скла, але при суттєво більших обмеженнях на максимальну потужність помпування.

ЛІТЕРАТУРА

1. Sirleto L. Ferrara M.A. Fiber amplifiers and fiber lasers based on stimulated Raman scattering: A Review. *Micromachines*, 2020, 11(3), 247; <https://doi.org/10.3390/mi11030247>.
2. Коротков П.А., Фелінський. Г. С., Волоконні ВКР лазери неперервної дії // УФЖ. Огляди. – 2007. – Т.4, № 1. – С. 36-60.

3. Islam M.N. Raman amplifiers for telecommunications // *IEEE J. Sel. Top. Quant. Electron.* – 2002. – Vol. 8, N 3. – P. 548-559.
4. Коротков П.А., Фелінський Г.С. ВКР підсилення світла в одномодових кварцових волокнах // *УФЖ. Огляди.* – 2009. – т.6, № 2. – С. 103-169.
5. Григорук В. І., Сердега І. В., Фелінський Г. С., Коротков П. А. Волоконні ВКР лазери та підсилювачі оптичного випромінювання, Розділ 2 у монографії: Взаємодія фізичних полів з наноструктурованими матеріалами. – К.:Каравела, 2018. – 382с., с. 62-128. ISBN 978-966-2229-77-6.
6. Puttnam B. J., Luis R. S., Rademacher G., Awaji Y., Furukawa H. 1 Pb/s Transmission in a 125 μ m diameter 4-core MCF," *2022 Conference on Lasers and Electro-Optics (CLEO)*, San Jose, CA, USA, 2022, pp. 1-2. <https://www.nict.go.jp/en/press/2022/05/30-1.html>
7. Puttnam B. J., Luis R. S., Rademacher G., Awaji Y., Furukawa H., 319 Tb/s Transmission over 3001 km with S, C and L band signals over >120nm bandwidth in 125 μ m wide 4-core fiber," *2021 Optical Fiber Communications Conference and Exhibition (OFC)*, San Francisco, CA, USA, 2021, pp. 1-3.
8. Takara H., Mizuno T., Kawakami H., Miyamoto Y., Masuda H., Kitamura K., Ono H., Asakawa S., Amma Y., Hirakawa K., Matsuo S., Tsujikawa K., Yamada M. 120.7-Tb/s MCF-ROPA unrepeated transmission of PDM-32QAM channels over 204 km, *J. Light. Technol.* 33, No. 7, 1473 (2015). DOI: 10.1109/JLT.2015.2397009.
9. Крутінъ, Я. В., Корчак, О. В., Резніков, М. І., & Фелінський, Г. С. (2022). Моделювання ВКР підсилювача в активному волокні TrueWave^{RS} з рівномірною смугою у C+L телекомунікаційних вікнах. *Вісті вищих учбових закладів. Радіоелектроніка*, 64(12), 715–730. <https://doi.org/10.20535/S0021347021120013>
10. Recommendation ITU-T G.652. Series G: Transmission systems and media, digital systems and networks. Optical fibre cables. Characteristics of a single-mode optical fibre and cable. Ed.9, Rec. ITU-T G.652 (11/2016).
11. Yao J., Deng H. Fiber Raman Amplifier Based on Improved Whale Algorithm. *The 2nd International Conference on Electronic Information and Communication Engineering (EICE 2023)* 13- 15 Jan 2022 Guangzhou, China, *J. Phys.: Conf. Ser.* 2525 012016, 2023 **DOI:** 10.1088/1742-6596/2525/1/012016
12. Jiang H.M., Xie K., Wang Y.F. Pump scheme for gain-flattened Raman fiber amplifiers using improved particle swarm optimization and modified shooting algorithm. *Optics Express*, 18(11), p.11033-45, 2010. <https://doi.org/10.1364/OE.18.011033> +
13. Liu T., Liu L., Chen J., Jiang H., Sun Q., Xi Y. Optimal design of Raman fibre amplifier based on terminal value optimization strategy and shuffled frog leaping algorithm. *Journal of Modern Optics*, 65(14): 1680-7, 2018. DOI:10.1080/09500340.2018.1455912 +
14. Jiang H.M., Xie K., Wang Y F. Optimization of pump parameters for gain flattened Raman fiber amplifiers based on artificial fish school algorithm. *Optics Communications*, 284(23): 5480-3, 2011. <https://doi.org/10.1016/j.optcom.2011.07.074> -
15. Chen J., Jiang H. Optimal Design of Gain-Flattened Raman Fiber Amplifiers Using a Hybrid Approach Combining Randomized Neural Networks and Differential Evolution Algorithm [J]. *IEEE Photonics Journal*, 10(2): 15, 2018. DOI: 10.1109/JPHOT.2018.2817843 +
16. Tizhoosh H. R. Opposition-based learning: A new scheme for machine intelligence, *International Conference on Computational Intelligence for Modelling, Control and Automation and International Conference on Intelligent Agents, Web Technologies and Internet Commerce (CIMCA-IAWTIC'06)*, Vienna, Austria, 2005, pp. 695-701, doi: 10.1109/CIMCA.2005.1631345.
17. Seyedali Mirjalili A.B., Lewis A. The Whale Optimization Algorithm. *Advances in Engineering Software*. Vol. 95, May 2016, p. 51-67, <https://doi.org/10.1016/j.advengsoft.2016.01.008>
18. Zhou H., Zeng X., Hong Y. Adaptive Exact Penalty Design for Constrained Distributed Optimization, *IEEE Transactions on Automatic Control*, vol. 64, no. 11, pp. 4661-4667, Nov. 2019, doi: 10.1109/TAC.2019.2902612.
19. Singh K., Patterh M.S., Bhamrah M.S. A Comparative Analysis of Dual-Order Bidirectional Pumping Schemes in Optical Fiber Raman Amplification. *Journal of Optical Communications*, 2019, 40(1): 1-6. <https://doi.org/10.1515/joc-2017-0018>
20. Zhang W., Feng X, Peng J., Liu X. A simple algorithm for gain spectrum adjustment of backward-pumped distributed fiber Raman amplifiers, *IEEE Photonics Technology Letters*, vol. 16, no. 1, pp. 69-71, Jan. 2004, doi: 10.1109/LPT.2003.818915 .
21. Achtenhagen M., Chang T.G., Nyman B. Analysis of a multiple-pump Raman amplifier, *Appl. Phys. Lett.* – 2001. – Vol. 78. – P. 1322–1324. <https://doi.org/10.1063/1.1352665>

22. Yan M., Chen J., Jiang W., Li J., Chen J., Li X. Automatic design scheme for optical-fiber Raman amplifiers backward-pumped with multiple laser diode pumps, in *IEEE Photonics Technology Letters*, vol. 13, no. 9, pp. 948-950, Sept. 2001, doi: 10.1109/68.942656.
23. Xiao P., Zeng Q., Huang J., Liu J. A new optimal algorithm for multipump sources of distributed fiber Raman amplifier, *IEEE Photonics Technology Letters*, vol. 15, no. 2, pp. 206-208, Feb. 2003, doi: 10.1109/LPT.2002.806086.
24. Zhou X., Lu C., Shum P., Cheng T. H. A simplified model and optimal design of a multiwavelength backward-pumped fiber Raman amplifier, *IEEE Photonics Technology Letters*, vol. 13, no. 9, pp. 945-947, Sept. 2001, doi: 10.1109/68.942655.
25. Serdeha I.V., Grygoruk V.I., Felinskyi G.S. Spectroscopic features of Raman gain profiles in single-mode fibers based on silica glass // *Ukr. J. Phys.* 2018. Vol. 63, No. 8, p. 683-700.
26. Felinskyi G. S., Grygoruk V. I., Serdeha I. V. Modelling of gain profiles and Raman lasing in TiO₂/GeO₂-doped silica fibres,” *Ukr. J. Phys. Opt.*, vol. 21, no. 1, pp. 15–25, 2020, doi: 10.3116/16091833/21/1/15/2020.
27. Felinskyi G. S., Grygoruk V. I., Serdeha I. V., Drobakhin O. O., Andreev M. V. Gaussian and Rational Approximation of Raman Gain Profile in TiO₂ Doped Silica Fiber, 2021 IEEE 26th International Seminar/Workshop on Direct and Inverse Problems of Electromagnetic and Acoustic Wave Theory (DIPED), 2021, pp. 130-133, doi: 10.1109/DIPED53165.2021.9552290
28. Krutin Ya. V., Korchak O. V., Reznikov M. I., Felinskyi G. S. Simulation of Raman amplifier using TrueWave RS active fiber with uniform bandwidth in C+L telecommunication windows, *Radioelectronics and Communications Systems*, 2021, Vol. 64, No. 12, pp. 619–632, ISSN 0735-2727, DOI: 10.3103/S0735272721120013
29. Petrychuk M. V., Grygoruk V. I., Pavlyuk S. P., Serdeha I. V., Felinskyi G. S. Interaction of physical fields with nanostructured materials, Chapter 2 «Light amplification based on stimulated Raman effect and spectroscopic modeling of Raman gain in single mode fiber». *Schriften des Forschungszentrums Julich*, 2020, vol.211, p.47-110. ISBN 978-3-95806-450-8.
30. Kononenko A.A., Zhiron G.B., Felinskyi G.S., Tytova O.I. Dynamics of distributed Raman gain in telecommunication True Wave^{RS} and G.652 fibers // *Proc. XXIII Int. Young Scientists' Conf. on Applied Physics, ICAP 2023*, May, 16-20, 2023, Kyiv, Ukraine, p. 141-142.
31. Reznikov M., Felinskyi G., Korchak A.V. Effect of amplified spontaneous emission on fiber span in backward pumped Raman amplifier / 2019 IEEE 8th Int. Conf. on Advanced Optoelectronics and Lasers, CAOL 2019, September 6-8, Sozopol, Bulgaria, p. 259-262. **DOI:** 10.1109/CAOL46282.2019.9019507
32. Григорук В.І., Коротков П.А., Фелінський Г.С. Нелінійні та лазерні процеси в оптичних волокнах. – К.: ВПЦ „Київський університет”, 2008. –576с.

REFERENCES:

1. L. Sirleto, M.A. Ferrara. Fiber amplifiers and fiber lasers based on stimulated Raman scattering:A Review. *Micromachines*, 2020, 11(3), 247; <https://doi.org/10.3390/mi11030247>.
2. P.A. Korotkov, G.S. Felinskyi. Continuous-Wave Fiber Raman Lasers // *Ukrainian Journal of Physics. Reviews.* – 2007. – Vol. 4, No. 1. – P. 36-60.
- 3.N. Islam. Raman amplifiers for telecommunications // *IEEE J. Sel. Top. Quant. Electron.* – 2002. – Vol. 8, N 3. – P. 548-559.
4. P. A. Korotkov and G. S. Felinskyi, “Forced-Raman-scattering-based amplification of light in one-mode quartz fibers,” *Ukr. J. Physics. Rev.* 6, No. 2, 103-169 (2009).
5. V. I. Grygoruk, I. V. Serdeha, G. S. Felinskyi, P. A. Korotkov, "Fiber Raman Lasers and Amplifiers of Optical Radiation," Chapter 2 in the monograph "Interaction of Physical Fields with Nanostructured Materials." - Kyiv: Karavella, 2018. - 382 p., pp. 62-128. ISBN 978-966-2229-77-6.
6. B. J. Puttnam, R. S. Luis, G. Rademacher, Y. Awaji and H. Furukawa, "1 Pb/s Transmission in a 125µm diameter 4-core MCF," 2022 *Conference on Lasers and Electro-Optics (CLEO)*, San Jose, CA, USA, 2022, pp. 1-2. <https://www.nict.go.jp/en/press/2022/05/30-1.html>
7. B. J. Puttnam, R. S. Luís, G. Rademacher, Y. Awaji and H. Furukawa, "319 Tb/s Transmission over 3001 km with S, C and L band signals over >120nm bandwidth in 125 µm wide 4-core fiber," 2021 *Optical Fiber Communications Conference and Exhibition (OFC)*, San Francisco, CA, USA, 2021, pp. 1-3.
8. H. Takara, T. Mizuno, H. Kawakami, Y. Miyamoto, H. Masuda, K. Kitamura, H. Ono, S. Asakawa, Y. Amma, K. Hirakawa, S. Matsuo, K. Tsujikawa, and M. Yamada, “120.7-Tb/s MCF-ROPA unrepeated transmission of PDM-32QAM channels over 204 km,” *J. Light. Technol.* 33, No. 7, 1473 (2015). DOI: 10.1109/JLT.2015.2397009.

9. Krutin, Y. V., Korchak, O. V., Reznikov, M. I., Felinsky, G. S. (2022). Simulation of Raman Amplifier Using TrueWave RS Active Fiber with Uniform Bandwidth in C+L Telecommunication Windows Bulletin of Higher Educational Institutions. Radio Electronics, 64(12), 715–730.
10. Recommendation ITU-T G.652. Series G: Transmission systems and media, digital systems and networks. Optical fibre cables. Characteristics of a single-mode optical fibre and cable. Ed.9, Rec. ITU-T G.652 (11/2016).
11. J. Yao and H. Deng. "Fiber Raman Amplifier Based on Improved Whale Algorithm" The 2nd International Conference on Electronic Information and Communication Engineering (EICE 2023) 13- 15 Jan 2022 Guangzhou, China, J. Phys.: Conf. Ser. 2525 012016, 2023 DOI: 10.1088/1742-6596/2525/1/012016
12. H.M. Jiang, K. Xie, Y.F. Wang. Pump scheme for gain-flattened Raman fiber amplifiers using improved particle swarm optimization and modified shooting algorithm. *Optics Express*, 18(11), p.11033-45, 2010. <https://doi.org/10.1364/OE.18.011033> +
13. T. Liu, L. Liu, J. Chen, H. Jiang, Q. Sun and Y. Xi. Optimal design of Raman fibre amplifier based on terminal value optimization strategy and shuffled frog leaping algorithm. *Journal of Modern Optics*, 65(14): 1680-7, 2018. DOI:10.1080/09500340.2018.1455912 +
14. H.M. Jiang, K. Xie, Wang Y F. Optimization of pump parameters for gain flattened Raman fiber amplifiers based on artificial fish school algorithm. *Optics Communications*, 284(23): 5480-3, 2011. <https://doi.org/10.1016/j.optcom.2011.07.074> -
15. J. Chen, H. Jiang. Optimal Design of Gain-Flattened Raman Fiber Amplifiers Using a Hybrid Approach Combining Randomized Neural Networks and Differential Evolution Algorithm [J]. *IEEE Photonics Journal*, 10(2): 15, 2018. DOI: 10.1109/JPHOT.2018.2817843 +
16. H. R. Tizhoosh, "Opposition-based learning: A new scheme for machine intelligence, " *International Conference on Computational Intelligence for Modelling, Control and Automation and International Conference on Intelligent Agents, Web Technologies and Internet Commerce (CIMCA-IAWTIC'06)*, Vienna, Austria, 2005, pp. 695-701, doi: 10.1109/CIMCA.2005.1631345. +
17. A.B. Seyedali Mirjalili, A. Lewis. The Whale Optimization Algorithm. *Advances in Engineering Software*. Vol. 95, May 2016, p. 51-67, <https://doi.org/10.1016/j.advengsoft.2016.01.008> +
18. H. Zhou, X. Zeng and Y. Hong, "Adaptive Exact Penalty Design for Constrained Distributed Optimization," *IEEE Transactions on Automatic Control*, vol. 64, no. 11, pp. 4661-4667, Nov. 2019, doi: 10.1109/TAC.2019.2902612.
19. K. Singh, M.S. Patterh, M.S. Bhamrah. A Comparative Analysis of Dual-Order Bidirectional Pumping Schemes in Optical Fiber Raman Amplification. *Journal of Optical Communications*, 2019, 40(1): 1-6. <https://doi.org/10.1515/joc-2017-0018>
20. W. Zhang, X. Feng, J. Peng and X. Liu, "A simple algorithm for gain spectrum adjustment of backward-pumped distributed fiber Raman amplifiers," *IEEE Photonics Technology Letters*, vol. 16, no. 1, pp. 69-71, Jan. 2004, doi: 10.1109/LPT.2003.818915.
21. M. Achtenhagen, T.G. Chang, B. Nyman, *et al.* "Analysis of a multiple-pump Raman amplifier", *Appl. Phys. Lett.* – 2001. – Vol. 78. – P. 1322–1324. <https://doi.org/10.1063/1.1352665>
22. M. Yan, J. Chen, W. Jiang, J. Li, J. Chen and X. Li, "Automatic design scheme for optical-fiber Raman amplifiers backward-pumped with multiple laser diode pumps," in *IEEE Photonics Technology Letters*, vol. 13, no. 9, pp. 948-950, Sept. 2001, doi: 10.1109/68.942656.
23. P. Xiao, Q. Zeng, J. Huang and J. Liu, "A new optimal algorithm for multipump sources of distributed fiber Raman amplifier," in *IEEE Photonics Technology Letters*, vol. 15, no. 2, pp. 206-208, Feb. 2003, doi: 10.1109/LPT.2002.806086.
24. X. Zhou, C. Lu, P. Shum and T. H. Cheng, "A simplified model and optimal design of a multiwavelength backward-pumped fiber Raman amplifier," in *IEEE Photonics Technology Letters*, vol. 13, no. 9, pp. 945-947, Sept. 2001, doi: 10.1109/68.942655.
25. I.V. Serdeha, V.I. Grygoruk, G.S. Felinskyi. Spectroscopic features of Raman gain profiles in single-mode fibers based on silica glass // *Ukr. J. Phys.* 2018. Vol. 63, No. 8, p. 683-700.
26. G. S. Felinskyi, V. I. Grygoruk, and I. V. Serdeha, "Modelling of gain profiles and Raman lasing in TiO₂/GeO₂-doped silica fibres," *Ukr. J. Phys. Opt.*, vol. 21, no. 1, pp. 15–25, 2020, doi: 10.3116/16091833/21/1/15/2020.
27. G. S. Felinskyi, V. I. Grygoruk, I. V. Serdeha, O. O. Drobakhin and M. V. Andreev, "Gaussian and Rational Approximation of Raman Gain Profile in TiO₂ Doped Silica Fiber," 2021 IEEE 26th International Seminar/Workshop on Direct and Inverse Problems of Electromagnetic and Acoustic Wave Theory (DIPED), 2021, pp. 130-133, doi: 10.1109/DIPED53165.2021.9552290

28. Ya. V. Krutin, O. V. Korchak, M. I. Reznikov, and G. S. Felinskyi "Simulation of Raman amplifier using TrueWave RS active fiber with uniform bandwidth in C+L telecommunication windows", Radioelectronics and Communications Systems, 2021, Vol. 64, No. 12, pp. 619–632, ISSN0735-2727, DOI: 10.3103/S0735272721120013
29. M. V. Petrychuk, V. I. Grygoruk, S. P. Pavlyuk, I. V. Serdeha, G. S. Felinskyi «Interaction of physical fields with nanostructured materials», Chapter 2 «Light amplification based on stimulated Raman effect and spectroscopic modeling of Raman gain in single mode fiber». Schriften des Forschungszentrums Julich, 2020, vol.211, p.47-110. ISBN 978-3-95806-450-8.
30. A.A. Kononenko, G.B. Zhirov, G.S. Felinskyi, O.I. Tytova Dynamics of distributed Raman gain in telecommunication True Wave^{RS} and G.652 fibers // тезисы Proc. XXIII Int. Young Scientists' Conf. on Applied Physics, ICAP 2023, May, 16-20, 2023, Kyiv, Ukraine, p. 141-142.
31. M. Reznikov, G. Felinskyi, and A.V. Korchak. Effect of amplified spontaneous emission on fiber span in backward pumped Raman amplifier / 2019 IEEE 8th Int. Conf. on Advanced Optoelectronics and Lasers, CAOL*2019, September 6-8, Sozopol, Bulgaria, p. 259-262. DOI: 10.1109/CAOL46282.2019.9019507
32. V.I. Hryhoruk, P.A. Korotkov, H.S. Felinsky. Nonlinear and Laser Processes in Optical Fibers. – Kyiv: Publishing and printing center 'Kyiv University', 2008. – 576 p.

**D.Sci., prof. Felinskyi G.S., Ph.D. Zhyrov G.B., Ph.D. Korchak O.V.,
Ph.D. Reznikov M.I., Kononenko A.A.**

MODELING OF DISTRIBUTED NONLINEAR OPTICAL AMPLIFICATION IN TRUEWAVE AND G.652 TELECOMMUNICATION FIBERS

Common techniques for modeling of the nonlinear optical amplifiers, specifically based on the effect Raman effect, despite the simplicity of its technical implementation, are quite complex and cumbersome due to the necessity of theoretically describing the nonlinear interaction of many pump and signal optical waves using the corresponding systems of high-order differential equation. The fundamental limitations of such methodologies lie not only in the number of equations but also in the existence of special points in each equation describing the dynamics of signal waves (these points correspond to threshold values of pump power). Under these conditions, the solutions instabilities of the differential equations and their ambiguity sometimes have a detrimental impact on modeling results. An alternative modeling approach using the specified pump approximation requires particular investigations of its practical applicability to the analysis of distributed optical amplification in telecommunications fibers.

Therefore, there is a need to determine the criterion for the applicability of the specified pump approximation for the development of a simplified model of nonlinear optical signal amplification under the conditions of their propagation along standard silica fibers. Among the undeniable advantages of analytical solutions obtained based on the simplified model there is the elimination of the mentioned constraints of solving systems of many differential equations.

This article is devoted to modeling the dynamics of distributed Raman amplification, as function the length of standard single-mode optical fiber (SMF) and pump power. In justifying the proposed modeling methodology, it is shown that the parameters of active fibers and fiber Raman amplifier (hereinafter referred to as FRA) schemes correspond to the criterion for the applicability of the specified pump approximation.

The paper presents an analytical expression for the criterion of the applicability of the specified pump approximation in the form of an upper limit of the signal power, which cannot exceed the amplified signal. Comparative analysis results of the distributed FRA parameters depending on the length of active fibers, such as G.652 and TrueWave^{RS}, are presented.

Keywords: SRS amplifier, optical signal amplification, pump power, pumping power, telecommunications systems.

УДОСКОНАЛЕННЯ СПОСОБІВ ВЕДЕННЯ ІНЖЕНЕРНОЇ РОЗВІДКИ В ІНТЕРЕСАХ ІНЖЕНЕРНОЇ ПІДТРИМКИ БОЙОВИХ ДІЙ ВІЙСЬК (СИЛ)

Досвід російсько-української війни свідчить, що із досить великими просторово-темповими показниками ведення бойових дій збільшуються й обсяги виконання одного із основних заходів інженерної підтримки – інженерної розвідки, що у свою чергу призводить до перевищення потрібного часу та необхідності залучення значної кількості ресурсів на її реалізацію.

Для розв'язання такої невідповідності слід передбачати окрім підсилення у силах та засобах, їх раціональний розподіл, а й вибір найефективніших способів виконання поставлених завдань. Нехтування завданнями (заходами) інженерної підтримки завжди призводить до невиправданих втрат в особовому складі, озброєнні і військовій техніці.

Мета дослідження – пошук нових, більш прогресивних способів ведення інженерної розвідки, розкрити роль, ризики, переваги і недоліки та проаналізувати можливість їх інтегрування в практику інженерних військ.

Основним завданням було визначення ефективності способів виконання завдань інженерної розвідки, склад оснащення інженерно-розвідувальних органів з урахуванням можливостей сучасних технічних засобів. Проаналізовано завдання інженерної розвідки в основних видах бою (операціях) та на різних рівнях до виконання яких залучаються підрозділи інженерних військ. Встановлено, що запропоновані способи ведення інженерної розвідки призведуть до різкої зміни умов її ведення та скорочення часу на виконання розвідувальних заходів інженерними підрозділами на окремих об'єктах. Вивчено роль, місце і вплив безпілотних літальних апаратів різних типів, що використовувалися силами оборони в ході виконання бойових завдань і встановлено, що найбільш ефективними способами, як в ході оборонного, так і наступального бою (операції) є комбіновані повітряно-наземні.

Упровадження пропонованих способів інженерної розвідки сприяє покращенню таких основних показників, як оперативність та достовірність, органів управління та військ (сил) порівняно з традиційними підходами.

Основний напрямок подальших досліджень необхідно спрямувати на розроблення різних способів ведення інженерної розвідки з урахуванням тенденцій у напрямку роботизації процесів для підвищення можливостей ведення контрміної боротьби.

Ключові слова: інженерна підтримка, інженерна розвідка, способи, інженерні заходи, безпілотні літальні апарати.

Вступ. Успішне ведення сучасних бойових дій (БД) військ (сил) неможливе без знання противника та здійснених ним інженерних завдань, а також без детального знання місцевості. Тому першочерговим заходом інженерної підтримки ведення БД військ (сил) є інженерна розвідка (ІР) противника та місцевості, сутність якої полягає у проведенні комплексу організаційних етапів щодо добування, узагальнення, оброблення й доведення до органів управління та військ необхідних інженерно-розвідувальних відомостей [1].

Ведення ІР може здійснюватися наземно та з повітря, при цьому класичними її способами є: спостереження, фотографування, безпосередній огляд, пошук та ін. Виконання заходів ІР в інтересах інженерної підтримки (ІП) ведення БД військ (сил) покладається на інженерно-розвідувальні органи, ефективність функціонування яких визначатиметься насамперед професійною і технічною компонентами [2, 3].

Основними перевагами повітряної розвідки перед наземною є значні просторово-часові показники. Втім застосування літальних апаратів, таких як вертольоти та літаки, передбачає створення складної багаторівневої організаційно-технічної системи, яка включає сукупність

обов'язкових взаємопов'язаних етапів від розроблення та узгодження програми польоту до технічної підтримки і супроводження виконання завдань. Окрім зазначеного, до проблемних питань необхідно віднести обмежені можливості спеціалізованого обладнання, яке не дозволяє здійснювати детальне обстеження окремих важливих об'єктів з відповідною точністю у стислі терміни, що призводить до часткового порушення принципів скритності, раптовості та достовірності [2, 3].

Натомість широкого застосування набули безпілотні літальні апарати (БПЛА) різного класу (типу), які фактично витісняють літаки і вертольоти, однак способи їх використання потребує дослідження на предмет доцільності та ефективності для виконання заходів ІР [3, 4].

Важливим аспектом є той факт, що переважна більшість органів ІР укомплектовані засобами, що розроблені в радянські часи, які вже є морально та фізично застарілими, а надходження від країн-партнерів новітніх засобів забезпечує часткове вирішення проблеми. Враховуючи факт інтенсивного застосування мінно-вибухових загороджень противником в ході російсько-української війни, впровадження досягнень в області інформаційних технологій у військову сферу та ін., все це обумовлює необхідність в пошуку нових підходів, способів до ведення ІР і створення нових засобів ведення ІР.

Слід зазначити, що найбільш достовірними розвідувальними відомостями вважаються ті, що отримані шляхом безпосереднього огляду і пошуком, як в ході БД, так і під час підготовки до них. Однак, враховуючи такий важливий комплексний фактор, як швидкоплинність ведення БД, при цьому співставляючи можливості розвідувального органу, своєчасність та якість виконання поставлених завдань, можна зробити висновок, що не у повній мірі відповідає сучасним вимогам, що висуваються, основними з яких є так звані "часові показники" ведення ІР [5 - 7].

Аналіз останніх досліджень та постановка задачі. Аналіз джерел у яких започатковано вирішення даної проблеми і на які опираються автори, свідчить, що питання удосконалення існуючих способів ведення ІР, в керівних документах, розкрито не в повному обсязі, що у свою чергу спонукає до опрацювання науково-методичних розробок та відповідних рекомендацій.

Наявний науково-методичний апарат базується на положеннях, які розробляли: у роботі [8] запропоновано узагальнену методику планування повітряної розвідки із використанням БпЛА для загального моніторингу великих територій на оперативно-тактичну глибину; у [9] детально проаналізовано та обґрунтовано доцільність ведення ІР з використанням БпЛА у районах інтенсивного ведення мінної війни та вимог до засобів даного типу; у [3] зазначено етапність організаційно-підготовчих заходів, порядок вибору способу виконання завдань, а також обґрунтовано основні тенденції розвитку технічних засобів ІР; у статті [10] проведено аналіз існуючих методів визначення координат наземних об'єктів за допомогою БпЛА та запропоновано алгоритм їх отримання на основі вдосконаленого псевдодальномірного методу із використанням малогабаритних БпЛА.

У положеннях, які розроблялися авторами [3, 8 - 13], безумовно враховуються окремі підходи і способи виконання інженерно-розвідувальних заходів в загальній системі ІІ БД військ (сил). Однак, отримані результати недостатньо враховують ряд питань: підготовки фахівців щодо застосування засобів ІР, які надходять від країн-партнерів, інтенсивних змін, що відбуваються в ході ведення російсько-української війни, і як головне – відсутністю системного розгляду даної проблеми, тож можуть бути адаптовані сучасним умовам ведення збройної боротьби лише частково.

Проте питання пошуку нових та адаптація відомих способів ведення ІР, вибору кращих серед них для підвищення рівня виконання завдань ІІ є актуальним та потребує детальних досліджень.

Мета статті. Досвід ІІ підготовки й ведення БД, зокрема питання ІР, як одного із головних і першочергових заходів, що проводиться в інтересах забезпечення підрозділів сил оборони України набуває особливого значення.

Таким чином, забезпечення стрімкості дій військ (сил) в умовах сучасної війни висунула на перший план актуальну проблему, а саме: пошук нових, більш прогресивних способів ведення ІР, які неодмінно повинні ґрунтуватися на отриманому досвіді в ході ведення російсько-української війни, а також виконання завдань підрозділами збройних сил країн-членів Альянсу.

Виклад основного матеріалу. Проведений аналіз завдань ІР в основних видах бою (операціях) та на різних рівнях, дає змогу систематизувати їх за ознаками, які наведено у табл. 1.

Таблиця 1

Класифікація завдань ІР в основних видах бою (операціях)

Перелік основних завдань ІР	Основні види БД	
	оборона	наступ
підтвердження аналізу місцевості на підтримку процесу розвідувального забезпечення тактичних дій	+	+
розвідка маршрутів, підтвердження інформації про місцевість або її оновлення	-/+	+
отримання інформації про пересування по пересічній місцевості, визначення прохідності місцевості для бойової техніки та транспортних засобів, стану доріг та мостів	-/+	+
розвідка природних перешкод, загороджень противника на підтримку маневру	-/+	+
визначення місць розташування, складу (угруповання), положення, оснащення, стану, можливостей, характеру і способів дій (намірів) інженерних військ противника	+	+
розвідка в інтересах підтримки передової (армійської) авіації	-/+	-/+
визначення об'єктів місцевої інфраструктури, комунальних об'єктів, ресурсів та маршрутів	-/+	+
ідентифікація боєприпасів, що не вибухнули	+	+
отримання інформації про бойові пошкодження та втрати	+	+
організація зв'язку та взаємодії між ІР та розвідками інших родів військ та служб щодо добування інженерних відомостей	+	+
супровід виконання завдань ІР	+	+

З проведеного аналізу видно, що вони мають практично однакову вагомість, а для їх виконання призначаються наступні органи: інженерні спостережні пости (ІСП); інженерні розвідувальні дозори (ІРД) та інженерні розвідувальні групи (ІРГ).

Як вже частково зазначалося раніше, інженерні розвідувальні відомості про противника, місцевість добуваються наземним та повітряним спостереженням, і фото- та відеозйомкою, безпосереднім оглядом, пошуком, а також вивченням захоплених документів і зразків озброєння, опитуванням місцевих жителів, допитом перебіжчиків та полонених. Крім того, інженерні розвідувальні відомості можуть бути отримані від військових та цивільних джерел, а також у результаті вивчення карт, супутникових знімків, воєнно-географічних описів, довідників та інших документів [2, 3].

Однак, зростання темпу ведення БД призвели до різкої зміни умов ведення ІР та скорочення часу на виконання розвідувальних заходів інженерними підрозділами на окремих об'єктах. Поряд з цим слід зазначити, що на даному етапі необхідно враховувати ряд обов'язкових показників, які притаманні практично усім способам ведення ІР [5]:

1. Час на організацію та ведення ІР об'єктів, на визначення стану яких прогнозується затратити найбільше часу (год.):

$$T_{\text{об.заг}}^{\text{ір}} = T_{\text{орг}}^{\text{ір}} + T_{\text{вед}}^{\text{ір}},$$

де $T_{\text{орг}}^{\text{ір}}$ – час на організацію ІР;

$T_{\text{вед}}^{\text{ip}}$ – час на ведення ІР.

2. Час на організацію ІР:

$$T_{\text{орг}}^{\text{ip}} = T_{\text{пр.р}} + T_{\text{пост.зав}} + T_{\text{підг.підр}} + T_{\text{висув}}^{\text{ІРО}},$$

де $T_{\text{орг}}^{\text{ip}}$ – час на організацію ІР;

$T_{\text{пр.р}}$ – час, який витрачає командир (начальник) для прийняття рішення на організацію ІР (за досвідом) приймається: рівень в/ч – до 25–30 хв (0,4 – 0,5 год);

$T_{\text{пост.зав}}$ – час, який командир (начальник) витрачає на постановку завдань інженерним розвідувальним органам, приймається: рівень в/ч – до 25 хв (0,4 год);

$T_{\text{підг.підр}}$ – час, який витрачає командир інженерного підрозділу (старший) на підготовку інженерно-розвідувального органу до ведення ІР приймається: для ІСП – до 1 год; для ПФ – до 1 год; для ІРГ (ІРД) – до 1,5 год;

$T_{\text{висув}}^{\text{ІРО}}$ – час висування інженерно-розвідувального органу для ведення ІР.

3. Час на висування інженерних розвідувальних органів до об'єктів розвідки:

$$T_{\text{висув}}^{\text{ІРО}} = \frac{L_{\text{м.вис.}}}{V_{\text{пересувІРО}}}.$$

Визначається залежно від віддалення районів зосередження інженерно-розвідувального органу до об'єктів ІР та засобів пересування, якими вони забезпечені.

4. Час на ведення ІР маршруту, об'єкта, на який прогнозується затратити найбільше часу:

$$T_{\text{м.вед}}^{\text{ip}} = \frac{L_{\text{м}}}{V_{\text{ip}}},$$

де $L_{\text{м}}$ – протяжність маршруту;

V_{ip} – темп ведення ІР інженерно-розвідувального органу: на ІРМ (БТР) – 15–20 км/год; на автомобілі – 5–10 км/год.

5. Загальна площа розвідки шляхів руху залежить від ширини дороги, включаючи узбіччя і кількості дорожніх споруд на дорогах. Час на розвідку місць розташування дорожніх споруд та шляхів руху визначається за виразами:

$$T_p = \frac{\sum S_o}{B_p}$$

$$T_p = \frac{\sum L_p}{B_p}$$

де S_o – площа дорожніх споруд на дорогах, км²;

L_p – довжина дороги, км;

B_p – нормативні можливості щодо ведення розвідки дорожніх споруд (км²/год), шляхів руху (км/год).

Бойові дії проти росії вимагають від ЗС України безперервного ведення розвідки. У більшості випадків ІР ведеться під вогневим впливом противника та при його "повітряному нагляді" за допомогою БпЛА [14]. При використанні противником БпЛА його вогневий вплив припинявся з метою отримання уявлення про характер дій нашого підрозділу ІР. Тому, для досягнення мети розвідки, дії розвідувального підрозділу завжди повинні детально плануватися та проводитися з максимальним дотриманням маскувальних заходів. При цьому

організується взаємодія з загальновійськовими підрозділами щодо вогневого прикриття дій розвідників, відволікаючих (демонстраційних) дій. Максимально враховуються погодні умови, використовуються засоби задимлення тощо. Слід зазначити, що якість проведення ІР значною мірою знижувалася через відсутність сучасних засобів розвідки: спеціальних протимінних броньованих автомобілів, портативних радіолокаційних станцій, БПЛА, сучасних дальномірів, приладів нічного бачення, біноклів, міношукачів, навігаційних апаратів типу СН-3003М та планшетів з програмованими топографічними картами.

Враховуючи досвід організації ІП БД, рекомендовано ІР спостереженням застосовувати тоді, коли об'єкт (місцевість), що проглядається, але противник не дає можливості до нього наблизитися. Її ведуть в усіх видах бойової діяльності військ безперервно. Особливо широко цей спосіб доцільно застосовувати в обороні та під час підготовки до наступу (контрнаступу). Спостереження починають з послідовного огляду місцевості і місцевих предметів справа наліво по зонах. У разі виявлення об'єкта розвідки визначають його координати, азимут і відстань від поста. Під час ведення розвідки спостереженням, також слід враховувати дані спостереження, які є у командира механізованого підрозділу, що здійснює оборону на даній ділянці, і організувати взаємодію з іншими спостережними постами, загальновійськовими, артилерійськими та іншими розвідувальними підрозділами.

Спостереження із застосуванням оптичних засобів може вестися на глибину 5-6 км [2], із застосування авіації та БПЛА для цих цілей дозволяє значно збільшити глибину спостереження в середньому у два-три рази. Тому доцільно усі інженерно-розвідувальні підрозділи забезпечити БПЛА, оснащеними сучасними приладами для ведення розвідки (засобами фото та відеофіксації), для управління якими у складі груп (постів) передбачити – оператора БПЛА.

З метою своєчасного забезпечення підрозділів розвідувальною інформацією систему спостереження слід будувати багаторівневою, а кількість ІСП постійно збільшувати.

Для ведення ІР противника і місцевості способом спостереження рекомендовано наступний склад ІСП: а) старший ІСП; б) один-два сапери-розвідники із засобами спостереження, підслуховування, пересування і зв'язку; в) 1-2 спостерігачі-оператори БПЛА, з приладами фото і відеофіксації.

Такий склад поста дозволяє організувати спостереження в заданому секторі, своєчасно зафіксувати і доповісти результати спостереження, організувати відпочинок спостерігачів. Оснащення ІСП: БПЛА з засобами ведення розвідки (приладами фото і відео фіксації), біноклями, перископами, дальномірами, компасами, годинниками (секундомірами), електричними кишеньковими ліхтариками, приладами нічного бачення, засобами зв'язку та пересування, письмовим приладдям тощо.

Досвід організації і ведення ІР спостереженням в умовах російсько-української війни свідчить про те, що її результативність багато у чому залежала від правильного вибору місця розміщення ІСП. Місце для ІСП слід обирати з таким розрахунком, щоб воно задовольняло наступним вимогам:

- а) давало можливість спостерігати за противником;
- б) забезпечувало детальний огляд у визначеному секторі;
- в) спонукало до кращого обладнання та якісного маскуванню поста;
- г) мало укриття від наземного та повітряного спостереження і вогню противника.

Під час обрання місця для розташування ІСП необхідно виходити із загального правила – "чим краще оснащення ІСП, тим більше важливих відомостей він може надати". Застосування БПЛА з засобами фото та відеофіксації дозволяло суттєво покращити можливості ІР.

Віддалення поста від противника у кожному окремому випадку залежатиме від тактичної обстановки, характеру місцевості та умов видимості. Місце, для розташування ІСП, рекомендовано обладнувати у вигляді відкритої або закритої, ретельно замаскованої споруди, зручної для розташування особового складу, приладів спостереження й захисту від ураження вогнем противника. Місце розташування ІСП повинно бути прив'язаним до найбільш характерного і стійкого орієнтира. Старший ІСП повинен визначити та довести до спостерігачів порядок обладнання місця для поста, скласти схему орієнтирів, перевірити справність засобів зв'язку, уточнити сектор спостереження, поставити завдання спостерігачам і

організувати їх роботу, визначити черговість зміни спостерігачів та доповісти про готовність до виконання завдань командирів підрозділу, від якого призначено пост. Зазвичай спостерігачам визначають сектори спостереження, які розбивають по глибині на три зони: ближню, середню і дальню. В обороні місцевості слід вивчати, починаючи з дальньої зони, а в наступі – з ближньої.

В умовах повномасштабного вторгнення армії російської федерації складність завдань покладених на класичні ІСП, викликали необхідність суттєвого підвищення їх розвідувальних можливостей, а саме сукупності кількісних та якісних показників вирішення розвідувальних завдань у визначений час і в конкретних умовах тактичної обстановки. Тому необхідно підвищувати можливості ІСП щодо ведення ІР та скорочувати час на проходження добутої інформації до кінцевого користувача. Напрямок удосконалення способів її ведення є застосування сучасних засобів розвідки (пов'язаних у єдиний комплекс), у тому числі встановлених на БПЛА. Як свідчить досвід організації ведення ІР в умовах БД, що для детального моніторингу місцевості ІСП необхідно оснащувати відеокамерою турельного типу (приладом фото- відеофіксації), яка забезпечує круговий огляд нижньої напівсфери оптичного та (або) інфрачервоного діапазону, засобами зв'язку, станцією радіолокації та навігаційною апаратурою.

Для ведення ІР з ІСП доцільно запровадити удосконалений спосіб із вертикально-горизонтальною зміною лінії спостереження. Його сутність полягає у веденні ІР не з певної точки, а з лінії спостереження, в центрі якої знаходиться сам ІСП, а її краями призначаються місця запуску БПЛА (рис. 1).

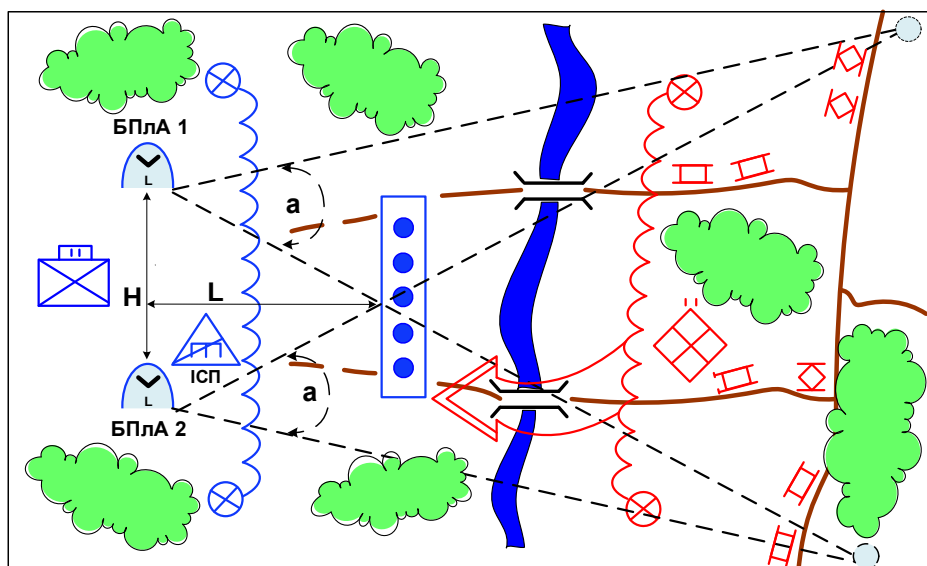


Рисунок 1 – Схема організації ведення ІР з ІСП способом вертикально-горизонтального переміщення лінії спостереження (варіант)

За таких умов довжина лінії спостереження повинна забезпечувати суцільну зону огляду (перетин полів зору оптичних приладів БПЛА) на дальності найближчих об'єктів ІР.

Для ведення розвідки запуск БПЛА слід здійснювати через нерівні проміжки часу, при цьому модуль пам'яті повинен мати можливість записати алгоритм зйомки панорами місцевості по висоті. Даний спосіб ведення ІР дозволяє не тільки своєчасно виявляти об'єкти розвідки, але й класифікувати їх, виокремлюючи із загальної маси хибні.

Під час ведення ІР з застосуванням способу вертикально-горизонтального переміщення лінії спостереження ймовірність розпізнавання об'єктів та можливості щодо їх класифікації суттєво зростають, що підтверджує його ефективність та доцільність використання органами ІР.

Оптимальний склад та оснащення ІСП для ведення розвідки із застосуванням цього способу наведено у табл. 2.

Орієнтовний склад та оснащення ІСП

Склад ІСП (чол.):		
старший (1)	розвідник-спостерігач (1)	розвідник-оператор БПЛА (2)
Оснащення ІСП (од.; к-т):		
транспортний засіб (1); БПЛА (2); прилади (комплексний прилад) спостереження, фотографування та відеофіксації координат об'єкта (1); автоматизоване робоче місце старшого поста (захищений планшет) (1); засоби зв'язку (3-4); міношукачі (2); засоби маскування (0,5-1); шанцевий інструмент (1)		

Місце для обладнання такого ІСП слід обирати між 2-ма точками старту БПЛА (див. рис. 1).

Для організації ведення ІР із застосуванням способу вертикально-горизонтального переміщення лінії спостереження, окрім звичайних питань старший поста повинен провести (рис. 2):



Рисунок 2 – Додаткові обов'язки старшого ІСП (варіант)

Особливості ведення ІР з ІСП способом вертикально-горизонтального переміщення лінії спостереження полягають у наступному:

- а) необхідність проведення точної фіксації координат посту;
- б) проведення розвідки місцевості із застосуванням приладів спостереження та БПЛА;
- в) розшифрування панорам та визначення полів невидимості, об'єктів місцевості та споруд (загороджень), що обладнує (встановлює) противник, районів зосередження його підрозділів, ОВТ, координат та відстаней до них;
- г) виокремлення об'єктів, які потребують уточнення (до розвідування);
- д) організація роботи посту згідно з доведеним алгоритмом дій, розшифрування матеріалів фото- та відеофіксації, що передбачає порівняння зображень, рознесених за часом, та визначення змін у секторі спостереження;
- е) складання донесення та доповідь старшому начальнику.

Завершення ведення розвідувальної діяльності ІСП повинно здійснюватися у призначений заздалегідь час, з початком БД або за вказівкою старшого начальника.

Наступним способом ведення ІР є безпосередній огляд, який застосовується у випадку, коли є можливість наблизитись до об'єкту, що розвідується, обстежити його і провести необхідні виміри. Найбільший ефект дає поєднання безпосереднього огляду і фото- та відеофіксації.

Сучасна збройна боротьба характеризується широкими можливостями впливу між протиборчими сторонами на мобільність військ (сил). За період ведення БД на території нашої держави чітко проглядається беззаперечний факт, що питання забезпечення пересування

військ (сил) набуває вагомості та невідкладності його вирішення. Водночас, діяльність російських військ спрямована на масштабне руйнування дорожньої інфраструктури основу якої складають постійні мости та переходи через перешкоди, а у поєднанні з впливом місцевості, значно послаблюють маневрові можливості підрозділів сил оборони [1].

Слід зазначити, що тільки на початковому етапі ведення повномасштабних бойових дій, загарбниками було знищено близько 300 мостів і шляхопроводів та 24 тис. км доріг, що завдало втрат економіці України орієнтовно 31,6 млрд. доларів США. Більшість із цих об'єктів, особливо мости – стратегічно важливі артерії у своїх регіонах та громадах, втрата (знищення) яких змушувала переорієнтовувати логістичні та евакуаційні ланцюжки [3].

Виходячи із зазначеного, першочерговим етапом, який проводиться перед ІР безпосереднім оглядом є: вибір напрямків (маршрутів) на топографічних (цифрових) картах з урахуванням наявності, напрямлення і стану існуючих доріг, характеру місцевості, природних умов, маскувальних можливостей, бойової обстановки (ймовірності дій противника), очікуваної інтенсивності руху військ, пори року і погоди та ін.

Удосконаленням даного способу є також застосування БпЛА в інтересах розвідувального органу [3]. На рис. 3 показано варіант організації ведення ІР безпосереднім оглядом із застосуванням тактичного БпЛА поля бою, який дозволяє здійснювати моніторинг маршруту руху, важливих об'єктів тощо.

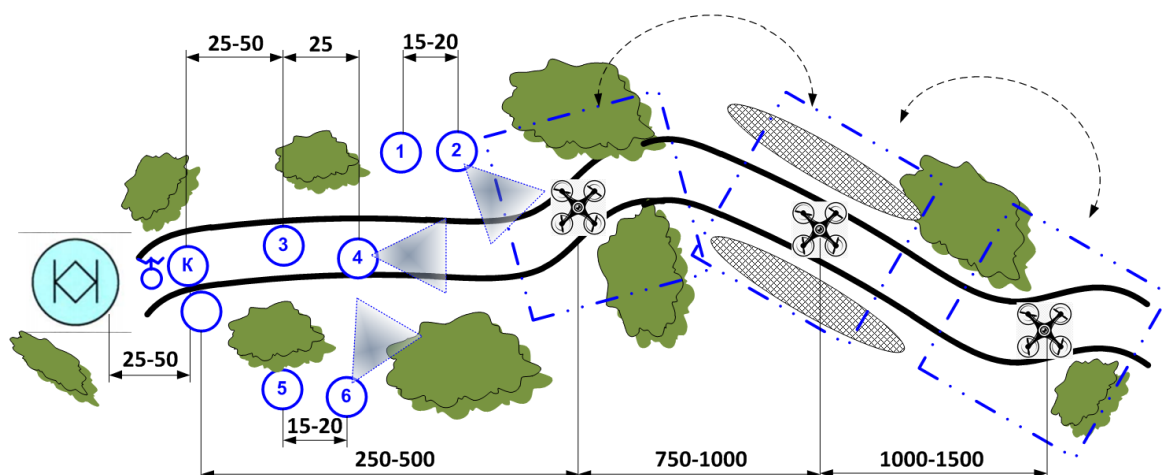


Рисунок 3 – Схема організації ведення ІР безпосереднім оглядом із застосуванням тактичного БпЛА поля бою (відстані у метрах) (варіант)

З метою ефективного моніторингу місцевості орган ІР доцільно оснащувати розвідувальною машиною на гусеничній або на колісній броньованій базі з розміщенням на її борту комплексу БпЛА класу "тактичні поля бою" з наступними основними характеристиками: маса – до 50 кг; висота польоту – до 3 км; дальність застосування (радіус управління) – до 40 км; тривалість перебування в повітрі – 8–10 годин; кількість одночасно пілотованих літальних апаратів 2 од.; можливість управління з землі та з борту машини; цільове навантаження – відеокамера, тепловізійна камера, навігатор, розрахований на використання системи GPS [3].

При цьому рекомендовано дотримуватись темпу ведення ІР із урахуванням умов наведених у табл. 3. [2, 3].

Умови та темпові показники у ході ведення ІР безпосереднім оглядом

Умови ведення ІР	Показник (км/год.)
грунтова дорога, сильно пошкоджене шосе з асфальтовим (бетонним) покриттям	1...3
дороги, де необхідна перевірка окремих підозрілих місць (ям, вибоїн, вирв) та узбіч	5...6
колонні шляхи, в умовах обмеженого часу, коли дії ІРД в пішому порядку неможливі, обов'язковим є застосування танка з колійним мінним тралом або БМР під прикриттям генератора перешкод	10...12

Серед існуючих наземних способів дій розвідувальних органів з ведення ІР шляхів пересування військ (окремих об'єктів місцевості), одним із найбільш ефективним є так званий метод "ПІДКОВА", застосування якого дозволяє не тільки виявляти, а й знешкоджувати більшість типів мін та фугасів [2, 3, 5, 15].

Сутність даного методу полягає в тому, що ІРД з бойовою охороною діє трьома групами: основна з пересувається дорогою з метою перевірки на наявність протитанкових мін, фугасів, керованих по радіо та із замикачами, а також протипіхотних вибухових пристроїв направленої дії, керованих по радіо. Дві допоміжні групи рухаються вздовж дороги ліворуч і праворуч на відстані 30...50 м від неї і попереду основної групи на відстані 50...60 м від неї з метою своєчасного виявлення лінії керування фугасами. Групи повинні знаходитися в зоні дії генератора перешкод та передатчиків перешкод, що переносяться. Дії усіх трьох груп постійно прикриваються бойовою охороною [1 - 3, 5].

Поряд з цим, і він непозбавлений недоліків, основними з яких є: залучення значної кількості особового складу та недостатня забезпеченість ефективними технічними інженерно-розвідувальними засобами для виконання завдань.

У цих умовах необхідно проводити ретельну ІР шляхів пересування військ із застосуванням органів ІР, способи яких вже не можуть базуватися на старих прийомах і повинні мати "об'єднувальний характер" повітряно-наземних способів.

Досвід організації ІІ БД свідчить про те, що безпосередній огляд найчастіше застосовували ІРД для ведення розвідки загороджень, перешкод, доріг, гідротехнічних споруд і інших об'єктів. Для отримання своєчасної та достовірної інформації про стан шляхів пересування, об'єктів необхідно застосовувати комплексний спосіб ведення ІР ІРД з використанням БПЛА (рис. 4).

Під час реалізації комплексного способу ведення ІР данні фото- та відеофіксації про об'єкти, маршрути висування, небезпечні та закриті ділянки на них та інші дані, що отримані за допомогою БПЛА, узагальнюються ІРД та доповідаються старшому начальнику.

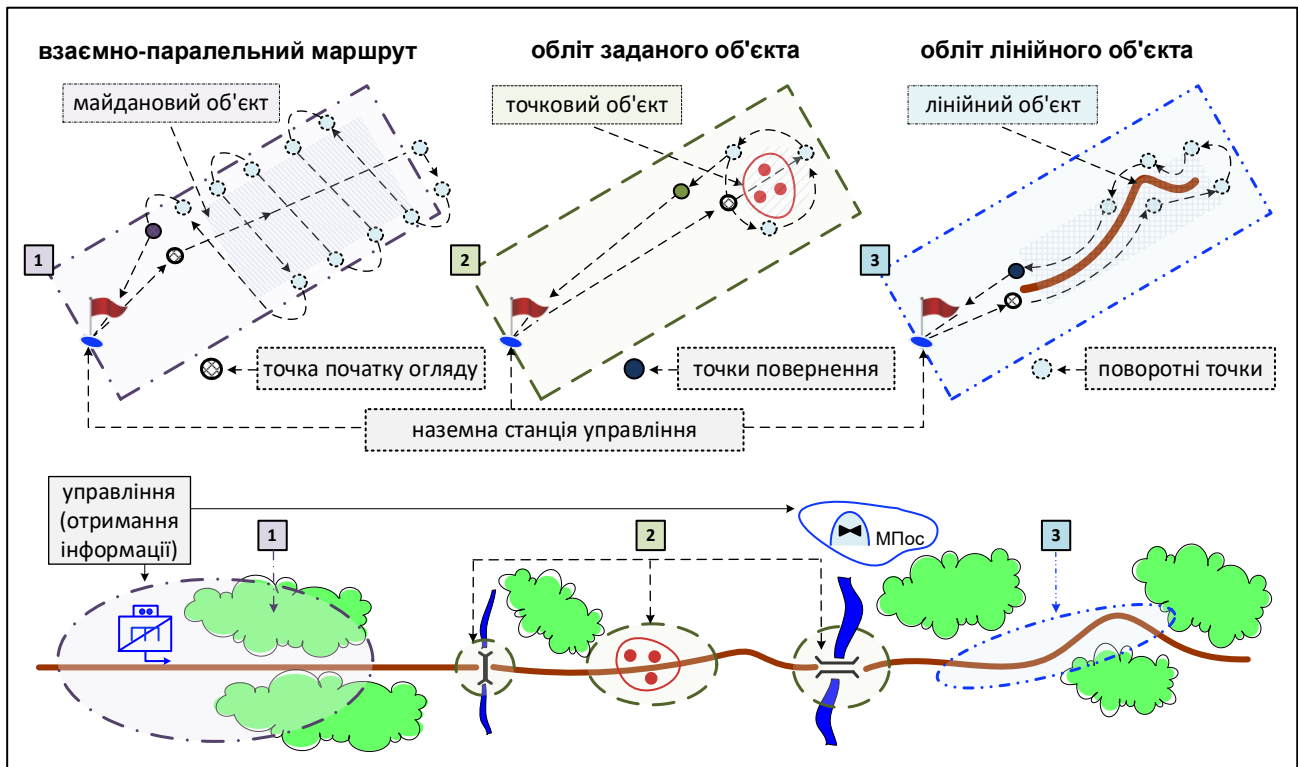


Рисунок 4 – Схема організації ведення інженерної розвідки комплексним способом (варіант)

Запуск БПЛА слід здійснюється з наземної станції керування, винесеної до маршруту, що розвішується, з таким розрахунком, щоб у будь-якій точці розвідки дальність зв'язку забезпечувалася не менше ніж на – 80 % або прилади зв'язку перебували на рухомому засобі.

Під час застосування комплексного способу, ІРД матиме наступний склад сил і засобів, що наведено у табл. 4.

Таблиця 4

Орієнтовний склад та оснащення ІРД

Склад ІРД (чол.):		
командир розрахунку (1)	сапер-розвідник (1)	розвідник (1)
водій (механік-водій) (1)	оператор та помічник БПЛА (по 2)	
Оснащення ІРД (од.; к-т):		
транспортний засіб (1); БПЛА (2); прилади (комплексний прилад) спостереження, фотографування та фіксації координат об'єкта (1); автоматизоване робоче місце командира ІРД (захищений планшет) (1); засоби зв'язку (4-6); засобами пошуку радіоліній (1); міношукачі (2); засоби маскування (0,5-1); шанцевий інструмент (1)		

У ході ведення ІР на маршруті командир ІРД повинен уточнити оператору БПЛА об'єкти, інформацію якої потребує вищий штаб, а також визначає способи ведення спостереження за ними, необхідні кути огляду для прийняття рішення на дорозвідування, небезпечні ділянки шляху, та інші ознаки, що можуть знизити темпи руху військ.

Час доповіді про результати ІР повинен визначити старший начальник. При виявленні противника, засідок, МВЗ, перешкод, руйнувань на маршруті, що розвідується, які впливають на темпи руху військ, проводиться негайна доповідь та організується пошук шляхів обходу.

Ведення ІР з застосуванням БПЛА (див. рис. 4) дозволить за рахунок збільшення висоти лінії спостереження суттєво скоротити час на обстеження як окремих об'єктів, так і визначених районів, своєчасно виявляти зміни в оточуючому середовищі викликані впливом противника (удари авіації, артилерії, дистанційно встановленні мінні поля тощо) або надзвичайні ситуації (руйнування важливих об'єктів, затоплення) та безперервно здійснювати

моніторинг визначеного району і дій противника, що можуть вплинути на маневр своїх військ у ході ведення оборони.

Як було відзначено раніше, з метою ведення ІР противника місцевості та об'єктів в інтересах ІІ ведення БД силами оборони призначалися ІРД. Склад і оснащення ІРД залежав від поставленого завдання, тактичної обстановки, що склалася та визначався у кожному конкретному випадку начальником інженерної служби (інженером-радником) або командиром підрозділу, що вислав дозор.

Отже, системне включення до складу інженерно-розвідувального органу БПЛА та інших сучасних засобів наданих, як країнами-партнерами, так волонтерськими організаціями в якості військово-технічної допомоги, збільшувало якість і швидкість виконання завдань, особливо коли потребувало вирішення проблем, пов'язаних з доступом до важкодоступних або небезпечних місць. Тому, у табл. 5, на основі проведеної експертної оцінки, було встановлено значення поправочного коефіцієнта при визначенні часу на ведення ІР $T_{\text{вед}}^{\text{ІР}}$ з урахуванням можливостей БПЛА.

ІР пошуком застосовувалась для отримання точних відомостей про характер оборони противника та місцевості як на його передньому краї, так і у глибині, а також для захоплення полонених, документів, зразків озброєння та спостереження.

Як правило, пошук здійснювали інженерні підрозділи (відділення, взвод), які були спеціально озброєні, оснащені та підготовлені до виконання завдань в умовах можливого зіткнення з противником. З особовим складом підрозділу виділеним для ведення розвідки пошуком, попередньо проводились тренувальні заняття для відпрацювання порядку проведення пошуку, а також усіх питань взаємодії з підрозділами, що його підтримували. Уся підготовка до майбутніх дій проводилась приховано.

Таблиця 5

Значення поправочного коефіцієнта

Назва об'єкта ІР	Ступінь деталізації обстеження	Значення
Гідротехнічні споруди:		
регуляційні	низька	0,8...0,85
дренажні	середня	0,85...0,9
водовідвідні	середня	0,85...0,9
водопропускні	висока	0,9...0,95
Шляхи руху військ (сил):		
автомобільні дороги оборонного значення	середня	0,85...0,9
військово-автомобільні дороги	висока	0,9...0,95
колонні та інші шляхи	висока	0,9...0,95
Територія (зона):		
ведення БД (непідконтрольна)	висока	0,9...0,95
нейтральна "сіра"	середня	0,85...0,9
підконтрольна	низька	0,8...0,85

Враховуючи сучасні та перспективні напрямки розвитку способів ведення ІР, що базуються на широкому застосуванні БПЛА [3, 7–13], можливостях вітчизняних та зарубіжних засобів інженерного озброєння призначених для вирішення розвідувальних завдань, а також з огляду на виконання завдань підрозділами збройних сил країн-членів НАТО, перспективний склад інженерно-розвідувального органу для здійснення пошуку (огляду) показано на рис. 5.

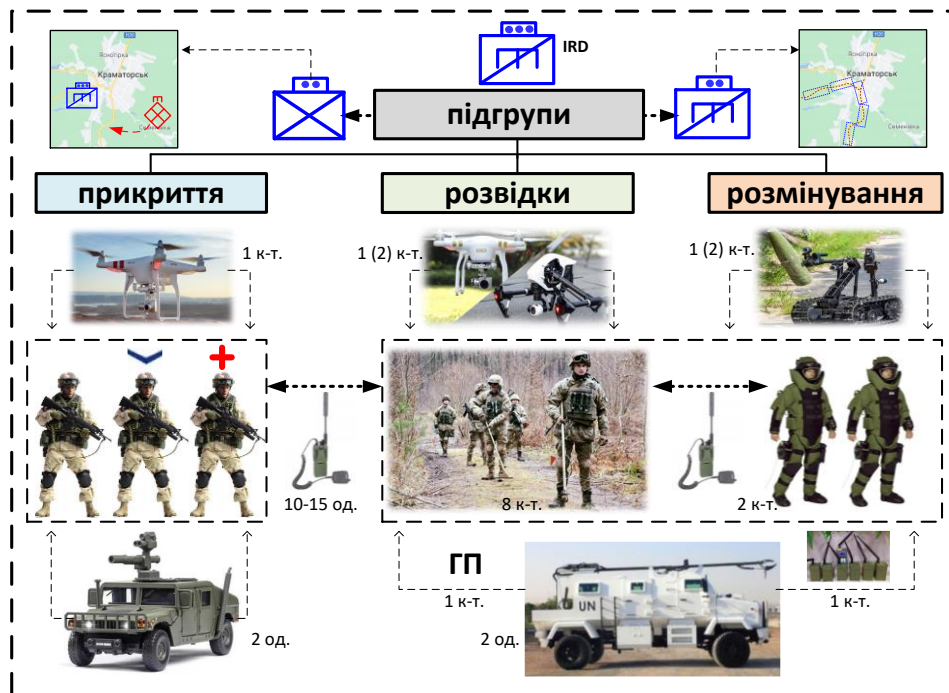


Рисунок 5 – Перспективний склад інженерно-розвідувального органу (варіант)

Необхідно також відзначити, що крім літальних апаратів, широкого застосування набувають й наземні роботизовані комплекси, які дозволять наблизитись до противника, добути і передати інформацію в умовах реального часу, що призведе до зменшення залучення і, що найважливіше, уникнення втрат особового складу.

Таким чином, реалізація запропонованих пропозицій може призвести до збільшення темпових показників ведення ІР, скорочення термінів отримання розвідувальних даних, створення резерву часу на прийняття командирами (штабами) обґрунтованих рішень і своєчасного реагування на раптово виникаючі зміни тактичної обстановки у ході підготовки та ведення БД.

Висновки. Виходячи з переліку завдань (заходів) і набутого бойового досвіду інженерних військ ЗС України, орган ІР формується у першу чергу з метою пошуку, знищення (знешкодження) загороджень на шляхах руху військ і ділянках місцевості, до складу якого неодмінно входить до двох інженерно-саперних відділень, посиленого кінологічним розрахунком мінно-розшукової служби та оснащеного засобами розвідки і розмінування, зв'язку, БПЛА, генераторами перешкод, вибуховими речовинами та засобами підривання, індивідуальним бронезахистом та укомплектованим транспортним засобом.

Існуючі способи ведення ІР мають базуватися на раціональному поєднанні їх з перспективними підходами. Основним чинником для змін є наявність новітніх засобів для ведення ІР, розвиток яких відбуватиметься у напрямку роботизації процесів з урахуванням широких можливостей ведення контрміної боротьби, що визначатиме технічний рівень та оснащеність розвідувальних підрозділів.

Отже, сучасними шляхами удосконалення ведення ІР є поєднання повітряно-наземних способів, які ґрунтуватимуться на використанні можливостей сучасних безпілотних систем, до яких відносяться: БПЛА, наземні роботизовані комплекси та ін.

ЛІТЕРАТУРА:

1. Фтемов Ю. О. Рекомендації з прикриття міжпозиційного простору із урахуванням заходів завчасної підготовки території до оборони. *Системи озброєння і військова техніка*. 2020. № 4(64). С. 43-48. <https://doi.org/10.30748/soivt.2020.64.05>. (дата звернення: 17.09.2023).
2. Організація виконання завдань частинами і підрозділами інженерних військ Збройних Сил України. Частина I. Основи інженерного забезпечення. Інженерна розвідка : навч. посібник / Мілютін В.А. та ін. Львів : НАСВ ЗС України, 2014. 142 с.

3. Фтемов Ю. О. Обґрунтування складу комплексу технічних засобів інженерної розвідки шляхів руху військ (сил). *Системи озброєння і військова техніка*. 2021. № 3(67). С. 45-51. <https://doi.org/10.30748/soivt.2021.67.06>. (дата звернення: 17.09.2023).
4. Лупандін В.А., Мегельбей Г.В., Мацько О.Й., Куртсеїтов Т.Л., Міроненко П.О. Основні тенденції створення та застосування груп безпілотних літальних апаратів. *Наука і техніка Повітряних Сил Збройних Сил України*. 2019. № 2(35). С. 88-96. <https://doi.org/10.30748/nitps.2019.35.11>. (дата звернення: 17.09.2023).
5. Інженерне забезпечення бою в сучасних операціях : навч. посібник / Нещадин О.В. та ін. Львів : НАСВ ЗС України, 2017. 320 с.
6. Панов В.Г., Ситнік О.В. Методичний підхід до оцінки системи добування та обробки розвідувальної інформації з інженерної обстановки. *Збірник наукових праць Національної академії Державної прикордонної служби України*. 2013. № 2(60). С. 164-169. http://nbuv.gov.ua/UJRN/znpnapv_vtn_2013_2_19. (дата звернення: 17.09.2023).
7. Конотопець М., Черевко Р. Аналіз функціонування системи управління інженерним забезпеченням в операціях, проблеми та шляхи їх вирішення. *Social development & Security*. 2018. № 1 (3). С. 37 – 44. URL: <https://paperssds.eu/index.php/JSPSDS/article/view/26/24>. (дата звернення: 17.09.2023).
8. Мирончук Ю.А., Оверчук С.П. Методика підготовки і планування повітряної розвідки на оперативно-тактичну глибину з використанням БПЛА. *Військово-технічний збірник*, 2019. № 21. С. 44-52. <https://doi.org/10.33577/2312-4458.21.2019.44-52>. (дата звернення: 17.09.2023).
9. Коцюрuba В.І., Цибуля С.А., Рибалко В.В. Обґрунтування доцільності використання способу повітряної розвідки районів інтенсивного застосування мінної зброї. *Social development & Security*. 2019. № 9(1). С. 60-68. <https://paperssds.eu/index.php/JSPSDS/article/view/88/85>. (дата звернення: 17.09.2023).
10. Майстренко О.В., Бурдейний М.В., Стегура С.І., Стеців С.В. Визначення координат наземних цілей з використанням малогабаритних БПЛА на основі вдосконаленого псевдодальномірного методу. *Військово-технічний збірник*, 2020. № 22, 43-47. <https://doi.org/10.33577/2312-4458.22.2020.4-47>. (дата звернення: 17.09.2023).
11. Кучеренко Ю. Ф., Науменко М.В., Кузнєцова М.Ю. Аналіз досвіду застосування безпілотних літальних апаратів та визначення напрямку їх подальшого розвитку при веденні мережецентричних операцій. *Системи озброєння і військова техніка*. 2018. № 1(53). С. 25-30. <https://doi.org/10.30748/soivt.2018.53.03>. (дата звернення: 17.09.2023).
12. Павленко М.А., Тіхонов І.М., Нікіфоров І.А. Рекомендації щодо ефективного використання ударних безпілотних літальних апаратів в операції Об'єднаних сил. *Наука і техніка Повітряних Сил Збройних Сил України*. 2021. № 1(42). С. 131-36. <https://doi.org/10.30748/nitps.2021.42.17>. (дата звернення: 17.09.2023).
13. Іващук Б.М., Павлуша Ю.Г., Іващук Л.А. Аналіз основних параметрів безпілотних авіаційних комплексів тактичного класу щодо ведення повітряної розвідки. *Системи озброєння і військова техніка*. 2021. № 2(66). С. 17-22. <https://doi.org/10.30748/soivt.2021.66.02>. (дата звернення: 17.09.2023).
14. Олексенко О. О., Авраменко О. В., Федоров А. В., Сніцаренко В. В., Чернавїна О. Є. Застосування безпілотних літальних апаратів збройними силами Російської Федерації у війні проти України. *Наука і техніка Повітряних Сил Збройних Сил України*. 2022. № 4 (49). С. 37-42. <https://doi.org/10.30748/nitps.2022.49.05>. (дата звернення: 17.09.2023).
15. Нероба В.Р. Роль мінної зброї в сучасних війнах і прикордонних конфліктах. *Збірник наукових праць Національної академії Державної прикордонної служби України*. 2019. № 81(3). С. 155-171. <https://doi.org/10.32453/3.v81i3.444>. (дата звернення: 17.09.2023).

REFERENCES:

1. Ftemov Y. (2020). Recommendations for covering the interpositional space, taking into account measures for early preparation of the territory for defense. *Weapon systems and military equipment*, 4 (64). p. 43-48. <https://doi.org/10.30748/soivt.2020.64.05>. [in Ukrainian].
2. Organization of the execution of tasks by parts and units of engineering troops of the Armed Forces of Ukraine. Part I. Fundamentals of engineering support. Engineering exploration : education manual / Milyutin V.A. etc. Lviv : NASV of the Armed Forces of Ukraine, 2014. 142 p. [in Ukrainian].

3. Ftemov Y. (2021). Justification of the set of technical means for engineering reconnaissance of troops (forces). *Weapon systems and military equipment*, 3 (67). p. 45-51. <https://doi.org/10.30748/soivt.2021.67.06>. [in Ukrainian].
4. Lupandin V., Megelbey G., Matsko O., Kurtseitov T., Mironenko P. (2019). The main trends of the development and application of a unmanned aerial vehicle groups. *Science and technology of the Air Force of the Armed Forces of Ukraine*, № 2 (35). p. 88-96. <https://doi.org/10.30748/nitps.2019.35.11>. [in Ukrainian].
5. Combat engineering support in modern operations: education manual / Neshchadin O.V. etc. Lviv : NASV of the Armed Forces of Ukraine, 2017. 320 p. [in Ukrainian].
6. Panov V., Sytnik O. (2013). Methodical approach to the evaluation of the system of extraction and processing of intelligence information on engineering environment. *Collection of scientific works of the National Academy of the State Border Service of Ukraine*, № 2 (60). p. 164-169. http://nbuv.gov.ua/UJRN/znpnapv_vtn_2013_2_19. [in Ukrainian].
7. Konotopets M., Cherevko R. (2018) Analiz funktsionuvannya systemy upravlinnya polem boyu inzhenernoho zabezpechennya operatsiyi, problemy ta shlyakhy yoho vyrishennya [Analysis of the functioning of battlefield control system of engineering support of an operation, problems and ways of its solution]. *Social development & Security*, 1 (3), p. 37-44. DOI: <http://doi.org/10.5281/zenodo.1183896> [in Ukrainian].
8. Myronchuk, Y., & Overchuk, S. (2019). Methodology of the preparation and planning the aerial reconnaissance of the operational-tactical depth with using the unmanned aircraft. *Military Technical Collection*, 21, p. 44-52. <https://doi.org/10.33577/2312-4458.21.2019.44-52>. [in Ukrainian].
9. Kotsyuruba V., Tsybulia S., Rybalko V. (2019). Obgruntuvannya dotsil'nosti vykorystannya sposobu povitryanoyi rozvidky rayoniv intensyvnoho zastosuvannya minnoyi zbroyi [Justification of the using of the method of air reconnaissance of area of intensive application of mine weapons]. *Social development & Security*, 9 (1), 60–68. DOI: <http://doi.org/10.33445/sds.2019.9.1.5>. [in Ukrainian].
10. Maistrenko O., Burdeinyi M., Stehura, S., Stetsiv, S. (2020). Determination of coordinates of terrestrial targets with the use of small UAVs on the basis of an improved pseudolongdimensional method. *Military Technical Collection*, 22. p. 43-47. <https://doi.org/10.33577/2312-4458.22.2020.43-47>. [in Ukrainian].
11. Kucherenko Y., Naumenko M., Kuznetsova M. (2018). Analysis experience use unbeatural vehicle apparatus and determination their further development during conduct netset central operations. *Weapon systems and military equipment*, 1 (53). p. 25-30. <https://doi.org/10.30748/soivt.2018.53.03>. [in Ukrainian].
12. Pavlenko M., Tykhonov Y., Nykyforov Y. (2021). Recommendations for the efficient use of unmanned aerial vehicles in Joint Forces Operation. *Science and technology of the Air Force of the Armed Forces of Ukraine*, 1 (42). p. 131-36. <https://doi.org/10.30748/nitps.2021.42.17>. [in Ukrainian].
13. Ivashchuk B., Pavlusha Y., Ivashchuk L. (2021). Research possibilities of tactical class air intelligence of unmanned aerial vehicles. *Weapon systems and military equipment*, 2 (66). p. 17-22. <https://doi.org/10.30748/soivt.2021.66.02>. [in Ukrainian].
14. Oleksenko O., Avramenko O., Fedorov A., Snitsarenko V., Chernavina O. (2022). Use of unmanned aerial vehicles by the armed forces of the Russian Federation in the war against Ukraine. *Science and technology of the Air Force of the Armed Forces of Ukraine*, 4 (49). p. 37-42. <https://doi.org/10.30748/nitps.2022.49.05>. [in Ukrainian].
15. Neroba V. (2019). The role of mine weapons in modern wars and border conflicts. *Collection of scientific works of the National Academy of the State Border Service of Ukraine*, 81 (3). p. 155-171. <https://doi.org/10.32453/3.v81i3.444>. [in Ukrainian].

**Ph.D. Ftemov Y., D.Sci.Tech. Kuprinenko O., Prof. Lienkov S. V.
Ph.D. Miroshnichenko O. V. , Ph.D Litvinenko N. I.**

IMPROVEMENT OF METHODS OF CONDUCTING ENGINEERING RECONNAISSANCE IN THE INTERESTS OF ENGINEERING SUPPORT OF COMBAT OPERATIONS OF TROOPS (FORCES)

The experience of the Russian-Ukrainian war shows that with the rather large spatial and temporal indicators of combat operations, the volume of one of the main measures of engineering support - engineering reconnaissance - increases, which in turn leads to an excess of the required time and the need to attract a significant amount of resources for its implementation.

To resolve this discrepancy, it is necessary to envisage not only the strengthening of forces and means and their rational distribution, but also the choice of the most effective ways to accomplish the tasks. Neglect of engineering support tasks (measures) always leads to unjustified losses in personnel, weapons and military equipment.

The purpose of the study is to find new, more advanced ways of conducting engineering reconnaissance, to reveal the role, risks, advantages and disadvantages, and to analyze the possibility of their integration into the practice of engineering troops.

The main task was to determine the effectiveness of methods of performing engineering intelligence tasks, the composition of equipment of engineering intelligence bodies, taking into account the capabilities of modern technical means. The tasks of engineering reconnaissance in the main types of combat (operations) and at different levels, which involve units of engineering troops, are analyzed. It is established that the proposed methods of conducting engineering reconnaissance will lead to a sharp change in the conditions of its conduct and reduce the time for the implementation of reconnaissance activities by engineering units at individual sites. The role, place and influence of unmanned aerial vehicles of various types used by the defense forces in the course of combat missions are studied and it is established that the most effective methods, both in the course of defensive and offensive combat (operation), are combined air-ground.

The implementation of the proposed methods of engineering intelligence contributes to the improvement of such key indicators as efficiency and reliability. command and control bodies and troops (forces) compared to traditional approaches.

The main direction of further research should be directed to the development of various methods of conducting engineering reconnaissance, taking into account trends in the direction of robotization of processes to improve the capabilities of mine action.

Keywords: engineering support, engineering intelligence, methods, engineering measures, unmanned aerial vehicles.

AUTOMATED INVOICE PROCESSING SYSTEM BASED ON RPA TECHNOLOGIES

Abstract: *The options for improving invoice processing using RPA (Robotic Process Automation) technology are covered in this article. The significance of the subject and the goal of the study are explained in the introduction. The study's major goal is to organize and analyze how robotic invoice processing (RPA) affects the invoice processing process. In the context of streamlining financial procedures, businesses today struggle with the issue of automated invoice processing (RPA). The study looks at this technology's application to processing invoices.*

The study's objective was to gather and examine data regarding the advantages and possibilities of employing robotic invoice processing (RPA) to streamline invoice processing. We paid specific attention to factors like improved accuracy and error avoidance, resource optimization and cost reduction, compliance and fraud risk reduction, greater profitability, and technology interoperability.

The article's primary goals are to examine the fundamental concepts and capabilities of robotic process automation (RPA) in the context of processing invoices; to research the approaches for implementing RPA in this process and evaluate how it affects efficiency and accuracy of operations; to think about potential future applications for RPA in this field; and to identify potential trends in the advancement of this technology. These goals are designed to offer a complete investigation and evaluation of robotic process automation (RPA) technology with regard to its influence on how it improves invoice processing in commercial environments.

One of the techniques utilized in the article is to examine the advantages and power of RPA in the context of processing invoices. The investigation' findings demonstrate that RPA technology has greatly enhanced invoice processing. Routine procedures can be automated with RPA, which lowers risks and boosts productivity. This technology is providing new chances for businesses across numerous industries.

Overall, the study demonstrates that robotic invoice processing (RPA) is a useful tool for improving the speed and accuracy of financial transactions, optimizing the processing of invoices, and helping the creation of business plans in the current fast-paced corporate environment.

Problem statement. Modern companies face an extremely large number of invoices and financial documents that have to be processed. These can be invoices for services, goods, payments to employees, tax returns, bank transactions, and others. Sending, receiving, verifying, processing and archiving these documents requires a huge amount of effort and time, especially if it is done by humans.

The traditional process of manual invoice processing is associated with high costs. These include staff salaries, time, and infrastructure organization. In addition, the human factor can lead to mistakes and inaccuracies in processing, which further can lead to losses and problems for companies.

Today's business rapidly changing environment demands speed and accuracy in all areas of business. Invoice processing is not an exception. Companies need to analyze and process invoices quickly, monitor financial flows, and make immediate decisions based on the data that is present in the document. The faster and more accurate invoice processing is, the more efficiently a business operates and the more sustainable and competitive it is in the marketplace.

The efficiency of invoice processing in turn affects the overall productivity and success of the business. Given these challenges, there is a need to improve invoice processing and implement effective technologies, such as RPA, to optimize this critical business process.

Overview of existing solutions and recent research. Nowadays, there are several main methods of processing invoices such as manual processing, the use of software to automate processing, and the implementation of artificial intelligence technologies, especially RPA. Due to

the fact that manual processing is time, labor, and resource-intensive and therefore unnecessarily expensive for businesses with numerous invoices.

RPA technology is a dynamically developing tool for optimizing business processes, including invoice processing. This technology lets software bots automate repetitive tasks that were previously performed by humans. This can include receiving and analyzing invoices, entering data into accounting systems, automatically generating reports, and other financial operations.

Many companies are already been successfully implementing RPA to optimize invoice processing. For instance, financial services companies use RPA to automate accounting and control financial transactions. In such a way, this technology can significantly increase the speed and accuracy of invoice processing, reduce mistakes, and optimize business processes overall.

Implementation of RPA to invoice processing. RPA technology has great potential to optimize and automate invoice processing in modern business environments. Here are a few steps on how RPA can be used for the automation of this business process:

1. Data receiving.

RPA can automatically monitor and retrieve invoices from many sources such as emails, payment platforms, or web portals. The software bot can identify, and collect data from invoices and filter them by type, date, and amount.

2. Data verification.

RPA bot can automatically verify the accuracy of invoice data and compare it to a company's internal databases. This may include comparing the amount on the invoice to the expected value, checking tax values, and other operations.

3. Data input into the accounting system.

RPA bot can automatically input received and verified data into the accounting system or any other application or web service which are dedicated to this reason. This process can help avoid the need for manual data entry and reduces the possibility of mistakes.

4. Reporting and analytics.

Software bots are able to generate different reports which are based on processed invoices. This will help companies quickly analyze financial flows and make management decisions.

5. Document flow management.

Using RPA for invoice processing lets businesses save time and resources, avoid human mistakes, and increase the efficiency and speed of financial information processing, which is a significant point for effective financial management and the success of a business.

Cross-industry benefits of RPA. RPA provides multiple cross-industry benefits. In the case of invoice processing, it specifically brings the following advantages:

1. Removal of geographical and time constraints.

The use of RPA allows businesses to operate 24/7 because software bots are not limited by location and time. This is especially important for worldwide companies that have operations in different parts of the world.

2. Compatibility with other systems and technologies.

RPA can be easily integrated with existing different systems and other informational technologies such as artificial intelligence, machine learning, and data analytics. This improves the ability for optimization and implementation of complex solutions for better management of financial and business processes. Taking into account these advantages, implementing RPA technology is a promising and effective solution for various business sectors to help increase productivity, reduce costs, and improve the quality of financial information processing.

3. Reducing Fraud Risk.

RPA can significantly reduce the risk of financial fraud and deception. Automated processes record and monitor transactions and notice any irregularities or suspicious transactions. This can help companies to respond quickly and prevent fraud by ensuring the security of financial data and transactions.

4. Compliance with Requirements.

Compliance with standards and requirements is mandatory nowadays in the business environment. With the help of RPA, companies will be able to automate various business processes, ensuring data accuracy and compliance with established standards and regulations.

5. Return on investment.

RPA implementation helps improve the efficiency of operations that leads to more efficient use of resources and increased profitability. Optimizing business processes for invoice processing saves time and money that can be dedicated to more strategic goals of business development and attract new investment.

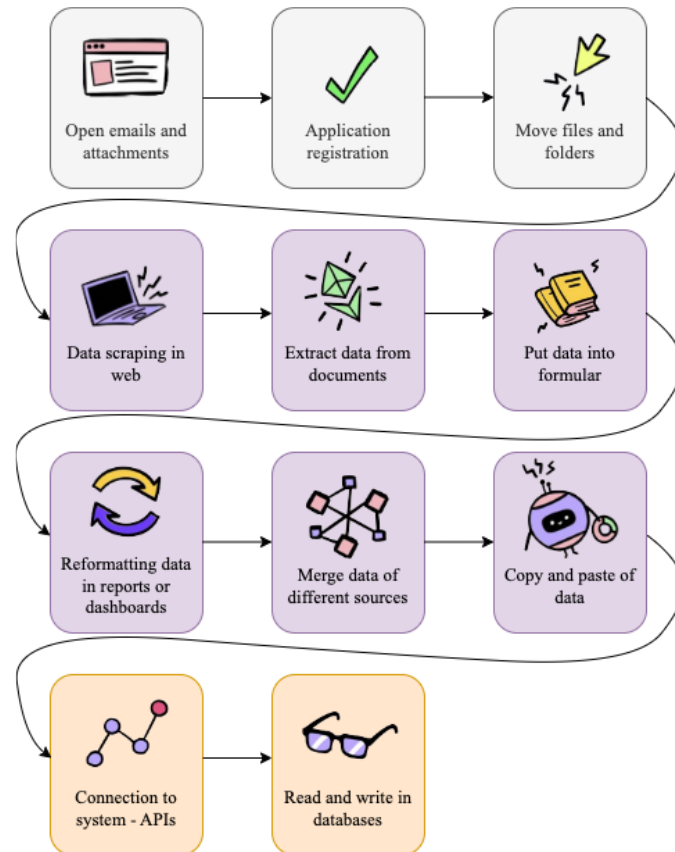


Figure - 1. Steps of document processing

Conclusions. The implementation of RPA technology into invoice processing opens up a wide range of perspectives for businesses in different areas. Software bots are programmed to perform actions according to specific business processes to get rid of monotonous and time-consuming tasks. This approach helps to increase work efficiency and significantly reduces the risk of human mistakes.

It is important to note that RPA does not only automate the processing of invoices, but also ensures their compliance with some set of and requirements. This is a key aspect in finance and accounting area, where data accuracy and regulatory compliance are critical points.

In addition, the use of RPA in invoice processing allows you to optimize costs and allocate corporate resources with maximum efficiency. This will help to increase profitability and bring new investments in the business.

After analysis, it is obvious that the use of RPA in invoice processing is an urgent need for companies in today's competitive business environment. This technology is getting a key tool to increase the level of efficiency and competitiveness, especially in the finance and accounting areas. The implementation of RPA in these areas will not only save businesses time and resources, but will also set high quality and reliability in the processing of financial information, which is an important factor in the successful operation and development of a business.

REFERENCES:

1. Asatiani, A., Penttinen, E.: Turning robotic process automation into commercial success – case OpusCapita. J. Inf. Technol. Teach. Cases 6, 2016, p. 67–74
2. Aguirre S., Rodriguez A. Automation of a business process using robotic process automation (RPA): Appl Comput Sci Eng Commun Comput, 2017.
3. Madakam S., Holmukhe R.M., Jaiswal D.K. The future digital work force: robotic process automation (RPA) JISTEM-Journal of Information Systems and Technology Management, 2019.
4. Van der Aalst, W.M.P, Bichler, M., Heinzl, A., Robotic Process Automation, Business and Information Systems Engineering 3, 2018, p. 1-4.
5. Nandan M., Arun Kumar A., Pobotic Process Automation Projects. Packt Publishing, 2020.
6. Hofmann, Peter, Samp, Caroline and Urbach, Nils, Robotic process automation, Electronic Markets, 30, 2020, p. 99-106.
7. Lacity, M., Willcocks, L.: What knowledge workers stand to gain from automation. Harvard Bus. Rev, 2015.
8. Fung, H.P.: Criteria, use cases and effects of information technology process automation. Adv. Robot. Autom. 3, 2014, p. 1–11.
9. Alok Mani Tripathi., Learning Robotic Process Automation. Packt Publishing., 2018.
10. Tansel Kaya C., Turkeyilmaz M., Birol B., Impact of RPA Technologies on Accounting Systems, Muhasebe ve Finansman Dergisi, 2019.

к.т.н. Батрак Є.О., к.т.н. Цьопа Н.В., Трояновська А.О.

АВТОМАТИЗОВАНА СИСТЕМА ОБРОБКИ РАХУНКІВ НА ОСНОВІ RPA-ТЕХНОЛОГІЙ

Анотація: У цій статті розглядаються варіанти оптимізації обробки рахунків за допомогою технології RPA (Robotic Process Automation). Вступ пояснює актуальність теми та мету дослідження. Основна мета дослідження полягає в систематизації та дослідженні впливу роботизованого процесу обробки рахунків (RPA) на процес обробки рахунків. Сьогодні підприємства стикаються з проблемою автоматичної обробки рахунків (RPA) у контексті оптимізації фінансових процесів. Дослідження стосується саме цієї технології та її використання в обробці рахунків.

Мета роботи полягала в тому, щоб зібрати та проаналізувати інформацію про переваги та можливості використання роботизованої обробки рахунків (RPA) для оптимізації обробки рахунків. Зокрема, були розглянуті такі аспекти, як ефективність та прискорення процесів; оптимізація ресурсів і зниження витрат; підвищення точності та уникнення помилок; відповідність стандартам і зниження ризику шахрайства; і підвищення прибутковості та сумісність з іншими технологіями.

Основними завданнями статті є розгляд основних принципів і можливостей роботизованої автоматизації процесів (RPA) у сфері обробки рахунків; дослідження методів впровадження RPA в процес обробки рахунків та оцінка того, як це впливає на продуктивність і точність операцій; розгляд майбутніх можливостей використання RPA в обробці рахунків та визначення потенційних тенденцій розвитку цієї технології. Ці цілі мають на меті провести ретельне дослідження та аналіз технології роботизованої обробки процесів (RPA) щодо її впливу на те, як вона оптимізує процеси обробки рахунків у бізнес-середовищах.

Аналіз переваг і можливостей RPA в контексті обробки рахунків є одним із методів, використаних у статті. Результати аналізу показують, що технологія RPA значно покращила обробку рахунків. RPA дозволяє автоматизувати рутинні процеси, що зменшує ризики та підвищує ефективність ведення бізнесу. Компанії в різних сферах отримують нові можливості завдяки цій технології.

Загалом дослідження свідчить про те, що роботизований процес обробки рахунків (RPA) є ефективним інструментом для оптимізації процесів обробки рахунків, підвищення ефективності та точності фінансових операцій і сприяння розвитку бізнес-планів у сучасних швидкозмінних бізнес-середовищах.

Ключові слова: автоматизована система, обробка рахунків, RPA, оптимізація бізнес-процесів, ефективність, фінансові операції.

FORECASTING THE STATE OF TELECOMMUNICATION NETWORKS USING QUANTILE AND LOGISTIC REGRESSION METHODS

In today's modern world, the ubiquity of information technology has intertwined telecommunications systems with every facet of human life. It's challenging to fathom a world where you're disconnected from the "World Wide Web" or unable to exchange data instantly via the intricate web of modern mobile devices. The vitality of staying connected online cannot be overstated, and ensuring the smooth functioning of telecommunications systems is paramount. This paper delves into the pivotal task of predicting and managing the performance of these networks, employing quantile and logical regression techniques. Our study leverages real-world data from telecommunication network operations to construct a predictive model capable of anticipating network conditions in advance. This predictive capability serves as the linchpin for intelligent decision-making systems, facilitating real-time network management. By implementing machine learning methods, specifically quantile regression, we achieve a sophisticated understanding of how various factors influence network performance. Our research doesn't just stop at forecasting; it extends to the realms of intellectual decision-making systems, where the insights gained from regression analysis play a pivotal role. These intelligent systems are equipped to make data-driven decisions on network resource allocation, maintenance schedules, and preemptive problem resolution. In essence, they act as the custodians of network stability, ensuring that telecommunication systems remain robust and responsive to the ever-evolving demands of modern society. This article sheds light on the indispensable role of regression methods in proactively managing the state of telecommunications networks. By harnessing the power of machine learning and data-driven insights, we pave the way for a future where network disruptions are minimized, and the seamless connectivity we've come to rely on remains a constant presence in our lives.

Keywords: *information technology, telecommunication system, intellectual decision-making system, machine learning, quantile regression.*

Introduction. Modern life is hard to imagine without information technology. A set of numerous digital radio-electronic devices connected to telecommunication systems not only help in organizing business processes at large enterprises, but also deeply entered our daily life. It is difficult to overestimate the importance of being in touch 24 hours a day and exchanging data at any second through networks consisting of modern mobile devices. Despite the fact that at first glance, many electronic devices seem to be independent, upon closer examination, they perform the functions of collecting, processing and transmitting information. And even if the device provides all of the above functionality, they still need to exchange information with each other through telecommunication networks.

At the moment, information technology has gone far ahead, which makes it possible to transfer information between devices at a high level. However, due to the complex multifunctional nature of these devices, the issues of maintaining high efficiency of information exchange play a key role in information technology. One of the main characteristics that determine the quality of the functioning of digital radio-electronic devices, designed solely to support the exchange of data between the remaining devices, is reliability. The operability and reliability of telecommunication systems and computer networks, consisting of radio-electronic devices for processing and transmitting information, will ultimately be characterized by the operability and reliability of the most inefficient device. Therefore, timely warning by identifying relevant inefficient devices is a key element in the analysis and monitoring of such systems.

Recently, to solve the problems of analysis and monitoring of telecommunication systems and computer networks, applied intelligent technologies are increasingly used [7]. Such technologies are based on the so-called machine learning technologies, on the basis of which decision-making systems are built for the intelligent control of complex distributed info communication

networks [1]. Machine learning algorithms designed for predictive use basically use the idea of autocorrelation between values over time. The general structure of the intelligent control system:

- telecommunications network;
- database of characteristics of the telecommunications system;
- data processing system based on machine learning technologies;
- decision making system;

Intelligent systems can differ significantly in their functions, but they always contain these blocks to one degree or another [2].

It is important to note that the main architectural feature that distinguishes the intelligent control system (Fig. 1.) from the one built according to the "traditional" scheme is due to the connection of storage mechanisms and intelligent data processing that characterize the operation of systems.

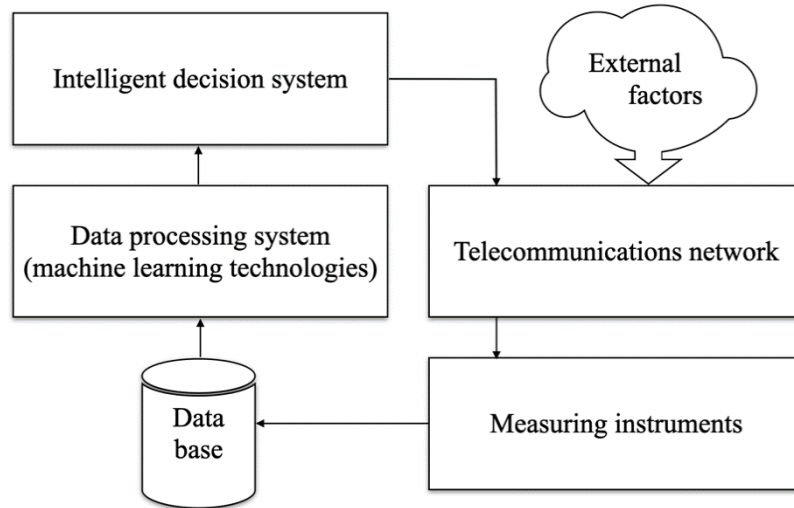


Figure - 1. General structure of the intelligent control system

This feature of intelligent systems allows real-time monitoring, analysis and effective management of the telecommunications network.

Formulation of the problem. The main purpose of the study is to build a mathematical model for predicting indicators that characterize the operation of telecommunication networks in order to optimize an intelligent decision-making system.

Research method. In this work, the quantile regression method was used as a machine learning model. In this work, the theory of logistic regression was used as a machine learning model.

Logistic regression [3, 4] is used to predict the probability of occurrence of some event based on the values of a set of features. To do this, the so-called dependent variable is introduced, which takes only one of two values - as a rule, these are the numbers 0 (the event did not occur) and 1 (the event occurred), and a set of independent variables (also called features, predictors or regressors) - real $x_1, x_2, \dots, x_n$, based on the values of which it is required to calculate the probability of accepting one or another value of the dependent variable.

It is assumed that the probability of an event occurring $y = 1$ equal:

$$P\{y = 1 | x\} = f(z),$$

where $z = \theta^T x = \theta_1 x_1 + \dots + \theta_n x_n$, x and θ column vectors of values of independent variables $x_1, x_2, \dots, x_n$ and parameters (regression coefficients) - real numbers $\theta_1, \theta_2, \dots, \theta_n$, respectively, $f(z)$ - the so-called logistic function (sometimes also called the sigmoid or logit function):

$$f(z) = \frac{1}{1 + e^{-z}}.$$

Since it takes only the values 0 and 1, the probability of the first possible value is equal to:

$$P\{y = 0 | x\} = 1 - f(z) = 1 - f(\theta^T x)$$

For brevity, the distribution function for given can be written in the following form:

$$P\{y | x\} = f(\theta^T x)^y (1 - f(\theta^T x))^{1-y}, \quad y \in \{0,1\}.$$

Advantages of the quantile regression method. The need to develop new methods of statistical estimation is dictated by the practical need for more adequate mathematical tools. Among the applied regression methods, the most common is the least squares method, which allows obtaining deep statistical results under the assumption that random errors are distributed according to a normal (Gaussian) law and (in most cases) are independent. There are also alternative approaches that require, however, strict assumptions about the type of distributions and other requirements regarding observations.

However, in practice, one often has to deal with more complex situations that do not fit into the standard assumptions of regression methods. Examples of such "violations" include:

1. the inaccuracy of setting the distribution that controls the observations in the sample, so that the assumptions of classical regression models about the homogeneity of the sample or about a sufficiently "beautiful" mechanism for the manifestation of homogeneity cannot be verified;

2. the presence of distributions with more "heavy tails" than the normal distribution, which necessitates the choice of estimation methods that give less weight to the extreme observed values, or even a complete rejection of the least squares method;

3. the presence in the sample of a small proportion of "outliers", that is, observations caused by some kind of "noise", which, as a rule, cannot be separated on the basis of a priori information. This requires the use of procedures that are not very sensitive to such "contamination" of the sample;

4. the dependence of the elements of the sample, which has a complex structure, so that it is difficult or even impossible to isolate and / or analyze (for example, using a covariance matrix).

In other words, in a number of practical problems that require the use of a regression approach, classical regression methods are inoperable and do not allow drawing correct conclusions about the nature of the process under study or the behavior of the object under consideration.

There have been repeated attempts to build alternative approaches. In particular, the so-called robust methods, which are resistant to deviations from the assumptions of the classical theory [5, 6], have been actively developed.

One of these approaches is the quantile regression method [8, 9, 10], which consists in replacing square deviations with absolute ones. It has a number of advantages:

- resistant to "outliers", which are often encountered in practical tasks;
- does not require independence or weak dependency;
- allows you to directly draw conclusions about the fluctuations of the predicted (estimated) indicator.

Thus, this method allows us to overcome the shortcomings of classical regression models, which are very sensitive to violations of their assumptions.

Selection of parameters. For selection of parameters $\theta_1, \theta_2, \dots, \theta_n$ it is necessary to make a training sample consisting of sets of values of independent variables and the corresponding values of the dependent variable y . Formally, this is the set of pairs $(x^{(1)}, y^{(1)}), \dots, (x^{(m)}, y^{(m)})$, where $x^{(i)} \in \mathfrak{R}^n$ – vector of values of independent variables, and $y^{(i)} \in \{0,1\}$ – their corresponding value y . Each such pair is called a training example.

The maximum likelihood method is usually used, according to which the parameters are chosen θ , maximizing the value of the likelihood function on the training sample:

$$\hat{\theta} = \arg \max_{\theta} L(\theta) = \arg \max_{\theta} \prod_{i=1}^m P\{y = y^{(i)} | x = x^{(i)}\}.$$

Maximizing the likelihood function is equivalent to maximizing its logarithm:

$$\ln L(\theta) = \sum_{i=1}^m \log P\{y = y^{(i)} | x = x^{(i)}\} = \sum_{i=1}^m y^{(i)} \ln f(\theta^T x^{(i)}) + (1 - y^{(i)}) \ln(1 - f(\theta^T x^{(i)})).$$

To maximize this function, for example, the gradient descent method can be applied. It consists in performing the following iterations, starting from some initial parameter value θ :

$$\theta := \theta + \alpha \nabla \ln L(\theta) = \theta + \alpha \sum_{i=1}^m (y^{(i)} - f(\theta^T x^{(i)})) x^{(i)}, \alpha > 0.$$

General quantile regression model. Let $(y_i, \mathbf{x}_i)$ – set of observations ($i=1 \div n$), where y_i – dependent variable in regression equation, and $\mathbf{x}_i = (x_{i1} \dots x_{im})$ – row vector of independent variables (covariate). Then the model is given by the relation [8, 9]

$$Quant_{\theta}(y_i | \mathbf{x}_i) = \mathbf{x}_i \boldsymbol{\beta}_{\theta}, \quad (1)$$

where $Quant_{\theta}(y_i | \mathbf{x}_i)$ denotes a conditional quantile y_i for probability θ on the regressor vector $\mathbf{x}_i$, and $\boldsymbol{\beta}_{\theta}$ – corresponding column vector of regression coefficients.

In other words, if i observation is described by a random vector $(\tilde{y}_i, \tilde{\mathbf{x}}_i)$, then the solution of an optimization problem of the form

$$\inf_{\boldsymbol{\beta}_{\theta}} \left\{ \mathbf{x}_i \boldsymbol{\beta}_{\theta} \mid F_{\tilde{y}_i | \tilde{\mathbf{x}}_i}(\mathbf{x}_i \boldsymbol{\beta}_{\theta} | \tilde{\mathbf{x}}_i = \mathbf{x}_i) \geq \theta \right\}.$$

Such a "direct" method requires knowledge of the conditional (joint) distribution or suitable assumptions about it.

Therefore, a nonparametric approach based on a large number is often used n notice $(y_i, \mathbf{x}_i)$, $i=1 \div n$. Within its framework, the assessment $\hat{\boldsymbol{\beta}}_{\theta}$ vector $\boldsymbol{\beta}_{\theta}$ from relation (1) is obtained by solving the minimization problem:

$$\min_{\boldsymbol{\beta}_{\theta}} \frac{1}{n} \left\{ \sum_{i: y_i \geq \mathbf{x}_i \boldsymbol{\beta}_{\theta}} \theta |y_i - \mathbf{x}_i \boldsymbol{\beta}_{\theta}| + \sum_{i: y_i < \mathbf{x}_i \boldsymbol{\beta}_{\theta}} (1-\theta) |y_i - \mathbf{x}_i \boldsymbol{\beta}_{\theta}| \right\} \quad (2)$$

For $\theta = \frac{1}{2}$ it is reduced to its special case - the classical problem of the least distances (LAD)

[11, 12]

$$\min_{\boldsymbol{\beta}_{\theta}} \frac{1}{n} \sum_i \frac{1}{2} |y_i - \mathbf{x}_i \boldsymbol{\beta}_{\theta}|$$

Representation of quantile regression as a linear programming problem. Problem (2) can be reduced to a linear programming problem of the form:

$$\begin{aligned} & \theta \cdot \mathbf{1} \cdot \mathbf{u}^+ + (1-\theta) \cdot \mathbf{1} \cdot \mathbf{u}^- \rightarrow \min \\ & \begin{cases} \mathbf{X} \boldsymbol{\beta}_{\theta} + \mathbf{u}^+ - \mathbf{u}^- = \mathbf{y}, \\ \mathbf{u}^+ \geq \mathbf{0}, \\ \mathbf{u}^- \geq \mathbf{0}, \end{cases} \end{aligned} \quad (3)$$

where $\mathbf{1}$ – row vector of suitable dimension, consisting of ones; $\mathbf{X}$ – covariate observation matrix (dimensions $n \times m$); $\mathbf{y}$ – vector of independent variable observations (dimensions n); $\mathbf{u}^+$ and $\mathbf{u}^-$ – vectors of positive and negative deviations, respectively, with components

$$\begin{aligned} u_i^+ &= (y_i - \mathbf{x}_i \boldsymbol{\beta}_{\theta})^+ = \begin{cases} y_i - \mathbf{x}_i \boldsymbol{\beta}_{\theta}, & y_i \geq \mathbf{x}_i \boldsymbol{\beta}_{\theta}, \\ 0, & \text{в противном случае,} \end{cases} \\ u_i^- &= (\mathbf{x}_i \boldsymbol{\beta}_{\theta} - y_i)^+ = \begin{cases} \mathbf{x}_i \boldsymbol{\beta}_{\theta} - y_i, & y_i < \mathbf{x}_i \boldsymbol{\beta}_{\theta}, \\ 0, & \text{в противном случае.} \end{cases} \end{aligned}$$

In practice, as the initial value of the vector $\hat{\boldsymbol{\beta}}_{\theta}$ to solve a linear programming problem, it is convenient to take the corrected least squares estimate. Another approach is that the initial value can be obtained from a quantile regression based on a small subset of the sample, which, as a result, significantly reduces the number of iterations and computation time.

Presenting a quantile regression model as a linear programming problem has several important implications. First, it is guaranteed that the estimate will be obtained in a finite number of iterations. Second, the parameter vector estimate will be robust to outliers. In other words, if $y_i - \mathbf{x}_i \hat{\boldsymbol{\beta}}_\theta > 0$, then y_i can be increased to almost $+\infty$, and vice versa if $y_i - \mathbf{x}_i \hat{\boldsymbol{\beta}}_\theta < 0$, then y_i can be reduced to almost $-\infty$ without changing the decision $\hat{\boldsymbol{\beta}}_\theta$.

Confidence intervals for quantile regression estimates. General instructions for constructing confidence intervals for quantiles can be found in the handbook [13]. Building confidence intervals (confidence bands) for quantile regression is their development. In particular, we can name the direct method, which does not depend on the distribution, the method of studentized intervals, and the method based on the bootstrap distribution [14].

The article uses a direct approach, since it is the most optimal, both in terms of minimizing computational procedures and the adequacy of the interval estimate in general. According to this method, the confidence band is estimated for an arbitrary vector $\mathbf{x}$ according to the formula

$$I_{\hat{\boldsymbol{\beta}}_\theta} = (\mathbf{x} \hat{\boldsymbol{\beta}}_{\theta-b}, \mathbf{x} \hat{\boldsymbol{\beta}}_{\theta+b}), \quad (4)$$

where $b = z_\gamma \sqrt{\frac{\mathbf{x} \mathbf{Q}^{-1} \mathbf{x} \cdot \theta(1-\theta)}{n}}$, $\mathbf{Q} = n^{-1} \sum_{i=1}^n \mathbf{x}_i' \mathbf{x}_i$, $\gamma \in (0,1)$ – confidence probability

(probability that the confidence interval will cover the true value), $z_\gamma = \Phi^{-1}(\gamma)$ – quantile of the standard normal distribution for probability γ , $\Phi^{-1}(\cdot)$ – function inverse to the standard normal distribution function.

Thus, to build a confidence interval for quantile regression estimates, we need to additionally estimate the quantile regression for probability levels $\theta \pm b$.

Getting data. The internal computer network of the enterprise was taken as the subject of the study. Using the SNMP protocol, data was collected that characterizes the operation of the network. Data on the functioning of the telecommunications network were recorded with an interval of 30 seconds. The following characteristics were determined for the analysis:

- number of lost packets;
- CPU frequency;
- processor temperature;
- bus voltage.

Data processing. All data were analyzed for missing observations and errors in values. For visual analysis, for each of the parameters, time series graphs were built (Fig. 1 and Fig. 2.).

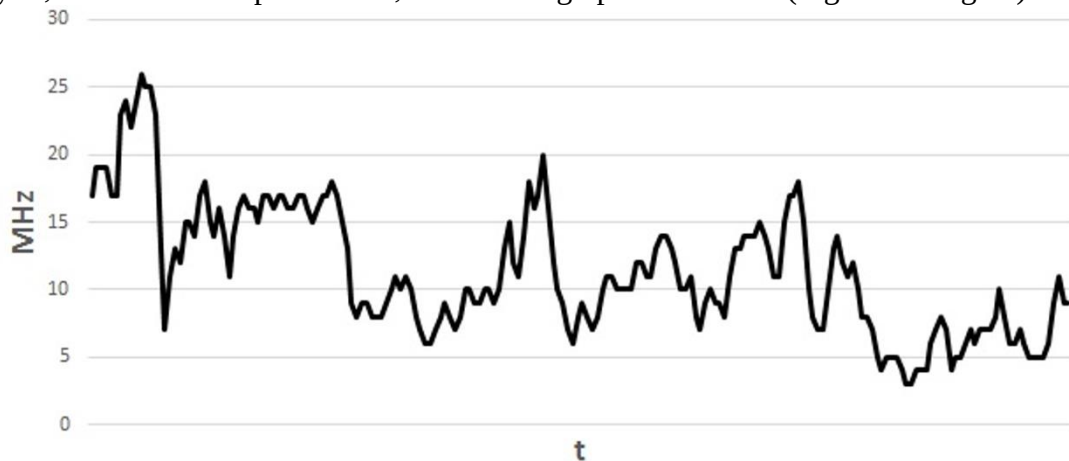


Figure - 2. Graph of processor load over time

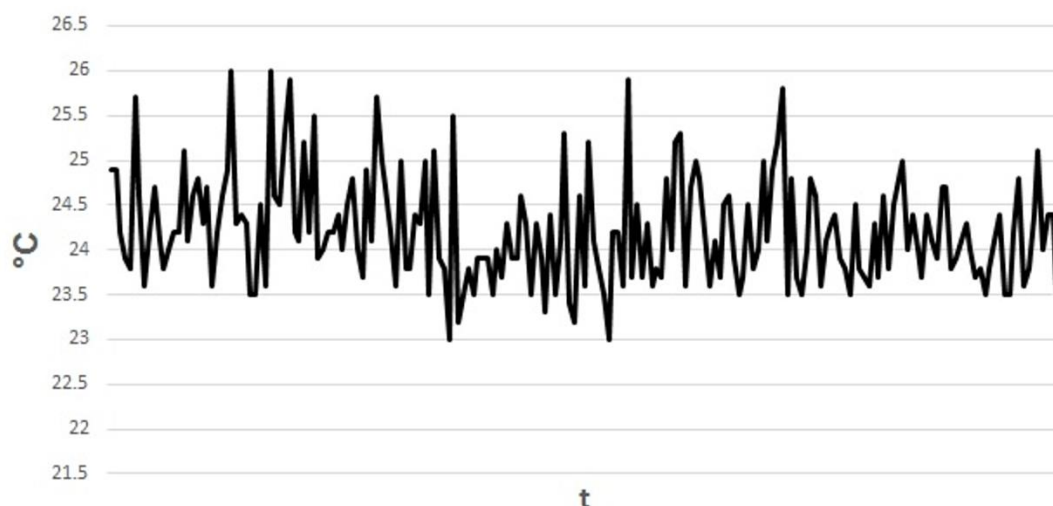


Figure - 3. Graph of CPU temperature over time

Conclusion

1. An analysis of the characteristics of the operation of digital radio electronic devices has shown that there is a pattern in the development of the values of these indicators over time. Moreover, there is no significant correlation between the characteristics, which means the independent nature of their behavior. Thus, the task of independent forecasting of the values of characteristics for the future makes it possible to prevent situations of overload of certain nodes of the telecommunication network, which was done in this work.

2. The possibility of using the quantile regression method to predict the values of parameters characterizing the operation of digital radio electronic devices has been proved.

3. The features of statistical monitoring of telecommunication networks are determined, namely: non-stationarity, periodicity (uneven loading of channels), non-linear influence of network operation characteristics on its efficiency.

4. Since the constructed quantile regression model could not fully explain the development of parameter values over time, the authors draw conclusions about the nonlinear dependencies of these indicators and set themselves the task of further research.

REFERENCES:

1. Khlaponin Y.I. Modern problems of creating complex real-time information and control systems / Khlaponin Yu.I., Nedaybida Yu.P., Kotova Yu.V. // *Information protection*. – 2012. – No. 4 (57). – P. 50-55.
2. Enyukov I.S. Statistical analysis and monitoring of scientific and educational Internet networks / I.S. Enyukov, I.V. Retinskaya; under. ed. A. N. Tikhonova. – M.: Finance and Statistics, 2004. – 320 p.
3. Khlaponin Yu.I. Modern problems of creating complex real-time information and control systems / Khlaponin Yu.I., Nedaybida Yu.P., Kotova Yu.V. // *Information protection*. – 2012. – No. 4 (57). – P. 50-55.
4. Ayvazyan S.A. Applied statistics: classification and dimensionality reduction / Ayvazyan S.A., Bukhstaber V.M., Enyukov I.S., Meshalkin L.D. Applied statistics: classification and dimensionality reduction. – M.: Finance and Statistics, 1989.
5. Andrews D.F. A Robust Method for Multiple Linear Regression // *Technometrics*. 1974. Vol. 16. P. 523–531.
6. Hogg R.V. Adaptive Robust Procedures: A Partial Review and Some Suggestions for Future Applications and Theory // *Journal of the American Statistical Association*. 1972. Vol. 43. P. 1041–1067.
7. Khlaponin Y.I. Establishment of neural measures in a statistical system of analysis and monitoring of telecommunication measures / Khlaponin Y.I., Zhiron G.B., Nikitchin O.M. - K.: Technological audit and production reserves, 2016. - P.35.
8. Koenker R., Bassett G., Jr. Regression Quantiles // *Econometrica*. 1978. Vol. 46. No.1. P.33–50.
9. Koenker R., Hallock K.F. Quantile Regression // *Journal of Economic Perspectives*. 2001. Vol. 15. No.4. P.143–156.

10. Huber P.J., Robust Statistics. 1981. New York: John Wiley and sons.
11. Karst O.J. Linear Curve Fitting Using Least Deviations // Journal of the American Statistical Association. 1958. Vol. 53. No. 281. P. 118–132.
12. Wagner H.M. Linear Programming Techniques Regression Analysis // Journal of the American Statistical Association. 1959. Vol. 54. No. 285. P.206–212.
13. Introduction to the theory of order statistics / Ed. A.E. Sarkhan and B.G. Greenberg. Per. from English Ed. AND I. Boyarsky. M.: Statistics, 1970.
14. Kenneth Q. Z., Stephen L. P. Direct Use of Regression Quantiles to Construct Confidence Sets in Linear Models // The Annals of Statistics. 1996. Vol. 24. No. 1. P. 287–306.
15. Serhey Lienkov, Genadiy Zhyrov, Ihor Pampukha, Ivan Chetverikov . Block Encryption Algorithm for Digital Information Using Open Keys for Selfgeneration of Closed Random Private Keys // 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), 18-20 Dec. 2019 Kyiv, Ukraine. Electronic ISBN: 978-1-7281-6144-0, Print on Demand(PoD) ISBN: 978-1-7281-6145-7, INSPEC Accession Number: 19452664 DOI: 10.1109/ATIT49449.2019.9030509.

д.т.н. проф. Хлапонін Ю.І. к.т.н. доц. Касім Н.Х., Тарасюк Д.М.

ПРОГНОЗУВАННЯ СТАНУ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ МЕТОДАМИ КВАНТИЛЬНОЇ ТА ЛОГІСТИЧНОЇ РЕГРЕСІЇ

У сучасному світі повсюдне поширення інформаційних технологій переплелись телекомунікаційні системи з усіма аспектами людського життя. Важко досягнути світ, де ви відключені від «Всесвітньої мережі» або не можете миттєво обмінюватися даними через заплутану мережу сучасних мобільних пристроїв. Життєвість підтримки зв'язку онлайн неможливо переоцінити, а забезпечення безперебійної роботи телекомунікаційних систем є першорядним. У цьому документі розглядається головне завдання прогнозування та керування продуктивністю цих мереж, використовуючи методи квантильної та логічної регресії. Наше дослідження використовує реальні дані з операцій телекомунікаційної мережі, щоб побудувати прогностичну модель, здатну заздалегідь передбачити стан мережі. Ця можливість прогнозування служить основою для інтелектуальних систем прийняття рішень, полегшуючи керування мережею в реальному часі. Впроваджуючи методи машинного навчання, зокрема квантильну регресію, ми досягаємо глибокого розуміння того, як різні фактори впливають на продуктивність мережі. Наше дослідження не обмежується лише прогнозуванням; він поширюється на сфери інтелектуальних систем прийняття рішень, де розуміння, отримане за допомогою регресійного аналізу, відіграє ключову роль. Ці інтелектуальні системи обладнані для прийняття керованих даними рішень щодо розподілу мережевих ресурсів, графіків технічного обслуговування та превентивного вирішення проблем. По суті, вони діють як зберігачі стабільності мережі, гарантуючи, що телекомунікаційні системи залишаються надійними та чуйними на вимоги сучасного суспільства, що постійно змінюються. Ця стаття проливає світло на незамінну роль регресійних методів у проактивному управлінні станом телекомунікаційних мереж. Використовуючи потужність машинного навчання та аналіз даних, ми прокладаємо шлях до майбутнього, де збої в роботі мережі зведені до мінімуму, а безперебійне з'єднання, на яке ми звикли покладатися, постійно буде присутнім у нашому житті.

Ключові слова: інформаційні технології, телекомунікаційна система, інтелектуальна система прийняття рішень, машинне навчання, квантильна регресія.

МОЖЛИВІ ВАРІАНТИ УДОСКОНАЛЕННЯ ІСНУЮЧИХ ПІДХОДІВ ДО ВИЯВЛЕННЯ ФЕЙКОВИХ НОВИН НА ОСНОВІ ВИКОРИСТАННЯ ПОТЕНЦІАЛУ АЛГОРИТМІВ МАШИННОГО ТА ГЛИБОКОГО НАВЧАННЯ, СЕНТИМЕНТУ НОВИННОГО КОНТЕНТУ Й ЕМОЦІЙ У КОМЕНТАРЯХ КОРИСТУВАЧІВ

На даний час серед джерел інформації Інтернет займає перше місце. В останній період суттєво зросла роль онлайн соціальних мереж (ОСМ), що має як позитивні, так і негативні наслідки. Негативна роль ОСМ пов'язується із поширенням фейкових новин, які впливають на повсякденне життя людей, маніпулюють їхніми думками та почуттями, змінюють їхні переконання і можуть призвести до прийняття неправильних рішень. Проблема розповсюдження фейкових новин в ОСМ на даний час є глобальною, а формування механізмів протидії – актуальним завданням сьогодення.

На сьогодні існують різні апробовані підходи до виявлення фейкових новин. Зокрема, один з підходів базується на використанні різних алгоритмів машинного (ML) та глибокого (DL) навчання. Інший – на використанні результатів аналізу настрою новинного контенту та аналізу емоцій у коментарях користувачів. Проведене авторами дослідження інших підходів виявлення фейкових новин, які відрізняються від наведених, дозволило зробити висновок про те, що зазначені підходи є ефективними і перспективними в частині використання їх потенціалу для розробки нових моделей з високими показниками ефективності на різних наборах даних.

У статті сформовано та формалізовано авторські ідеї щодо удосконалення існуючих підходів виявлення фейкових новин на основі використання потенціалу зазначених підходів. Перша ідея базується на реалізації механізму комбінування методів машинного (ML) та глибокого (DL) навчання, а також результатів аналізу настрою новинного контенту й емоцій у коментарях користувачів, при якому враховується можливість забезпечення достатнього рівня ефективності виявлення фейкових новин, певного рівня значень показників обраної метрики, а також певного рівня функціональних характеристик авторського методу. Друга ідея базується на реалізації механізму комбінування функціоналу двох методів з числа зазначених двох груп, який би забезпечував оптимальні параметри виявлення фейкових новин за визначеними критеріями та показниками.

Обґрунтування ідей передбачало попереднє здійснення: постановки досліджуваної задачі; функціонального аналізу алгоритмів машинного (ML) та глибокого (DL) навчання, а також алгоритмів виявлення фейкових новин, що базуються на використанні результатів аналізу настрою новинного контенту й емоцій у коментарях користувачів; опису метрики для оцінки ефективності методів виявлення фейкових новин. За результатами обґрунтування перспективності ідей проведено формалізацію задач виявлення фейкових новин в авторській постановці.

Ключові слова: онлайн соціальні мережі; фейкові новини; метод; модель; алгоритм; формалізація.

Вступ та постановка проблеми у загальному вигляді. До недавнього часу люди отримували новини та інформацію переважно з газет і телевізійних каналів. Проте з появою Інтернету ситуація змінилася кардинально. Інтернет зайняв перше місце серед джерел інформації [1]. Суттєво зросла роль онлайн соціальних мереж (ОСМ) [2 - 4]. Стрімкий технологічний розвиток, що спостерігається в останні роки, особливо в галузі мобільної промисловості, зробив соціальні медіа, такі як Facebook, Twitter, Instagram та Sina Weibo, доступними і невід'ємною частиною нашого повсякденного життя [2, 5]. У результаті дослідження, проведеного в 2017 році, встановлено, що 67% осіб у США отримують новини в основному з соціальних мереж [6]. Згідно з Global Overview Report (<https://datareportal.com/reports/digital-2021-global-overview-report>, доступно 11 листопада 2021

року) кількість людей у світі з обліковими записами в ОСМ у 2021 році досягла рівня приблизно 4,20 мільярди, що складає понад 53% загального населення світу [7]. ОСМ стали не лише засобом комунікації між людьми, а й інструментом обміну інформацією та формування громадської думки [8]. Соціальні медіа надали віртуальне середовище для публікацій [9], обговорення, обміну поглядами та глобальної взаємодії між користувачами [10], без обмежень за місцем, часом або обсягом контенту [11].

Основна причина використання соціальних медіа користувачами у всьому світі - отримання новин та оперативне слідкування за поточними подіями.

Багато людей використовують соціальні медіа для публікації новин та інформації через свої облікові записи або сторінки, оскільки публікація новин на цих платформах відрізняється від публікації у традиційних ЗМІ тим, що не займає багато часу, не потребує витрат і не підлягає обмеженням аудиту [5, 12]. Структура соціальних медіа дозволяє поширювати новини в режимі реального часу та швидко, незалежно від достовірності цих новин [3]. Наприклад, у США в 2012 році 49% користувачів ділилися новинами в соціальних мережах. Згідно з доповіддю Pew Research Center (<https://www.pewresearch.org/>, доступно 23 серпня 2021 року), у 2016 році понад 62% користувачів щоденно отримували новини з ОСМ [12], а у 2018 році дві третини дорослого населення США отримували новини з платформ соціальних медіа [13].

Однак, в останній період ОСМ відіграють не лише позитивну, а й негативну роль. Це пов'язано із забезпеченням ними поширення фейкових новин. Дослідження, проведене в 2016 році, показало, що 23% осіб у США ділилися фейковими новинами, як навмисно, так і ненавмисно [14]. У Китаї більше третини інформаційних повідомлень, які стають трендами на мікроблогах, є фейковою інформацією [15]. Деякі популярні джерела інформації, що вважаються надійними (наприклад, Вікіпедія), також поширюють невірну інформацію або фейкові новини [16].

Фейкові новини можна визначити як опубліковані новинні статті, що містять неправдиву інформацію з метою свідомого введення читачів в оману [2] або здійснення зловживань [17]. Зазвичай у фейкових новинах містяться високопровокаційні повідомлення, створення яких переслідує фінансову чи політичну цілі. У 2017 році «фейкові новини» за версією словника [5] були оголошені офіційним словом року.

Згідно з доповіддю GDATA, 59% користувачів ОСМ стикалися з неправдивою інформацією [18]. Понад 57% користувачів ОСМ очікували, що опубліковані новини будуть неточними [13]. Сайт Statista представив статистику (<https://www.statista.com/statistics/649221/fake-news-expose-responsible-usa/>, доступно 4 березня 2021 року) за 27 серпня 2019 року, що базується на опитуванні, проведеному у США в 2018 році, щодо того, як ОСМ відповідають за поширення фейкових новин. Згідно наведених даних, 29% учасників вважають, що за поширення фейкових новин в основному відповідають соціальні медіа, а 60% відмітили, що ці платформи за поширення фейкових новин відповідають частково. Фейкові новини мають на 70% більше шансів поширюватися, ніж новини реальні [12]. Згідно з дослідженнями щодо швидкості поширення фейкових новин, твіти, які містять фальсифіковану інформацію в Twitter, досягають користувачів у шість разів швидше, ніж надійні твіти [19]. Швидкість поширення фейкових новин в Інтернеті більша, ніж реальних [12], оскільки люди цікавляться новою інформацією або новинами [20] та схильні ділитися останньою інформацією [21], особливо розповідати про важливі новини, не перевіряючи їх достовірність [22]. Повторний перегляд фейкових новин робить їх одержувачам знайомими, підвищує їх вірогідність і призводить до їх поширення як реальних новин [23].

Фейкові новини впливають на повсякденне життя людей [1, 8], маніпулюють їхніми думками та почуттями [24, 25], змінюють їхні переконання [26] і можуть призвести до прийняття неправильних рішень [1]. Розповсюдження фейкових новин у соціальних мережах негативно впливає на суспільство [27, 28] у багатьох сферах, зокрема таких, як політична, економічна, соціальна, медична, технологічна та спортивна [15, 26]. Основними намірами поширення фейкових новин є фінансовий зиск, поширення ненависті на підставі

екстремістських мотивів, маніпулювання свідомістю людей з політичних міркувань або створення упереджених думок з виборчих міркувань [29, 30] тощо. Результатом поширення фейкових новин, як правило, є страх, паніка та фінансові втрати [28].

Все це вказує на негативні наслідки поширення фейкових новин і їх негативний соціальний вплив.

Про негативну роль фейкових новин можна судити, зокрема з таких прикладів. Одна з новин на Reddit спричинила реальну стрілянину (<https://www.rollingstone.com/politics/politics-news/anatomy-of-a-fake-news-scandal-125877/>, доступно на 15 березня 2022 року). Під час виборчої кампанії до виборів президента США у 2016 році було виявлено понад мільйон постів, пов'язаних із фейковою новиною, відомою як PIZZAGATE (<https://tinyurl.com/z38z5zh>, доступно на 15 червня 2022 року). У фейковій новині про мусульманську спільноту в Індії (<https://thelogicalindian.com/fact-check/muslim-spit-restaurant-covid-19-coronavirus-20457>, доступно 16 липня 2021 року) на підставі доповіді BBC (<https://www.bbc.com/news/world-asia-india-53165436>, доступно 16 липня 2021 року) стверджувалось, що мусульмани намірено поширюють COVID-19. Це призвело до збільшення ворожнечі до мусульман і закликів до економічного бойкоту. Крім того, 20 найпопулярніших фейкових новин були більш обговорюваними, ніж 20 найпопулярніших реальних історій (<https://tinyurl.com/y8dckwhr>, доступно на 15 червня 2022 року).

У 2021 році Facebook оголосив, що було закрито близько 1,3 мільярда фейкових облікових записів та видалено понад 12 мільйонів публікацій з хибною інформацією про COVID-19 та вакцини [31].

У багатьох людей виникають труднощі у відрізненні фейкових новин від реальних, незалежно від статі, віку чи рівня освіти [16]. Відрізнити фейкові новини від реальних складно, оскільки, як свідчать наукові дослідження, людська здатність розрізняти правдиву та неправдиву інформацію відносно незначна і становить близько 54% [32].

Оскільки фейкові новини стали глобальним викликом і великою загрозою для демократії, економіки та мирного співіснування [33], різні суб'єкти (громадські організації, журналісти, політики, дослідники) працюють над зменшенням ризику [12].

Отже, проблема розповсюдження фейкових новин в ОСМ на даний час є глобальною, а формування механізмів протидії – актуальним завданням сьогодення. Її вирішення пов'язується з формуванням моделей, які виявляють фейкові новини та обмежують можливість їх поширення [34].

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми. На даний час існують різні апробовані підходи до виявлення фейкових новин. Зокрема, один з підходів базується на використанні різних алгоритмів машинного (ML) та глибокого (DL) навчання. Інший – на використанні результатів аналізу настрою новинного контенту та аналізу емоцій у коментарях користувачів. Існує і ряд інших підходів, які заслуговують на увагу, подальший аналіз і дослідження. При цьому кожен із них характеризується певним рівнем ефективності на різних масивах даних.

Слід зауважити, що для перевірки ефективності підходів часто застосовуються такі набори даних, як LIAR, FakeNewsNet-PolitiFact, FakeNewsNet-GossipCop і COVID-19.

LIAR – це великий, доступний для широкого загалу набір даних фейкових новин [35]. Набір даних містить близько 12800 записів і дві основні складові: профілі користувачів і короткі політичні заяви. Характеристики профілю користувача включають ім'я спікера, роботу, партійну належність, штат, кредитну історію та контекст. Заяви (зроблені в період з 2007 по 2016 рік) були позначені редакцією Politifact.com за допомогою шести деталізованих категорій: правда, переважно правда, наполовину правда, майже неправда, неправда і шар зігрівається. Ці шість міток є відносно збалансованими за розміром. Загалом кожна заява має свою пов'язану мітку та інформацію про автора цієї заяви.

FakeNewsNet - це комплексний набір даних (<https://github.com/KaiDMML/FakeNewsNet>, доступно на 20 березня 2022 року), який складається з повних текстових новинних статей, зібраних з веб-сайтів politifact.com і gossipcop.com (доступно на 18 березня 2022 року). Кожен з них містить новинні статті та інформацію про соціальний контекст.

COVID-19 - це збірник соціальних медіа-повідомлень, коментарів і новин, пов'язаних із COVID-19, класифікованих як реальні або фейкові на основі їхньої правдивості. Набір даних [36] був зібраний з різних соціальних медіа-платформ, таких як Twitter і YouTube. Крім того, організатори збірника зібрали 10700 соціальних медіа-повідомлень та новинних статей про COVID-19 у формі анотованого набору даних англійською мовою.

Також слід зауважити, що критеріями оцінки, які широко використовуються в завданнях класифікації тексту, часто є точність (A), точність (P), чутливість (R) та $F1$ -показник. Також при роботі з незбалансованим набором даних для оцінки продуктивності моделей в якості міри продуктивності часто використовується площа під кривою ROC (AUC), яка є мірою для порівняння алгоритмів навчання та побудови оптимальних моделей навчання [37-39].

До переліку класичних алгоритмів ML прийнято відносити логістичну регресію (LR), метод опорних векторів (SVM), дерево рішень (DT), наївний байєсівський класифікатор (NB), випадковий ліс (RF), $XGBoost$ (XGB), а також комбінацію цих алгоритмів. До високорівневих алгоритмів ML відносять згорткові нейронні мережі (CNN), двонаправлені рекурентні мережі з короткотривалою пам'яттю ($BiLSTM$), двонаправлені рекурентні мережі з вентиляними блоками ($BiGRU$), комбінації $CNN-BiLSTM$ і $CNN-BiGRU$, а також гібридний підхід на основі цих технік. Моделями на основі глибокого навчання є моделі $BERTbase$ та $RoBERTabase$.

У роботі [40] представлено огляд підходів до виявлення фейкових новин на основі використання алгоритмів машинного навчання ML з двома сценаріями методів представлення слів (статистичними та контекст-незалежними). Крім того, у роботі [40] проведено порівняльну оцінку восьми передових моделей машинного навчання, а саме CNN , $BiLSTM$, $BiGRU$, $CNN-BiLSTM$, $CNN-BiGRU$, різних гібридних моделей з двома типами моделей текстового представлення (контекст-незалежними і контекст-свідомими моделями вбудови), $BERTbase$, $RoBERTabase$.

Авторами роботи [40] встановлено, що комбінація класичних методів машинного навчання з ознаками $TF-IDF$ краща за інші методи на наборі даних $LIAR$, включаючи передові моделі машинного навчання. Метод $BERTbase$ забезпечив точність на рівні з найкращими моделями. $RoBERTabase$ показав найкращі результати на наборі даних $PolitiFact$ з $F1$ -оцінкою 93.17%. Метод SVM з ознаками $TF-IDF$ продемонстрував результати кращі за результати моделей глибокого навчання на наборі даних $GossipCop$. На наборі даних $COVID-19$ найкращою моделлю був $BERTbase$. Однак експериментальні результати засвідчили, що жодна окрема техніка не змогла забезпечити найкращі показники продуктивності на всіх наборах даних.

Багато досліджень щодо виявлення фейкових новин в $ОСМ$ залежать від однієї чи декількох ознак, таких як вміст, мережеве поширення або користувач [41 - 43]. Аналіз коментарів користувачів для визначення їхнього ставлення до новин може відігравати важливу роль у виявленні фейкових новин [44 - 46] та надавати уявлення про достовірність опублікованих новин [5, 34]. У роботі [47] стверджується, що коментарі користувачів мають велику дискримінантну цінність при виявленні фейкових новин, де вираження сентименту [38] або емоцій [48] має вирішальне значення. У праці [20] зазначено, що реакція користувачів на фейкові новини виражає емоції страху, огиди та здивування, тоді як на реальні новини - емоції очікування, суму, радості та довіри. Однак автори цієї праці не досліджували, наскільки добре емоції можуть ідентифікувати фейкові новини. Згідно [49], новизна може бути важливою складовою фейкових новин і значно підвищувати можливості їх поширення та прийняття в суспільстві. Більшість існуючих досліджень, які використовують аналіз сентименту, зосереджуються на сигналах сентименту вмісту фейкових новин [50]. Часто користувачі використовують емодзі замість текстових коментарів, щоб висловити свої думки про певні новини в $ОСМ$ [51 - 53]. У цьому контексті техніки глибокого навчання (DL) суттєво сприяють класифікації, прогнозуванню та аналізу текстового контенту [54, 55]. Це пов'язано з їхньою здатністю до ефективного навчання [2, 12], виявлення ознак і складних патернів [56, 57].

У працях [3, 58] продемонстровано, що додавання ознак на основі аналізу настроїв та аналізу емоцій збільшує точність виявлення фейкових новин для більшості моделей глибокого навчання порівняно з використанням лише текстових ознак. Також авторами зазначених праць встановлено, що ознаки на основі аналізу настроїв новин та аналізу емоцій коментарів користувачів цих новин можуть бути використані соціальними медіа-платформами для боротьби з поширенням фейкових новин. Проте, застосування зазначеного підходу пов'язане з труднощами при роботі з незбалансованим набором даних.

Проведене авторами дослідження інших підходів виявлення фейкових новин дозволило зробити висновок про те, що проаналізовані вище підходи є ефективними і перспективними в частині використання їх потенціалу для розробки нових моделей з високими показниками ефективності виявлення фейкових новин на різних наборах даних.

Тому метою даної статті є формування та формалізація авторської ідеї щодо удосконалення існуючих підходів виявлення фейкових новин на основі використання потенціалу алгоритмів машинного (ML) та глибокого (DL) навчання, а також результатів аналізу настроїв новинного контенту й аналізу емоцій у коментарях користувачів.

Виклад основного матеріалу

Для досягнення визначеної мети вбачається за доцільне:

здійснити постановку досліджуваної задачі;

здійснити функціональний аналіз алгоритмів машинного (ML) та глибокого (DL) навчання, а також алгоритмів виявлення фейкових новин, що базуються на використанні результатів аналізу настроїв новинного контенту й емоцій у коментарях користувачів;

описати метрику для оцінки ефективності методів виявлення фейкових новин;

описати авторську ідею комплексування потенціалу алгоритмів машинного (ML) та глибокого (DL) навчання, а також результатів аналізу настроїв новинного контенту й емоцій у коментарях користувачів;

здійснити формалізацію задачі виявлення фейкових новин, що реалізує авторську ідею її вирішення.

Постановка досліджуваної задачі.

Задача виявлення фейкових новин розглядатиметься, як бінарна класифікація на основі заданих ознак і моделі для прогнозування вірогідності того, що певна новина є фейковою чи реальною.

Формально задача виглядає так. Нехай задано множину новинних статей, висловлювань або твітів $A = \{a_1, a_2, \dots, a_k\}$, де k – це довжина вхідного тексту, із заданими початковими ознаками. Завдання полягає у встановленні фейковості чи реальності їх контенту на основі застосування до заданих ознак кожного елемента множини A авторської моделі.

Функціональний аналіз алгоритмів машинного (ML) та глибокого (DL) навчання, а також алгоритмів виявлення фейкових новин, що базуються на використанні результатів аналізу настроїв новинного контенту й емоцій у коментарях користувачів.

Авторами ряду наукових праць для виявлення фейкових новин було досліджено і випробувано велику кількість ML-алгоритмів. Зокрема:

Логістична регресія (LR): Логістична регресія - це статистична модель, яка застосовується як базова модель для широкого спектру завдань текстової класифікації.

Support Vector Machine (SVM): Класифікатор SVM - це потужний класифікатор, який є перспективним для вирішення низки завдань обробки природної мови.

Мультиноміальний наївний байєсівський (MNB): MNB - це популярний вид ймовірнісного алгоритму, який дає суттєві результати в різних завданнях обробки природної мови.

Дерево рішень (DT): DT - це алгоритм на основі дерева, в якому кінцеві вузли представляють високорівневі ознаки. Кожен вузол відображає вихід, а листок - клас мітки. У вузлах приймається рішення на підставі навчання з нагляду, яке перетворює відображення ознак і значень у бажані результати.

Випадковий ліс (RF): RF – це алгоритм, що складається з набору дерев рішень, кожне з яких навчено на випадковому наборі ознак.

XGBoost (XGB): XGB - це комбінований алгоритм машинного навчання, в основі якого знаходиться градієнтний бустінг і який базується на деревах рішень. За допомогою бустінгу дерева будуються послідовно і кожне з них спрямоване на зменшення помилок попереднього.

Ensemble: Ensemble - це метод навчання, який об'єднує наведені вище алгоритми машинного навчання для покращення продуктивності.

Також було досліджено такі алгоритми:

CNN: CNN – це одновимірний згортковий нейронна мережа, що є потужним методом машинного навчання для автоматичного виділення ознак з текстових вхідних даних. CNN може автоматично видобувати локальні ознаки, вона менш обчислювально витратна, ніж інші алгоритми машинного навчання. Її архітектура включає один шар CNN з 128 фільтрами розміром ядра 5, які активуються функцією активації ReLU. Згенеровану карту ознак потім вдосконалюють і зменшують за допомогою шару максимального зведення, що призводить до отримання найбільш відповідної інформації. Після цього вихід розгортають і передають на вихідний шар з одиницею, яка активується сигмоїдною функцією активації.

LSTM: Модель LSTM [59] виправляє недоліки RNN, додаючи адитивну та мультиплікативну взаємодії до формули рекурентності та окремий стан пам'яті. Складність моделі можна збільшити, стекаючи LSTM-шари. За допомогою трьох гейтів - входу, забуття і виходу - моделі LSTM усувають проблеми ванішення та вибуху градієнта, які властиві RNN. Важливою характеристикою моделей LSTM є їхня здатність захоплювати віддалені залежності. У них використовується один шар BiLSTM з 128 одиницями для кодування вхідного тексту.

GRU: У варіанті GRU існують лише два гейти: гейт оновлення та гейт скидання. Гейт оновлення об'єднує гейти забуття та входу і вирішує, яка інформація буде передана поточному стану. Гейти скидання визначають, коли ігнорувати попередній прихований стан [60].

Проста RNN розглядає контекст минулого, але не може враховувати контекст майбутнього. Тому для врахування майбутнього та попереднього контексту використовуються бідирекційні LSTM (BiLSTM) і бідирекційні GRU (BiGRU) завдяки їхнім конструкціям. Для забезпечення їх переваги об'єднуються шари прихованих обчислень вперед і назад, що контролює потік інформації в обох напрямках і призводить до кращого навчання.

Незважаючи на те, що BiLSTM та BiGRU виявляють переваги при вирішенні ряду проблем NLP, вони не позбавлені двох недоліків: зі збільшенням високорозмірного вхідного простору зростає їх складність, що призводить до ще більшої складності при їх оптимізації; ці моделі можуть захоплювати інформацію про послідовний і наступний контекст (концепція бідирекційності), вони не можуть фокусуватися на найважливіших частинах контекстуальної інформації тексту. Щоб усунути перший недолік, можна використовувати CNN для зменшення розмірності простору ознак, зберігаючи при цьому інформативні ознаки з тексту. Крім того, CNN може захоплювати та виділяти локальні патерни.

CNN-BiLSTM: Гібридизація моделей на основі рекурентних мереж із CNN допомагає виділяти суттєві ознаки, захоплювати локальні контекстуалізовані патерни та покращувати точність моделі. Спочатку використовується один шар CNN з 128 фільтрами та розміром ядра 5 для обробки вхідних векторів і виділення локальних ознак. Результати карт ознак шару CNN подаються на вхід одному шару BiLSTM з 128 одиницями, щоб вивчити довгострокові залежності локальних ознак новинних статей. Далі йде вихідний шар з однією одиницею, активованою сигмоїдною функцією. За допомогою RNN можна вивчити і захопити часові та контекстуальні ознаки та довгострокові залежності вхідного тексту, а важливі локальні ознаки можна виявити, використовуючи потужність CNN у роботі з просторовими відношеннями [61, 62].

CNN-BiGRU: Схожа до моделі CNN-BiLSTM. Відмінність полягає в тому, що архітектуру із шаром BiLSTM замінено шаром BiGRU.

Гібрид (Hybrid): Це гібридна модель, яка об'єднує три моделі: один шар CNN із 128 нейронами та розміром ядра 5, за яким слідує максимальне згортання, потім шар BiLSTM з 128 одиницями, а далі шар BiGRU з 128 одиницями.

Ще один підхід з виявлення фейкових новин базується на застосуванні трансформерів. Однак їх використання на даний час поки що обмежене.

Для вирішення досліджуваної проблеми дослідники пропонували різні методи інтерпретації значення слова за допомогою векторів вбудовування. Методи на основі нейронних мереж, такі як Word2Vec і GloVe, загалом використовувалися для навчання векторів вбудовування слова з великих корпусів слів. Однак ці моделі вбудовування мають недолік у тому, що вони не враховують контекст і статичні вбудовування слів генеруються незалежно від їх контексту. Тому для досягнення більш точних результатів модель повинна бути здатною вловлювати семантичні та контекстуальні патерни. Більше того, вдосконалені моделі машинного навчання можуть автоматично видобувати семантичну інформацію з вхідних даних для виявлення фейкового контенту, але вони не можуть точно розпізнавати фейковий контент без глибокого розуміння тексту. Таким чином, в останні роки зросло зацікавлення до парадигми уваги. У галузі обробки природної мови спостерігається загальний зсув парадигми, спрямований на розробку набору моделей, які не лише підвищують точність, але й вирішують проблему відсутності маркованих даних.

Крім того, існує нагальна потреба в автоматичному виявленні фейкових новин. Це складна задача, оскільки існуючі моделі машинного навчання (до появи моделей на основі трансформерів) не забезпечували глибокого семантичного розуміння текстових вхідних даних. Це призвело до впровадження попередньо навчених мовних моделей на основі трансформерів. Використання таких моделей, навчених на великих немаркованих даних, для завдань класифікації тексту стає все більш популярним. Для адаптації до завдання наступного рівня над новими шарами нейронних мереж розташовуються попередньо навчені шари у мовних моделях [63]. У цьому випадку на верхньому рівні попередньо навчених мовних моделей (PLMs) додається повністю з'єднаний (FC) шар для цілей класифікації.

Ключовими моделями з потужним мовним представленням, навченим на величезних обсягах текстового корпусу, є моделі BERT [64] і RoBERTa [65].

BERT: BERT – модель, що використовує багаторівневий бідирекціональний трансформерний кодер, який одночасно моделює лівий і правий контексти [64]. У результаті BERT генерує вектори, які враховують контекст. BERT у подальшому надає можливість подолати однобічне обмеження, проводячи передпочаткове навчання з використанням невідосконаленого завдання передбачення, яке включає в себе маскову мовну модель (Masked Language Model, MLM), яка розуміє контекст і передбачає слова. Таким чином, модель може генерувати векторне представлення, яке захоплює загальну інформацію вихідного тексту. Семантичне представлення кожного слова у вхідному тексті можна покращити за допомогою механізму уваги, підсилюючи семантичне представлення на основі контексту слова. Механізм уваги відіграє важливу роль в архітектурі трансформера, оскільки надає різні ваги різним частинам тексту в залежності від їхнього внеску в результат. Функція уваги відображає запити та слідує за парами ключ-значення та векторами-результатами. Механізм уваги використовує функцію активації Softmax, яка нормалізує вхідні дані до значення між 0 і 1.

Незважаючи на те, що BERT містить мільйони параметрів (наприклад, BERTbase має 110 мільйонів параметрів, а BERTlarge - 340 мільйонів параметрів) [64], BERT є відносно ефективним для застосування у завданнях наступного рівня з використанням спільно налаштованих параметрів на основі попередньо навченої моделі.

RoBERTa [65]: RoBERTa - оптимізована версія підходу BERT. У цьому методі BERT перенавчається за допомогою: вдосконаленої методології навчання, включаючи видалення завдання передбачення наступного речення з попереднього навчання; використання у 10 разів більшої кількості даних, ніж BERT; введення динамічного маскування з більшими

пакетами даних, так що токени, які маскуються, змінюються під час навчання, на відміну від статичного маскування, використовуваного в BERT. Таким чином, RoBERTa відрізняється від BERT в способі підходу до попереднього навчання.

Аналіз функціонального аспекту застосування наведених методів передбачає проведення аналізу попередньої обробки вхідного тексту. Попередня обробка вхідного тексту включала в себе видалення стоп-слів і пунктуації. Текст проходив процес токенизації на токени і побудови словника на основі вивченої лексики в даному текстовому корпусі. Такий словник використовувався для відображення кожного токена в єдиний цілочисельний ідентифікатор. Отримані послідовності доповнювалися або обрізалися до фіксованої кількості записів, оскільки моделям необхідно було подавати вектори однакової довжини. При цьому недоліком є те, що при обрізанні послідовностей втрачалася деяка (корисна) інформація. Ці послідовності потім перетворювалися в фіксовані вектори вбудовування слова. Потім нейронні мережі ініціалізувалися контекстно-незалежними попередньо навченими моделями вбудовування слова, такими як Word2Vec і GloVe, та контекстно-інформованими попередньо навченими мовними моделями BERTbase. У класичних алгоритмах машинного навчання для перетворення токенизованих текстів в ознаки використовувалися CountVectorizer (CV) та TF-IDF, як статистичні здобувачі ознак для моделей машинного навчання.

Також для аналізу функціонального аспекту застосування наведених методів доцільно оцінити результати застосування описаних вище моделей при виявленні фейкових новин на різних масивах даних.

Аналіз результатів на наборі даних LIAR.

Як впливає з [40], найкращий результат точності, досягнутий на наборі даних LIAR, становив 63,9% для комбінації з ознаками TF-IDF. Типовий результат при цьому становить 62%. Найгірший результат склав 51,78% для DT з ембедінгами GloVe. Класифікатор не міг виявити деякі закономірності у вхідному тексті.

При проведенні порівняльної оцінки результатів різних моделей встановлено, що більшість моделей досягли точності не більше 62% з BERTbase, а модель CNN-BiLSTM з використанням ембедінгів BERTbase точності 63,06%. Найгірший результат було досягнуто для моделей на основі рекурентних мереж з ембедінгами Word2Vec.

Оскільки набір даних LIAR містить короткі політичні заяви, складно отримати корисні вказівки, які могли б допомогти розрізнити фейкові новини від реальних новин, зокрема при використанні складних моделей, таких як LSTM, оскільки це може збільшити ризик перенавчання.

Як зазначено в роботі [66], інформація новинної статті та розмір набору даних - це важливі фактори, що впливають на продуктивність моделей на основі рекурентних мереж. Такі моделі більш схильні долати перенавчання, коли в новинній статті надається достатньо інформації. Отримані результати показують, що класичні методи машинного навчання випереджають високо вдосконалені методи глибокого навчання на наборі даних LIAR, включаючи найновіші передові мовні моделі, такі як BERTbase та RoBERTabase.

Аналіз результатів на наборі даних FakeNewsNet.

Результати, які отримані на наборах даних PolitiFact і GossipCor, свідчать про те, що надійність має постійно високу точність, випереджаючи базові SAF та CNN навіть з комбінаціями соціальних вказівок та контенту новин на обох наборах даних. Найбільше значення точності (89,93%) на наборі даних PolitiFact було досягнуто за допомогою комбінації із CV як методу вилучення ознак. Ця модель (Ensemble+CV) виявилася другою за результатами на наборі даних GossipCor, з SVM+TF-IDF ($F1$ -оцінка 91,55%) з числа інших моделей на наборі даних GossipCor. Методи глибокого навчання, зокрема найновіші передові мовні моделі, забезпечили високу продуктивність у багатьох завданнях обробки природної мови. RoBERTabase показав найкращий результат на наборі даних PolitiFact з $F1$ -оцінкою 93,17%, тоді як результати точності (92%) були на рівні з передовою моделлю машинного навчання за допомогою представлень BERTbase. Для набору даних GossipCor CNN-BERTbase виявився найкращою моделлю (значення $F1$ 91,45%). Це свідчить про те,

що контекстно-орієнтовані моделі на основі трансформатора допомагають виявляти корисні закономірності для розрізнення фейкових новин від реальних. Оскільки набір даних GossipCop досить незбалансований, різні методи збалансування, такі як вибіркове збільшення та зменшення, можуть допомогти збалансувати набір даних і підвищити продуктивність виявлення.

Аналіз результатів на наборі даних COVID-19.

BERT ефективно може виявляти фейковий контент, оскільки він має можливість кодувати глибоку семантичну контекстуальну інформацію. За результатами досліджень можна зробити висновок, що модель BERTbase, до якої додано лінійний шар для класифікації, показала найкращі результати порівняно з аналогами та іншими класичними моделями машинного та глибокого навчання на наборі даних COVID-19. Другою за ефективністю на наборі даних COVID-19 була модель CNN-BERTbase.

У зв'язку з тим, що методи векторних просторів, такі як CV та TF-IDF, не враховують контекст, використання цих представлень з моделями машинного навчання ґрунтується на зовнішньому вигляді токенів при прийнятті остаточних рішень, незалежно від їхнього контексту. Результати дослідження свідчать про те, що моделі векторного простору неефективні у виявленні глибокої семантики та контекстуальних закономірностей, що містяться в користувацькому змісті, створеному на Twitter. Однією з головних переваг BERT (та його модифікацій) у випадку Twitter (де користувацький зміст часто містить орфографічні помилки, шум та скорочення), є використання підтокенів замість фіксованих токенів. Це ідеально підходить для використання з такими даними [67], оскільки воно оперує на рівні підтокенів замість стандартних контекст-незалежних векторних вбудов слів на рівні слова.

Оцінимо тепер функціональний аспект алгоритмів виявлення фейкових новин, що базуються на використанні результатів аналізу настрою новинного контенту й емоцій у коментарях користувачів.

Насамперед відмітимо, що перевірку моделей, що відповідають зазначеним алгоритмам, як правило, здійснюють на наборі даних Fakeddit.

Набір даних Fakeddit (<https://github.com/entitize/Fakeddit>, доступний на 22 лютого 2022 року) є великомасштабним та багатомодальним набором даних (текст та зображення), зібраним з соціальної медіа-платформи Reddit за період з 19 березня 2008 року по 24 жовтня 2019 року [68]. Цей набір даних складається з понад мільйона повідомлень з різних галузей. До цих повідомлень додаються різні ознаки, такі як зображення, коментарі, користувачі, домени та інші метадані. У цьому наборі даних міститься багато шуму та нульових значень. Одне повідомлення може містити кілька коментарів або не мати коментарів. Для кожного повідомлення дослідники надали три мітки, класифіковані двома, трьома та шістьма способами.

У роботі [69] відзначається, що існує зв'язок між настроєм опублікованих новин та правдивістю новин. На основі цього автори роботи використовували ознаку, засновану на настрої (відношення кількості позитивних слів до кількості негативних слів), для розвитку власної моделі виявлення фейкових новин. Для покращення точності визначення фейкових новин у [70] запропоновано нову стратегію, яка включає збагачення об'єднаного набору даних настроєм як ключовою ознакою. Ефективність запропонованої стратегії перевірялася на основі трьох різних наборів даних. Результати показали ефективність запропонованого рішення. У роботі [50] підтверджено, що різницю між фейковими та справжніми новинами можна відрізнити за допомогою подвійної емоції (емоція видавця та суспільна емоція). Автори цієї роботи запропонували «Ознаки подвійної емоції», щоб виразити подвійну емоцію та взаємодію між ними. Вони також показали, що запропоновані ними ознаки легко інтегруються в існуючі моделі виявлення фейкових новин.

У роботі [71] запропоновано стратегію EmoCred, модель на основі довгострокової пам'яті (LSTM), яка враховує емоційні сигнали для виявлення різниці між справжніми та фейковими твердженнями. Головним кроком EmoCred є вилучення емоційних сигналів з тверджень. Дослідники вивчали три різні методи визначення емоційних сигналів у

твердженнях: метод, який використовує сучасні лексикони емоцій та базується на лексоні (emoLexi); метод, який визначає інтенсивність емоцій у твердженнях (emoInt); метод нейронної мережі (NN), який вказує на рівень інтенсивності тверджень і представляє кількість емоційних реакцій, які це твердження може викликати у читачів (emoReact). Дослідження авторів зазначеної праці, в якому використані реальні набори даних, продемонструвало цінність емоційних сигналів при оцінці вірогідності.

У роботі [72] проведено класифікацію новин на реальні та фальшиві на основі аналізу емоцій у новинах за допомогою комбінації моделей, що включають у себе згорткові нейронні мережі (CNN) і мережі BI-LSTM з механізмом уваги. Результати застосування моделі виявилися кращими, ніж результати застосування інших моделей.

Нижче наведені результати застосування описаних вище моделей при виявленні фейкових новин на різних масивах даних.

У роботі [68] наведено багатомодальний набір даних Fakeddit, застосовано модель BERT для виявлення фейкових новин на основі тексту і техніки ResNet для виявлення фейкових новин на основі зображень. Дослідники виявили, що точність результатів моделі, побудованої на основі BERT і ResNet з використанням ознак як тексту, так і зображень, була кращою, ніж у моделі, яка використовує лише текст для виявлення фейкових новин.

У роботі [73] запропоновано модель виявлення фейкових новин, яка ґрунтується на DeepNet та реальних даних наборів даних BuzzFeed і Fakeddit. З використанням факторизації тензорів, яка інтегрує контент новин та дані, що базуються на соціальному контексті, DeepNet демонстрував кращі параметри, ніж поточні моделі виявлення фейкових новин. Результати показали, що використання комбінації ознак на основі соціального контексту і ознак контенту новин призводило до більш точних результатів DeepNet.

У роботі [74] також використано набір даних Fakeddit і представлено багатомодальну мережеву архітектуру, яка дозволяє об'єднувати різні рівні та види об'єднання інформації, включаючи не тільки текст заголовків, але і метадані та інший контент, що стосується заголовків новин. Їхня методологія для виявлення неправдивої інформації залежить від чотирьох модальностей вводу: основний текстовий контент новини або запису; додаткова інформація або реакція на основний контент (наприклад, коментарі); візуальний контент запису; будь-які інші доступні метадані. Для врахування унікальності фундаментальної структури модальностей, автори роботи вони об'єднали інформацію на різних рівнях. Результати запропонованої ними моделі були покращені завдяки додатковим модальностям, що свідчить про те, що вони надають цінну інформацію.

Унікальна мережа вилучення та мережа мислення, відома як SERN, а також механізм визначення уваги на основі речення, були наведені в роботі [75]. Автори роботи пояснили, що відповіді, надіслані різними читачами, містять як факти, так і деякі висновки. Вони використали графічну мережу мислення. Дослідники у своїй роботі використали набори даних Fakeddit і RHEME та вказали, що запропонована ними модель продемонструвала перспективні результати порівняно з іншими сучасними моделями.

У роботі [76] розроблено підхід, який використовує ознаки контенту новин та ознаки соціального контексту для виявлення фейкових новин. Підхід авторів цієї праці базується на архітектурі трансформатора, яка складається з двох блоків: блоку кодування для вилучення значущих представлень з даних фейкових новин та блоку декодування для передбачення майбутньої поведінки на основі минулих даних. Вони провели обширні випробування на даних Fakeddit та NELEA-GT-2019, щоб оцінити ефективність запропонованого ними підходу. Вони використовували стратегію недорогого семпсування, яка включає видалення записів з більшості класу з метою наближення більшості класу до меншості класу, щоб вирішити проблему нерівноваги даних в обох наборах даних. Автори роботи [76] використовували ознаки соціального контексту набору даних Fakeddit. За результатами застосування їхньої моделі можна зробити висновок, що для оптимальної роботи моделі потрібно враховувати як контент новин, так і соціальний контекст.

За результатами порівняльного оцінювання наведених моделей встановлено, що найефективніша модель виявлення, яка використовується на валідаційному наборі даних, це

Bi-LSTM зі значенням AUC 96,77% та 97,81% за $F1$ -оцінкою. Проте, навіть для неї мають місце труднощі при роботі з незбалансованим набором даних.

Таким чином, проведений функціональний аналіз алгоритмів машинного (ML) та глибокого (DL) навчання, а також алгоритмів виявлення фейкових новин, що базуються на використанні результатів аналізу настрою новинного контенту й емоцій у коментарях користувачів, дозволяє зробити такі висновки: на даний час жодна з проаналізованих існуючих моделей виявлення фейкових новин не є універсальною для різних наборів даних; різні моделі та їх комбінації мають як переваги, так і недоліки, які не дозволяють ефективно застосовувати моделі; зважаючи на переваги та недоліки проаналізованих моделей, за доцільне вбачається дослідити питання про можливість поєднання описаних у даній роботі підходів до виявлення фейкових новин; поєднання підходів може розглядатися як на рівні комбінування методів з різних підходів, так і на рівні комбінування їх функціоналу на базі окремого методу; при проведенні дослідження щодо удосконалення моделей доцільно детермінувати метрику продуктивності методів і встановити масиви даних, на базі яких проводитиметься перевірка ефективності запропонованого методу.

Метрика для оцінки ефективності методів виявлення фейкових новин.

За результатами проведеного аналізу в якості показників продуктивності методів виявлення фейкових новин вбачається за доцільне обрати точність (A), точність (P), чутливість (R), $F1$ -показник, а також площу під кривою ROC (AUC).

Точність (A) - це міра здатності класифікатора правильно класифікувати інформацію як фейкову або реальну. Точність (A) можна оцінити так

$$A_{accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \cdot \quad (1)$$

Точність (P) - це міра точності класифікатора, згідно якої низьке значення вказує на велику кількість помилкових позитивних результатів. Точність (P) представляє собою кількість позитивних прогнозів, поділену на загальну кількість позитивних значень класу, передбачених, і обчислюється за формулою

$$P_{recision} = \frac{TP}{TP + FP} \cdot \quad (2)$$

Чутливість (R) вважається мірою повноти класифікатора (наприклад, низьке значення чутливості вказує на багато помилкових негативних результатів), де кількість справжніх позитивів ділиться на суму справжніх позитивів і кількості помилкових негативів:

$$R_{ecall} = \frac{TP}{TP + FN} \cdot \quad (3)$$

$F1$ -показник ($F1$) обчислюється як зважена гармонічна середня точності і чутливості класифікатора:

$$F1 = \frac{2 \cdot P_{recision} \cdot R_{ecall}}{P_{recision} + R_{ecall}} = \frac{2 \cdot TP}{2 \cdot TP + FP + FN} \cdot \quad (4)$$

У формулах (1)-(4) TP , TN , FP , FN - це відповідно справжні позитиви, справжні негативи, помилкові позитиви і помилкові негативи.

Площа під ROC -кривою, відома як AUC , є мірою, яка використовується для порівняння алгоритмів навчання та побудови оптимальних моделей навчання. AUC , що близька до 1, вказує на перевагу системи, яка може точно відрізнити реальні та фейкові новини, тоді як AUC , що близька до 0, вказує на слабку систему (тобто система вважатиме всі фейкові новини реальними і навпаки) [38]. Наприклад, якщо AUC дорівнює 0,9, це означає, що модель на 90% може відрізнити негативні і позитивні класи. AUC зазвичай використовується в задачах незбалансованої класифікації [37], таких як виявлення фейкових новин.

Міра AUC може бути знайдена з виразу

$$AUC = \frac{1 - FPR + TPR}{2} \cdot \quad (5)$$

Справжній позитивний рівень або TPR - це скорочення, яке вказує на відсоток позитивних прикладів, які успішно класифіковані. На відміну від цього, FPR , який вказує на хибно позитивний рівень, це відношення випадків, які були неправильно класифіковані як негативні, до всіх інших випадків [39].

Авторські ідеї щодо комплексування потенціалу алгоритмів машинного (ML) та глибокого (DL) навчання, а також результатів аналізу настрою новинного контенту й емоцій у коментарях користувачів.

З урахуванням результатів проведеного аналізу авторам видається, що подальше дослідження механізмів виявлення фейкових новин можна здійснювати за двома напрямками (ідеями).

Ідея 1.

Ідея 1 базується на реалізації механізму комбінування методів машинного (ML) та глибокого (DL) навчання, а також результатів аналізу настрою новинного контенту й емоцій у коментарях користувачів. Однак доцільне комбінування має враховувати можливість забезпечення певної ефективності виявлення фейкових новин, певного рівня значень показників обраної метрики, а також певний рівень функціональних характеристик авторського методу.

Ідея 2.

Ідея 2 базується на реалізації механізму комбінування функціоналу ефективних існуючих методів на базі окремо обраного методу. При цьому важливим завданням є коректне обрання базового методу та вибір того функціоналу існуючих методів з числа аналізованих, який би забезпечив достатній рівень ефективності реалізації авторської ідеї на різних наборах даних.

Формалізація задач виявлення фейкових новин, що реалізує авторські ідеї.

Для перевірки гіпотези щодо ефективності авторських ідей 1, 2 доцільною є формалізація постановки задач. Здійснимо її.

Формалізація задачі згідно ідеї 1.

Нехай задано множину новинних статей, висловлювань або твітів $A = \{a_1, a_2, \dots, a_k\}$, де k – це довжина вхідного тексту, із невідомими початковими ознаками. Завдання полягає у встановленні фейковості чи реальності контенту елементів множини A на основі застосування до ознак кожного елемента множини A авторської моделі.

Авторська модель являє собою комбінацію алгоритмів машинного (ML) та глибокого (DL) навчання, а також алгоритмів виявлення фейкових новин на основі аналізу настрою новинного контенту й емоцій у коментарях користувачів. Умовне позначення цих алгоритмів таке: $M_1, M_2, \dots, M_n$. Їх кількість рівна n . Серед елементів $M_i, \left(i = \overline{1, n}\right)$ можуть бути «чисті»

алгоритми машинного (ML) та глибокого (DL) навчання, або їх комбінації, що досліджені на даний час, а також «чисті» алгоритми виявлення фейкових новин на основі аналізу настрою новинного контенту й емоцій у коментарях користувачів, що проаналізовані вище, або їх можливі комбінації.

Нехай кожен з алгоритмів $M_i, \left(i = \overline{1, n}\right)$ на наборі даних $j, \left(j = \overline{1, s}\right)$ має певну ефективність $E_i^{(j)}, \left(i = \overline{1, n}, j = \overline{1, s}\right)$.

Зважаючи на те, що для кожного алгоритму $M_i, \left(i = \overline{1, n}\right)$ на окремих наборах даних $j, \left(j = \overline{1, s}\right)$ відомими є величини $A_{accuracy.i}^{(j)}, P_{recision.i}^{(j)}, R_{ecall.i}^{(j)}, F1_i^{(j)}, AUC_i^{(j)}$ (визначаються із використанням формул (1)-(5)), то ефективність алгоритму $M_i, \left(i = \overline{1, n}\right)$ на масиві

даних $j, \left(j = \overline{1, s} \right)$ можна представити у вигляді

$$E_i^{(j)} = g_i^{(j)}(A_{accuracy.i}^{(j)}, P_{recision.i}^{(j)}, R_{ecall.i}^{(j)}, F1_i^{(j)}, AUC_i^{(j)}). \quad (6)$$

Тоді ефективність кожного алгоритму $M_i, \left(i = \overline{1, n} \right)$ на довільному наборі даних може являти собою функцію $E_i = f(E_i^{(1)}, E_i^{(2)}, \dots, E_i^{(s)})$.

А отже, ефективність авторського алгоритму може бути представлена у вигляді

$$E = \bar{f}(E_1, \dots, E_n) = \bar{f}(E_1^{(1)}, \dots, E_n^{(1)}, \dots, E_1^{(s)}, \dots, E_n^{(s)}). \quad (7)$$

Зважаючи на фізичний зміст задачі виявлення фейкових новин, при опрацюванні авторської моделі необхідним є підбір таких моделей $M_i, \left(i = \overline{1, n} \right)$, застосування яких дозволило б у межах заданого часу розв'язати задачу, а також не перевищити задану обчислювальну складність алгоритму.

Нехай для кожної моделі $M_i, \left(i = \overline{1, n} \right)$ відомими є величини:

$T_i^{(j)}$ - максимальна тривалість роботи моделі $M_i, \left(i = \overline{1, n} \right)$ на масиві даних $j, \left(j = \overline{1, s} \right)$;

C_i - обчислювальна складність алгоритму $M_i, \left(i = \overline{1, n} \right)$.

Тоді загальний час роботи $M_i, \left(i = \overline{1, n} \right)$ на всіх наборах даних $j, \left(j = \overline{1, s} \right)$ можна представити у вигляді

$$T_i = \tilde{f}(T_i^{(1)}, \dots, T_i^{(s)}), \quad (8)$$

а загальний час роботи авторської моделі на всіх наборах даних може бути представлений так:

$$T = \hat{f}(T_1, \dots, T_n). \quad (9)$$

З урахуванням введених позначень, обчислювальну складність авторської моделі можна описати функціональною залежністю

$$C = \bar{f}(C_1, \dots, C_n). \quad (10)$$

А отже, задачу побудови авторської моделі можна сформулювати, як оптимізаційну задачу вибору з числа алгоритмів $M_i, \left(i = \overline{1, n} \right)$ тих з них, які б забезпечили

$$E \rightarrow \max, \quad (11)$$

де E визначається за формулою (7), при виконанні умов

$$T \leq T_{ep}, \quad (12)$$

$$C \leq C_{ep}, \quad (13)$$

де T і C знаходяться, відповідно, з формул (9) і (10).

У виразах (12), (13) T_{ep} , C_{ep} - це задані граничні значення тривалості роботи авторської моделі на масиві $A = \{a_1, a_2, \dots, a_k\}$ і обчислювальної складності моделі.

Слід зауважити, що в авторській моделі (1)-(13) виявлення фейкових новин невідомими є функціональні залежності $g_i^{(j)}$, f , $\bar{f}$, $\tilde{f}$, $\hat{f}$, $\bar{f}$. Їх встановлення є окремим завданням.

Як приклад, зважаючи на ймовірнісний зміст задачі виявлення фейкових новин, ефективність E в (7) може являти собою таку функціональну залежність

$$E = 1 - \prod_{i,j} \left(1 - \overline{E_i^{(j)}} \right), \left(i = \overline{1, n}, j = \overline{1, s} \right). \quad (14)$$

Застосування формули (14) для виявлення ефективності E не становить значних обчислювальних труднощів при наявності даних щодо величин (6).

Слід також зауважити, що суть задачі легко оцінити з даних, що наведені в табл. 1.

Таблиця 1

Існуючі моделі $M_i, \left(i = \overline{1, n} \right)$	Ефективність існуючих моделей на досліджуваних наборах даних $j, \left(j = \overline{1, s} \right)$				Максимальна тривалість роботи моделі $M_i, \left(i = \overline{1, n} \right)$ на масиві даних $j, \left(j = \overline{1, s} \right)$				Обчислювальна складність алгоритму $M_i, \left(i = \overline{1, n} \right)$
	$j = 1$	$j = 2$	...	$j = s$	$j = 1$	$j = 2$	...	$j = s$	
M_1	$E_1^{(1)}$	$E_1^{(2)}$	...	$E_1^{(s)}$	$T_1^{(1)}$	$T_1^{(2)}$	...	$T_1^{(s)}$	C_1
M_2	$E_2^{(1)}$	$E_2^{(2)}$	...	$E_2^{(s)}$	$T_2^{(1)}$	$T_2^{(2)}$	...	$T_2^{(s)}$	C_2
...	...	...	...	...	...	...	...	...	...
M_n	$E_n^{(1)}$	$E_n^{(2)}$	...	$E_n^{(s)}$	$T_n^{(1)}$	$T_n^{(2)}$	...	$T_n^{(s)}$	C_n
Граничні значення окремих величин					T_{zp}				C_{zp}

Формалізація задачі згідно ідеї 2.

Нехай задано множину новинних статей, висловлювань або твітів $A = \{a_1, a_2, \dots, a_k\}$, де k – це довжина вхідного тексту, із відомими початковими ознаками. Завдання полягає у встановленні фейковості чи реальності контенту елементів множини A на основі застосування до ознак кожного елемента множини A авторської моделі.

Авторська модель являє собою комбінацію алгоритмів машинного (ML) та глибокого (DL) навчання з алгоритмами виявлення фейкових новин на основі аналізу настрою новинного контенту й емоцій у коментарях користувачів.

Умовне позначення алгоритмів машинного (ML) та глибокого (DL) навчання (чи їх досліджених комбінацій) таке: $M_i^{(1)}, \left(i = \overline{1, l} \right)$. Умовне позначення алгоритмів виявлення фейкових новин на основі аналізу настрою новинного контенту й емоцій у коментарях користувачів (чи їх досліджених комбінацій) таке: $M_j^{(2)}, \left(j = \overline{1, r} \right)$.

Авторська модель являє собою поєднання однієї з моделей з масиву $M_i^{(1)}, \left(i = \overline{1, l} \right)$ із однією з моделей масиву $M_j^{(2)}, \left(j = \overline{1, r} \right)$. Позначимо можливі авторські моделі як $M_k = M_i^{(1)} \cup M_j^{(2)}, \left(k = \overline{1, l \cdot r} \right)$.

Нехай кожен з алгоритмів $M_i^{(1)}, \left(i = \overline{1, l} \right)$ на визначеному наборі даних має певну ефективність $E_i^{(1)}, \left(i = \overline{1, l} \right)$, а кожен з алгоритмів $M_j^{(2)}, \left(j = \overline{1, r} \right)$ ефективність $E_j^{(2)}, \left(j = \overline{1, r} \right)$.

Зазначені ефективності можуть бути знайдені з урахуванням формул (1)-(5), наприклад у вигляді

$$E_i^{(1)} = g_i^{(1)}(A_{accuracy.i}^{(1)}, P_{recision.i}^{(1)}, R_{ecall.i}^{(1)}, F1_i^{(1)}, AUC_i^{(1)}), \quad (15)$$

$$E_j^{(2)} = g_j^{(2)}(A_{accuracy.j}^{(2)}, P_{recision.j}^{(2)}, R_{ecall.j}^{(2)}, F1_j^{(2)}, AUC_j^{(2)}). \quad (16)$$

Із урахуванням (15)-(16) ефективність авторських моделей $M_k, \left(k = \overline{1, l \cdot r}\right)$ може бути подана, як

$$E_k = f(E_i^{(1)}, E_j^{(2)}). \quad (17)$$

Зважаючи на фізичний зміст задачі виявлення фейкових новин, при опрацюванні авторської моделі необхідним є підбір такої моделі з масиву $M_k = M_i^{(1)} \cup M_j^{(2)}, \left(k = \overline{1, l \cdot r}\right)$, застосування якої дозволило б у межах заданого часу розв'язати задачу, а також не перевищити задану обчислювальну складність алгоритму.

Нехай для кожної моделі $M_i^{(1)}, \left(i = \overline{1, l}\right)$ відомими є величини:

$T_i^{(1)}$ - максимальна тривалість роботи моделі $M_i^{(1)}, \left(i = \overline{1, l}\right)$ на визначеному досліджуваному масиві даних;

$C_i^{(1)}$ - обчислювальна складність алгоритму $M_i^{(1)}, \left(i = \overline{1, l}\right)$.

А для кожної моделі $M_j^{(2)}, \left(j = \overline{1, r}\right)$ ці величини такі:

$T_j^{(2)}$ - максимальна тривалість роботи моделі $M_j^{(2)}, \left(j = \overline{1, r}\right)$ на визначеному досліджуваному масиві даних;

$C_j^{(2)}$ - обчислювальна складність алгоритму $M_j^{(2)}, \left(j = \overline{1, r}\right)$.

Тоді загальний час роботи $M_k, \left(k = \overline{1, l \cdot r}\right)$ можна представити у вигляді

$$T_k = \tilde{f}(T_i^{(1)}, T_j^{(2)}). \quad (18)$$

З урахуванням введених позначень, обчислювальну складність авторської моделі можна описати функціональною залежністю

$$C_k = \bar{f}(C_i^{(1)}, C_j^{(2)}). \quad (19)$$

А отже, задачу побудови авторської моделі можна сформулювати, як оптимізаційну задачу вибору з числа алгоритмів $M_k, \left(k = \overline{1, l \cdot r}\right)$ того з них, який би забезпечував

$$E_k \rightarrow \max, \quad (20)$$

де E_k визначається за формулою (17), при виконанні умов

$$T_k \leq T_{k.zp}, \quad (21)$$

$$C_k \leq C_{k.zp}, \quad (22)$$

де T_k і C_k знаходяться, відповідно, з формул (18) і (19).

У виразах (21), (22) $T_{k.zp}$, $C_{k.zp}$ - це задані граничні значення тривалості роботи

авторської моделі $M_k, \left(k = \overline{1, l \cdot r}\right)$ на масиві $A = \{a_1, a_2, \dots, a_k\}$ і обчислювальної складності моделі.

Слід зауважити, що в авторській моделі (1)-(5), (15)-(22) виявлення фейкових новин невідомими є функціональні залежності $g_i^{(1)}, g_j^{(2)}, f, \tilde{f}, \bar{f}$. Їх встановлення є окремим завданням.

Висновки з даного дослідження і перспективи подальшого розвитку. Таким чином, у ході дослідження проаналізовано ряд положень, які дозволили сформулювати авторські ідеї щодо можливих підходів до формування нових моделей виявлення фейкових новин. З урахуванням проведеного аналізу можна зробити висновок, що ці ідеї можуть мати перспективу щодо можливого поліпшення існуючих результатів. Проведена формалізація авторських ідей дозволяє наблизитися до формування механізмів перевірки сформульованих гіпотез.

Перспективами подальших розвідок вбачається програмування та вирішення сформульованих авторських оптимізаційних задач, що стосуються формування удосконалених моделей виявлення фейкових новин, а також вирішення окремих часткових завдань стосовно визначення функціональних залежностей, які визначають окремі складові цих моделей.

ЛІТЕРАТУРА (REFERENCES):

1. Bondielli, A.; Marcelloni, F. A survey on fake news and rumour detection techniques. *Inf. Sci.* 2019, 497, 38–55. [CrossRef]
2. Islam, M.R.; Liu, S.; Wang, X.; Xu, G. Deep learning for misinformation detection on online social networks: A survey and new perspectives. *Soc. Netw. Anal. Min.* 2020, 10, 82. [CrossRef] [PubMed]
3. Bahad, P.; Saxena, P.; Kamal, R. Fake News Detection using Bi-directional LSTM-Recurrent Neural Network. *Procedia Comput. Sci.* 2019, 165, 74–82. [CrossRef]
4. Machová, K.; Mach, M.; Porezaný, M. Deep Learning in the Detection of Disinformation about COVID-19 in Online Space. *Sensors* 2022, 22, 9319. [CrossRef]
5. Liu, Y.; Wu, Y.-F.B. Fned: A deep network for fake news early detection on social media. *ACM Trans. Inf. Syst. (TOIS)* 2020, 38, 1–33. [CrossRef]
6. Zhou, X.; Jain, A.; Phoha, V.V.; Zafarani, R. Fake News Early Detection: An Interdisciplinary Study. *arXiv* 2019, arXiv:1904.11679.
7. DataReportal. Digital 2021 Global Digital Overview; DataReportal: Singapore, 2021.
8. Kwak, H.; Lee, C.; Park, H.; Moon, S. What is Twitter, a Social Network or a News Media? In *Proceedings of the 19th International Conference on World Wide Web; Association for Computing Machinery: New York, NY, USA*, 2010; pp. 591–600. [CrossRef]
9. Friggeri, A.; Adamic, L.; Eckles, D.; Cheng, J. Rumor cascades. In *Proceedings of the International AAAI Conference on Web and Social Media, Ann Arbor, MI, USA*, 1–4 June 2014; Volume 8.
10. Zhou, X.; Zafarani, R. A Survey of Fake News: Fundamental Theories, Detection Methods, and Opportunities. *ACM Comput. Surv.* 2020, 53, 1–40. [CrossRef]
11. Conroy, N.K.; Rubin, V.L.; Chen, Y. Automatic deception detection: Methods for finding fake news. *Proc. Assoc. Inf. Sci. Technol.* 2015, 52, 1–4. [CrossRef]
12. Habib, A.; Asghar, M.Z.; Khan, A.; Habib, A.; Khan, A. False information detection in online content and its role in decision making: A systematic literature review. *Soc. Netw. Anal. Min.* 2019, 9, 50. [CrossRef]
13. Sansonetti, G.; Gasparetti, F.; D’aniello, G.; Micarelli, A. Unreliable Users Detection in Social Media: Deep Learning Techniques for Automatic Detection. *IEEE Access* 2020, 8, 213154–213167. [CrossRef]

14. Vosoughi, S.; Roy, D.; Aral, S. The spread of true and false news online. *Science* 2018, 359, 1146–1151. [CrossRef]
15. Zhao, Z.; Resnick, P.; Mei, Q. Enquiring Minds: Early Detection of Rumors in Social Media from Enquiry Posts. In *Proceedings of the 24th International Conference on World Wide Web; International World Wide Web Conferences Steering Committee: Geneva, Switzerland, 2015*; pp. 1395–1405. [CrossRef]
16. Kumar, S.; West, R.; Leskovec, J. Disinformation on the web: Impact, characteristics, and detection of wikipedia hoaxes. In *Proceedings of the 25th International Conference on World Wide Web, Montreal, QC, Canada, 11–15 April 2016*; pp. 591–602.
17. Potthast, M.; Kiesel, J.; Reinartz, K.; Bevendorff, J.; Stein, B. A stylometric inquiry into hyperpartisan and fake news. *arXiv* 2017, arXiv:1702.05638.
18. Tchakounté, F.; Calvin, K.A.; Ari, A.A.A.; Mbogne, D.J.F.J.J.o.K.S.U.-C.; Sciences, I. A smart contract logic to reduce hoax propagation across social media. *J. King Saud Univ.-Comput. Inf. Sci.* 2020, 34, 3070–3078. [CrossRef]
19. Rath, B.; Gao, W.; Ma, J.; Srivastava, J. Utilizing computational trust to identify rumor spreaders on Twitter. *Soc. Netw. Anal. Min.* 2018, 8, 64. [CrossRef]
20. Vosoughi, S.; Roy, D.; Aral, S. The spread of true and false news online. *Science* 2018, 359, 1146–1151. [CrossRef]
21. Al-Rakhami, M.S.; Al-Amri, A.M. Lies Kill, Facts Save: Detecting COVID-19 Misinformation in Twitter. *IEEE Access* 2020, 8, 155961–155970. [CrossRef]
22. Alkhodair, S.A.; Ding, S.H.; Fung, B.C.; Liu, J. Detecting breaking news rumors of emerging topics in social media. *Inf. Process. Manag.* 2020, 57, 102018. [CrossRef]
23. Zubair, T.; Raquib, A.; Qadir, J. Combating Fake News, Misinformation, and Machine Learning Generated Fakes: Insight’s from the Islamic Ethical Tradition. *ICR J.* 2019, 10, 189–212. [CrossRef]
24. Allcott, H.; Gentzkow, M. Social media and fake news in the 2016 election. *J. Econ. Perspect.* 2017, 31, 211–236. [CrossRef]
25. Shu, K.; Sliva, A.; Wang, S.; Tang, J.; Liu, H. Fake News Detection on Social Media: A Data Mining Perspective. *arXiv* 2017, arXiv:1708.01967.
26. Trends, G. “Fake News—Explore—Google Trends”. Available online: <https://trends.google.com/trends/explore?date=2010-01-01%202022-07-14&q=%22fake%20news%22> (accessed on 20 July 2022).
27. Langin, K. Fake news spreads faster than true news on Twitter—Thanks to people, not bots. *Sci. Mag.* 2018. Available online: <https://www.science.org/content/article/fake-news-spreads-faster-true-news-twitter-thanks-people-not-bots> (accessed on 20 February 2022).
28. Zubiaga, A.; Aker, A.; Bontcheva, K.; Liakata, M.; Procter, R. Detection and Resolution of Rumours in Social Media: A Survey. *ACM Comput. Surv.* 2018, 51, 1–36. [CrossRef]
29. Evolvi, G. Hate in a tweet: Exploring internet-based islamophobic discourses. *Religions* 2018, 9, 307. [CrossRef]
30. Al-Makhadmeh, Z.; Tolba, A. Automatic hate speech detection using killer natural language processing optimizing ensemble deep learning approach. *Computing* 2020, 102, 501–522. [CrossRef]
31. Feng, S.; Banerjee, R.; Choi, Y. Syntactic Stylometry for Deception Detection. In *Proceedings of the 50th Annual Meeting of the Association for Computational Linguistics (Volume 2: Short Papers); Association for Computational Linguistics: Jeju Island, Republic of Korea, 2012*; pp. 171–175.
32. de Oliveira, N.R.; Medeiros, D.S.; Mattos, D.M. A sensitive stylistic approach to identify fake news on social networking. *IEEE Signal Process. Lett.* 2020, 27, 1250–1254. [CrossRef]
33. Zhou, X.; Jain, A.; Phoha, V.V.; Zafarani, R. Fake news early detection: A theory-driven model. *Digit. Threat. Res. Pract.* 2020, 1, 1–25. [CrossRef]
34. Lin, L.; Chen, Z. Social rumor detection based on multilayer transformer encoding blocks. *Concurr. Comput. Pract. Exp.* 2021, 33, e6083. [CrossRef]

35. Wang, W.Y. “Liar, Liar Pants on Fire”: A New Benchmark Dataset for Fake News Detection. arXiv 2017, arXiv:1705.00648.
36. Patwa, P.; Sharma, S.; Pykl, S.; Guptha, V.; Kumari, G.; Akhtar, M.S.; Ekbal, A.; Das, A.; Chakraborty, T. Fighting an infodemic: COVID-19 fake news dataset. In Proceedings of the International Workshop on Combating Online Hostile Posts in Regional Languages during Emergency Situation; Springer: Berlin/Heidelberg, Germany, 2021; pp. 21–29.
37. Eke, C.I.; Norman, A.A.; Shuib, L.; Nweke, H.F. Sarcasm identification in textual data: Systematic review, research challenges and open directions. *Artif. Intell. Rev.* 2020, 53, 4215–4258. [CrossRef]
38. Alonso, M.A.; Vilares, D.; Gómez-Rodríguez, C.; Vilares, J. Sentiment analysis for fake news detection. *Electronics* 2021, 10, 1348. [CrossRef]
39. Elhadad, M.K.; Li, K.F.; Gebali, F. Detecting Misleading Information on COVID-19. *IEEE Access* 2020, 8, 165201–165215. [CrossRef]
40. Alghamdi, O.; Lin, Y.; Luo, S.: A comparative study of machine learning and deep learning techniques for fake news detection. *Information* 2022, 13, 576, 28 p.
41. Guo, M.; Xu, Z.; Liu, L.; Guo, M.; Zhang, Y. An Adaptive Deep Transfer Learning Model for Rumor Detection without Sufficient Identified Rumors. *Math. Probl. Eng.* 2020, 2020, 7562567. [CrossRef]
42. Varshney, D.; Vishwakarma, D.K. Vishwakarma, Hoax news-inspector: A real-time prediction of fake news using content resemblance over web search results for authenticating the credibility of news articles. *J. Ambient Intell. Humaniz. Comput.* 2020, 12, 8961–8974. [CrossRef]
43. Kim, Y.; Kim, H.K.; Kim, H.; Hong, J.B. Do Many Models Make Light Work? Evaluating Ensemble Solutions for Improved Rumor Detection. *IEEE Access* 2020, 8, 150709–150724. [CrossRef]
44. Yaakub, M.R.; Latiffi, M.I.A.; Zaabar, L.S. A review on sentiment analysis techniques and applications. *IOP Conf. Ser. Mater. Sci. Eng.* 2019, 551, 012070. [CrossRef]
45. Santhoshkumar, S.; Babu, L.D. Earlier detection of rumors in online social networks using certainty-factor-based convolutional neural networks. *Soc. Netw. Anal. Min.* 2020, 10, 20. [CrossRef]
46. Tian, L.; Zhang, X.; Wang, Y.; Liu, H. Early detection of rumours on twitter via stance transfer learning. In *Advances in Information Retrieval: 42nd European Conference on IR Research, ECIR 2020, Lisbon, Portugal, 14–17 April 2020, Proceedings, Part I 42*; Springer: Cham, Switzerland, 2020; Volume 12035, p. 575.
47. Albahar, M. A hybrid model for fake news detection: Leveraging news content and user comments in fake news. *IET Inf. Secur.* 2021, 15, 169–177. [CrossRef]
48. Ghanem, B.; Rosso, P.; Rangel, F. An emotional analysis of false information in social media and news articles. *ACM Trans. Internet Technol. (TOIT)* 2020, 20, 1–18. [CrossRef]
49. Kumari, R.; Ashok, N.; Ghosal, T.; Ekbal, A. What the fake? Probing misinformation detection standing on the shoulder of novelty and emotion. *Inf. Process. Manag.* 2022, 59, 102740. [CrossRef]
50. Zhang, X.; Cao, J.; Li, X.; Sheng, Q.; Zhong, L.; Shu, K. Mining dual emotion for fake news detection. In *Proceedings of the WWW '21: The Web Conference 2021, Ljubljana, Slovenia, 19–23 April 2021*; pp. 3465–3476.
51. Zimbra, D.; Abbasi, A.; Zeng, D.; Chen, H. The state-of-the-art in Twitter sentiment analysis: A review and benchmark evaluation. *ACM Trans. Manag. Inf. Syst. (TMIS)* 2018, 9, 1–29. [CrossRef]
52. Feng, Z. Hot news mining and public opinion guidance analysis based on sentiment computing in network social media. *Pers. Ubiquitous Comput.* 2019, 23, 373–381. [CrossRef]
53. Imran, A.S.; Daudpota, S.M.; Kastrati, Z.; Batra, R. Cross-cultural polarity and emotion detection using sentiment analysis and deep learning on COVID-19 related tweets. *IEEE Access* 2020, 8, 181074–181090. [CrossRef]
54. Pota, M.; Ventura, M.; Catelli, R.; Esposito, M. An effective BERT-based pipeline for Twitter sentiment analysis: A case study in Italian. *Sensors* 2020, 21, 133. [CrossRef]

55. Dang, C.N.; Moreno-García, M.N.; Prieta, F.D.L. An approach to integrating sentiment analysis into recommender systems. *Sensors* 2021, 21, 5666. [CrossRef]
56. Li, Q.; Hu, Q.; Lu, Y.; Yang, Y.; Cheng, J. Multi-level word features based on CNN for fake news detection in cultural communication. *Pers. Ubiquitous Comput.* 2020, 24, 259–272.
57. Correia, F.; Madureira, A.M.; Bernardino, J. Deep Neural Networks Applied to Stock Market Sentiment Analysis. *Sensors* 2022, 22, 4409. [CrossRef] [PubMed]
58. Subramani, S.; Wang, H.; Vu, H.Q.; Li, G. Domestic violence crisis identification from facebook posts based on deep learning. *IEEE Access* 2018, 6, 54075–54085. [CrossRef]
59. Hochreiter, S.; Schmidhuber, J. Long short-term memory. *Neural Comput.* 1997, 9, 1735–1780. [CrossRef]
60. Cho, K.; van Merriënboer, B.; Gulcehre, C.; Bahdanau, D.; Bougares, F.; Schwenk, H.; Bengio, Y. Learning Phrase Representations using RNN Encoder-Decoder for Statistical Machine Translation. *arXiv* 2014, arXiv:1406.1078.
61. Zhang, X.; Chen, F.; Huang, R. A combination of RNN and CNN for attention-based relation classification. *Procedia Comput. Sci.* 2018, 131, 911–917. [CrossRef]
62. Zhou, C.; Sun, C.; Liu, Z.; Lau, F. A C-LSTM neural network for text classification. *arXiv* 2015, arXiv:1511.08630.
63. Gururangan, S.; Marasović, A.; Swayamdipta, S.; Lo, K.; Beltagy, I.; Downey, D.; Smith, N.A. Don't stop pretraining: Adapt language models to domains and tasks. *arXiv* 2020, arXiv:2004.10964.
64. Devlin, J.; Chang, M.W.; Lee, K.; Toutanova, K. Bert: Pre-training of deep bidirectional transformers for language understanding. *arXiv* 2018, arXiv:1810.04805.
65. Liu, Y.; Ott, M.; Goyal, N.; Du, J.; Joshi, M.; Chen, D.; Levy, O.; Lewis, M.; Zettlemoyer, L.; Stoyanov, V. Roberta: A robustly optimized bert pretraining approach. *arXiv* 2019, arXiv:1907.11692.
66. Khan, J.Y.; Khondaker, M.T.I.; Afroz, S.; Uddin, G.; Iqbal, A. A benchmark study of machine learning models for online fake news detection. *Mach. Learn. Appl.* 2021, 4, 100032. [CrossRef]
67. Horne, L.; Matti, M.; Pourjafar, P.; Wang, Z. GRUBERT: A GRU-Based Method to Fuse BERT Hidden Layers for Twitter Sentiment Analysis. In *Proceedings of the 1st Conference of the Asia-Pacific Chapter of the Association for Computational Linguistics and the 10th International Joint Conference on Natural Language Processing: Student Research Workshop; Association for Computational Linguistics: Suzhou, China, 2020; pp. 130–138*
68. Nakamura, K.; Levy, S.; Wang, W.Y. r/fakeddit: A new multimodal benchmark dataset for fine-grained fake news detection. *arXiv* 2019, arXiv:1911.03854.
69. Ajao, O.; Bhowmik, D.; Zargari, S. Sentiment aware fake news detection on online social networks. In *Proceedings of the ICASSP 2019—2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Brighton, UK, 12–17 May 2019; pp. 2507–2511*.
70. Bhutani, B.; Rastogi, N.; Sehgal, P.; Purwar, A. Fake news detection using sentiment analysis. In *Proceedings of the 2019 Twelfth International Conference on Contemporary Computing (IC3), Noida, India, 8–10 August 2019; pp. 1–5*.
71. Giachanou, A.; Rosso, P.; Crestani, F. Leveraging emotional signals for credibility detection. In *Proceedings of the 42nd International ACM SIGIR Conference on Research and Development in Information Retrieval, Paris, France, 21–25 July 2019; pp. 877–880*.
72. Kumar, S.; Asthana, R.; Upadhyay, S.; Upreti, N.; Akbar, M. Fake news detection using deep learning models: A novel approach. *Trans. Emerg. Telecommun. Technol.* 2020, 31, e3767. [CrossRef]
73. Kaliyar, R.K.; Kumar, P.; Kumar, M.; Narkhede, M.; Namboodiri, S.; Mishra, S. DeepNet: An efficient neural network for fake news detection using news-user engagements. In *Proceedings of the 2020 5th International Conference on Computing, Communication and Security (ICCCS), Patna, India, 14–16 October 2020; pp. 1–6*.

74. Kirchknopf, A.; Slijepčević, D.; Zeppelzauer, M. Multimodal Detection of Information Disorder from Social Media. In Proceedings of the 2021 International Conference on Content-Based Multimedia Indexing (CBMI), Lille, France, 28–30 June 2021; pp. 1–4.
75. Xie, J.; Liu, S.; Liu, R.; Zhang, Y.; Zhu, Y. SeRN: Stance extraction and reasoning network for fake news detection. In Proceedings of the ICASSP 2021—2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Toronto, ON, Canada, 6–11 June 2021; pp. 2520–2524.
76. Raza, S.; Ding, C. Fake news detection based on news content and social contexts: A transformer-based approach. *Int. J. Data Sci. Anal.* 2022, 13, 335–362. [CrossRef]

Barmak Oleksandr, Borovyk Oleh, Borovyk Dmytro, Skrypnyk Tetyana

POSSIBLE OPTIONS FOR IMPROVING EXISTING APPROACHES TO FAKE NEWS DETECTION BASED ON USING THE POTENTIAL OF MACHINE AND DEEP LEARNING ALGORITHMS, SENTIMENT OF NEWS CONTENT AND EMOTIONS IN USER COMMENTS

Currently, the Internet ranks first among sources of information. In the recent period, the role of online social networks (OSN) has significantly increased, which has both positive and negative consequences. The negative role of OSN is related to the spread of fake news that affects people's daily lives, manipulates their thoughts and feelings, changes their beliefs and can lead to wrong decisions. The problem of spreading fake news in OSN is currently global, and the formation of countermeasures is an urgent task today.

Today, there are various proven approaches to detecting fake news. In particular, one of the approaches is based on the use of different machine (ML) and deep (DL) learning algorithms. The other is based on the results of sentiment analysis of news content and analysis of emotions in user comments. The research conducted by the authors of other approaches to detecting fake news, which differ from the ones given, made it possible to conclude that the mentioned approaches are effective and promising in terms of using their potential for the development of new models with high performance indicators on various data sets.

In the article, the author's ideas regarding the improvement of existing approaches to detecting fake news based on the use of the potential of these approaches are formed and formalized. The first idea is based on the implementation of the mechanism of combining machine (ML) and deep (DL) learning methods, as well as the results of the analysis of the sentiment of news content and emotions in user comments, which takes into account the possibility of ensuring a sufficient level of effectiveness in detecting fake news, a certain level of the values of the selected metrics, as well as a certain level of functional characteristics of the author's method. The second idea is based on the implementation of a mechanism combining the functionality of two methods from among the specified two groups, which would provide optimal parameters for detecting fake news according to defined criteria and indicators.

The substantiation of the ideas involved the preliminary implementation of: setting the researched problem; functional analysis of machine (ML) and deep (DL) learning algorithms, as well as fake news detection algorithms based on the use of the results of sentiment analysis of news content and emotions in user comments; description of metrics for evaluating the effectiveness of methods for detecting fake news. According to the results of the substantiation of the perspective of the ideas, the tasks of detecting fake news in the author's production were formalized.

Keywords: online social networks; fake news; method; model; algorithm; formalization.

ВИМОГИ З КІБЕРЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ ТА СЕРВІСІВ ЗВ'ЯЗКУ ПІД ЧАС ЇХ РОЗГОРТАННЯ ТА ЕКСПЛУАТАЦІЇ НА ПУНКТАХ УПРАВЛІННЯ СКЛАДОВИХ СИЛ ОБОРОНИ ТА БЕЗПЕКИ

Актуальність даної роботи обумовлена тим, що за останні роки війська зв'язку постійно розвивались та оснащувались новітніми цифровими засобами зв'язку, що дозволяє їм успішно виконувати завдання за призначенням. Сьогодні інформаційно-комунікаційні системи які розгорнуті на пунктах управління різних ланок управління забезпечують виконання пріоритетних завдань з управління військами. Функціонально, система зв'язку та інформаційні системи розгорнуті на пунктах управління, як єдине інформаційно-комунікаційне середовище на основі впровадження новітніх інформаційно-комунікаційних технологій, протоколів обміну інформацією, комплексів, систем та засобів зв'язку, що забезпечує обмін усіма видами інформації між органами військового управління (органами управління) та пунктами управління на всіх ланках управління. Діюча система зв'язку забезпечує обмін інформацією із гарантованою захищеністю в єдиному інформаційному просторі як сукупність матеріальних функцій (в тому числі персоналу та інших ресурсів), що об'єднуються для виконання певного завдання.

В свою чергу інформаційні системи, як сукупність обладнання, методів та процедур, і, в разі необхідності, персоналу, організованого для виконання функцій обробки інформації діють у відповідності до визначеної структури, а саме:

- сервіси, в контексті зв'язку та інформаційні системи;
- архітектура, в контексті зв'язку та інформаційні системи;
- функції, в контексті сервіс-орієнтованої архітектури;
- взаємосумісність;
- захист інформації та кіберзахист.

Зрозуміло, що чим важливіший об'єкт управління, тим більш ємкісний потік інформації може бути спрямований на нього. Зазначене дозволяє противнику/зловмиснику визначити найбільш важливі цілі і спрямувати на них інші види інформації або придушити їх різними способами. Так, в інтересах забезпечення кіберзахисту електронних інформаційних ресурсів, комунікаційних і технологічних систем пунктів управління Збройних Сил України розгорнута і функціонує технологічна інфраструктура кіберзахисту Збройних Сил України, яка є складовою єдиної системи захисту інформації та кіберзахисту в інформаційно-комунікаційних системах Міністерства оборони і Збройних Сил України. В цих умовах, для вирішення завдань з унеможливлення небажаних втручань, порушення сталого функціонування інформаційно-комунікаційного середовища на пунктах управління, проти ваги в здобутті конфіденційної інформації, викрадення даних та інше розгортаються мінімально необхідні компоненти інфраструктури кіберзахисту. Основними компонентами відповідної технологічної інфраструктури кіберзахисту є система управління подіями інформаційної безпеки (Security Information Event Management, SIEM), платформа обміну інформацією про загрози (Malware Information Sharing Platform & Threat Sharing, MISP), система централізованого управління міжмережевими екранами та система виявлення і протидії кіберзагрозам, у тому числі комп'ютерним вірусам, на кінцевому обладнанні.

Тому, вирішення завдань з забезпечення кіберзахисту в ході розгортання та експлуатації електронних комунікаційних мереж та сервісів зв'язку на пунктах управління різних ланок управління виявляється доволі серйозним та актуальним завданням.

Ключові слова: пункт управління, інформаційно-комунікаційне середовище, кіберпростір, кіберзагроза, кібербезпека, кібероборона.

Вступ. Питання кібербезпеки (КБ) в Збройних Силах України (ЗС України), а особливо в зоні проведення військових дій, сьогодні майже не висвітлюється. При цьому відомо, що деструктивному впливу піддається не тільки електронно-комунікаційна система, а і особовий

склад який залучений до виконання бойових завдань [1]. Новітні засоби розвідки дають змогу дізнатися не лише про місце, з якого ведуться переговори, а й безпосередньо про зміст переговорів та листування. І головною проблемою в цьому питанні, на жаль, є не розробка та доопрацювання десятків інструкцій та керівництв, а недостатня обізнаність особового складу, щодо налаштування політик безпеки особистих мобільних пристроїв та озброєння-військової техніки зв'язку.

Сьогодні більшість тих, хто залучений до складу Сил оборони та безпеки (СО), включаючи рядовий і офіцерський склад, не усвідомлюють про наявність кіберзагроз та потенційно можливі негативні наслідки, які можуть створити небезпеку життєво важливим інтересам громадянам, особам, суспільству і державі. В цих умовах, важливо забезпечити цілісність і конфіденційність інформації під час виконання бойових завдань, перебуваючи **в районах зосередження, бойового злагодження, пунктах управління (ПУ), пунктах постійної дислокації. Визнавати відповідальність за проведення переговорів службового характеру з використанням персональних мобільних пристроїв та електронних комунікаційних мереж.** Нажаль військовослужбовці не в змозі самотійно забезпечити безпечне налагодження та експлуатацію тих чи інших додатків/застосунків, програмного забезпечення (ПЗ), набору інструментів, технологій і даних від несанкціонованого доступу.

Інформація – це найважливіший актив, а стабільне функціонування системи зв'язку і комунікаційних систем (СЗКС) та послуг має важливе значення для належного управління системою консультацій, командування і управління (СЗ). Складові СО і союзники покладаються на використання СЗКС для ефективного обміну інформацією та ефективного функціонування. Така побудова СЗКС (CIS) потребує ряду принципів, які дозволять отримувати переваги технологій, а також розібратися з пов'язаними ризиками і складнощами виконання операцій з інформаційним перевантаженням [2].

Врахування принципів зв'язку та інформаційних систем (en: Communication and Information Systems Principles) дозволить СО спільно використовувати інформацію в рамках єдиного інформаційного простору. Зазначене надає право командирам та штабам всіх рівнів отримати значні переваги під час планування та ведення операцій (бойових дій), покращити ситуаційну обізнаність, управління військами (силами) та зброєю. Такий підхід дозволить СО отримувати переваги з використання та впровадження інформаційних технологій (ІТ).

За цих умов постає доволі суттєва проблема, щодо забезпечення доступності, цілісності, конфіденційності та КБ до інформації яка циркулює в інформаційно-комунікаційних систем (ІКС) ПУ органів військового управління (ОВУ). Особливо це стосується систем і мереж, які використовуються суб'єктами СО для управління особливо важливою інформацією. Виконання вимог з: надійності і безпеки відповідних сервісів зв'язку, виявлення та протидії зловмисній діяльності, доступності, цілісності та безпеки інформації які включають елементи фізичної безпеки (наприклад, безпеку персоналу та документів) і ЗІ є ключовими елементами безпеки в СЗКС [3]. Також, доволі суттєвим питанням є виконання заходів з забезпечення безпеки зв'язку і комп'ютерної безпеки, управління службами СЗКС у відповідь на зловмисні дії, вчинені в кіберпросторі. У той же час, інформація повинна бути захищена до належного рівня, гарантуючи доступність до достовірної інформації авторизованим користувачам і унеможливив доступ до достовірної інформації неавторизованих осіб.

Отже, розробка базових вимог з кіберзахисту ІКС та сервісів зв'язку під час їх розгортання та експлуатації на ПУ складових СО є вкрай важливим. Їх запровадження та виконання оперативним складом ПУ різних ланок управління забезпечить сталу експлуатацію захищених інформаційно-телекомунікаційних послуг (сервісів) на ПУ, ефективну технічну підтримку базових і функціональних служб, а також ІТ для обробки даних та їх відображення в системі управління військами, функціональну взаємодію та сумісництво СЗКС на ПУ складових СО.

Аналіз останніх досліджень. Аналіз існуючої нормативно-правової бази щодо створення та функціонування системи КБ та кібероборони в ІКС спеціальних користувачів

свідчить про те, що Національна система КБ, одним із трьох завдань якої є кіберзахист державного інформаційного ресурсу, створюється і розвивається відповідно до Конституції України, законів України та інших нормативно-правових актів, що регулюють суспільні відносини у сфері національної безпеки, оборони, інформаційної та КБ і захисту інформації. Виходячи з цього, системи кіберзахисту в ІКС спеціальних користувачів також створюються та функціонують відповідно до вимог законів та нормативно-правових актів України, а саме:

Законів України: “Про національну безпеку України” [4]; “Про основні засади забезпечення кібербезпеки України” [5]; “Про захист інформації в інформаційно-телекомунікаційних системах” [6]; “Про розвідку” [7]; “Про Національну програму інформатизації” [8]; “Про ратифікацію Конвенції про кіберзлочинність” [9]; “Про Державну службу спеціального зв’язку та захисту інформації України” [10]; “Про державну таємницю” [11]; “Про доступ до публічної інформації” [12]; “Про захист персональних даних” [13]; “Про оборону України” [14]; “Про інформацію” [15]; “Про Збройні Сили України” [16].

Документів довгострокового та оборонного планування України: Стратегія національної безпеки України [17]; Стратегія кібербезпеки України [18]; Стратегія воєнної безпеки України [19]; Стратегічний оборонний бюлетень України [20]; Питання Апарату Ради національної безпеки і оборони України, Про Національний координаційний центр кібербезпеки [21]; Стратегія інформаційної безпеки України [22].

Нормативних документів міжнародних організацій, згода на використання яких надана Верховною Радою України. Зокрема, рекомендації Міжнародного союзу електрозв’язку (ITU), міжнародні стандарти з інформаційної безпеки ISO/IEC 27000, стандарти (рекомендації) Національного інституту стандартів і технологій США – NIST та стандартів та специфікацій національного інституту стандартів (ANSI).

Нормативно-правових актів Міністерства оборони України (Далі – МО України) та ЗС України, більшість з яких має обмеження доступу, видаються відповідно до вимог законів України, підзаконних актів державних органів, уповноважених у сферах електронних комунікацій, інформатизації, захисту інформації тощо, частина з яких також не є відкритою інформацією відповідно до вимог законів України [5, 6, 10].

Мета статті. Вирішення завдань забезпечення кіберзахисту електронних комунікаційних мереж та сталого функціонування сервісів зв’язку на пунктах управління різних ланок управління є вкрай актуальним, а формулювання та реалізація відповідних технічних вимог є ключовим елементом для складових сил оборони та безпеки в умовах сьогодення.

Виклад основного матеріалу. Формування та розвиток нової моделі системи зв’язку та інформаційних систем СО України здійснюється у відповідності з кращими практиками ключових іноземних партнерів, передусім Європейського Союзу, Сполучених Штатів Америки та інших держав-членів НАТО, на основі національних інтересів України.

Стратегічні принципи зв’язку та інформаційних систем (en: CIS strategic principles) СО (визначені відповідно до документу Ради штабу НАТО з консультацій, командування та управління AC/322-D (2018) 0020. Alliance C3 Strategy – Part 1, 27 April 2018.) включають [23]:

- спільне використання інформації в рамках єдиного інформаційного простору із запровадженням та супроводженням реєстру інформаційних ресурсів, електронних баз даних інформації та інформаційного менеджменту;

- забезпечення безперешкодного обміну інформацією між стаціонарними СЗКС та польовими мережами зв’язку;

- функціонування інформації в мережевому захищеному середовищі балансує між принципами “обов’язок щодо розповсюдження” (en: “duty to share”) та “потреби в інформації” (en: “need to know”);

- масштабованість СЗКС та їх сервісів (здатність динамічно адаптуватись до змін вимог), гнучкість (здатність адаптуватись до змін умов обстановки яка склалась), захищеність (здатність забезпечити політики безпеки в існуючому середовищі ризиків) та стійкість (здатність до відновлення системи після вразливості “нульового дня”);

- забезпеченість СЗКС відповідними сервісами згідно методології DOTMLPFI;

Примітка. 6 DOTMLPFI (Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities, and Interoperability) – напрямки розвитку оборонних потенціалів (Доктринальна база (D), Організація (O), Підготовка (T), Ресурсне забезпечення (M), Персонал (P), Якість управління та освіта (L), Військова інфраструктура (F), Взаємосумісність (I)), які є складовою процесу оборонного планування НАТО (en: NATO Defense Planning Process) [2].

– опис та забезпеченість спроможностей СЗКС, як сервісів, сервіс-орієнтовану архітектуру та запровадження підходів до їх життєвого циклу;

– підтримку обміну інформацією з обмеженням доступу будь-якого рівня та всіх функціональних сервісів, притаманних окремим структурним підрозділам ОВУ;

– відкритість, модульність та гнучкість для повторного використання, динамічність до розвитку і взаємосумісності та здатність до інтеграції в існуючі та майбутні спроможності архітектур СЗКС;

– відповідність пріоритету розвитку спроможностей парадигмі “ABC” (Adopt, Buy, Create) (тобто, модернізація наявного, далі – закупівля готових ресурсів, і, як крайня міра – створення нового або їх комбінація);

– заснування дисципліни з корпоративної архітектури;

– адекватну захищеність проти всіх категорій загроз, у т.ч. тих, що впливають із кіберпростору, зв’язку та інформаційних систем, їх сервісів та електронних систем;

– підтримку колективних заходів з кіберзахисту (кібероборони) всіх складових СО; запровадження практик ITIL (Бібліотека інфраструктури ІТ (en: Information Technology Infrastructure Library, ITIL)).

Об’єднана ІКС СО повинна використовувати гнучкі та адаптовані набори нематеріальних (політика безпеки, визначені процеси і процедури, стандартизація інформаційного циклу) та матеріальних (стаціонарна та польова мережі, сервіси та підтримуючі інфраструктури зі зв’язку) засобів, якими забезпечуються складові СО. Розгортання об’єднаної ІКС СО зі створенням єдиного інформаційного простору повинно відповідати таким принципам:

- цінова ефективність від використання;
- можливості максимального повторного використання;
- відповідність принципам єдиного інформаційного простору;
- урахування СЗ-таксономії;
- поетапний підхід;
- використання уніфікованих мережевих стандартів та рішень;
- підтримка угруповань СО, склад яких динамічно змінюється;
- інформаційна орієнтованість мережі.

Об’єднання систем зв’язку та інформаційних систем в ІКС складових СО повинно здійснюватись за допомогою визначених рівнів взаємосумісності, а саме ізольована, поєднана, функціональна, доменів та корпоративна. При цьому взаємосумісності систем зв’язку та інформаційних систем не є абсолютною умовою. Оговорюючи об’єднану ІКС СО, вважається за необхідне розглянути інциденти КБ, існуючі загрози та їх модифікації порушення захисту інформації які носять вірогідний та імовірний характер впливу на стале функціонування ПУ різних ланок управління СО та безпеки. Їх можливо класифікувати за категоріями та ступенем небезпеки. При цьому, кіберінциденти, що потребують реагування у разі їх виявлення, поділяються на категорії. Категорія кіберінциденту визначає причину, через яку приймається рішення про необхідність реагування на інцидент КБ [24].

Для кожної категорії кіберінцидентів визначений цифровий код, назва українською та англійською мовами, а також пріоритет. Категорії інцидентів КБ на ПУ різних ланок управління СО та безпеки подано в таблиці 1.

Таблиця 1

Категорії інцидентів КБ на ПУ різних ланок управління СО та безпеки

од	Пріоритет	Назва категорії інциденту КБ в ІКС
	9	Зловмисна інформація (Abusive content)
	4	Шкідливий програмний засіб (Malicious Code)
	8	Збір інформації зловмисником (Information Gathering)
	5	Спроба зловмисника щодо вторгнення до системи (Intrusion Attempts)
	1	Вторгнення зловмисника до системи (Intrusion)
	3	Загроза доступності інформації (Availability)
	2	Загроза конфіденційності та/або цілісності інформації (Information Content Security)
	6	Махінації (Fraud)
	7	Наявність відомих вразливостей (Vulnerability)
0	10	Інше (Other)

Інцидент, який може бути віднесений до декількох категорій, реєструється (обліковується) як інцидент категорії, яка має вищий пріоритет. Опис інцидентів КБ в ІКМ ПУ різних ланок управління СО та безпеки наведено в таблиці 2.

Таблиця 2

Опис інцидентів КБ в ІКМ ПУ різних ланок управління СО та безпеки

	Опис інциденту КБ	Назва категорії кіберінциденту (код)
	2	3
	Компрометація облікового запису системи (сервісу), в тому числі в результаті крадіжки паролів зловмисником	Вторгнення зловмисника до системи (5)
	Компрометація системи, в тому числі в результаті експлуатації вразливості або роботи шкідливого програмного забезпечення, що дозволяє віддалене керування	Вторгнення зловмисника до системи (5)
	Несанкціоноване підключення пристрою до ІКС, в тому числі цифрової радіостанції до системи цифрового радіозв'язку	Вторгнення зловмисника до системи (5)
	Порушення порядку доступу до інформації в системі (в тому числі в результаті експлуатації вразливості або роботи шкідливого програмного забезпечення)	Загроза конфіденційності та/або цілісності інформації (7)

	Опис інциденту КБ	Назва категорії кіберінциденту (код)
	Відмова в обслуговуванні або порушення сталого функціонування сервісу (об'єкта ІКС) в результаті DoS-, DDoS-атаки, помилкових, дій користувачів, відключення електричної енергії, тощо	Загроза доступності інформації(6)
	Виявлення шкідливого програмного засобу, що не дозволяє віддалене керування та не несе загрози цілісності і конфіденційності та/або доступності інформації	Шкідливий програмний засіб (2)
	Виявлення спроб використання зловмисником вразливостей ПЗ, невдалих спроб автентифікації в системі, в тому числі в системі цифрового радіозв'язку	Спроби зловмисника щодо вторгнення до системи (4)
	Розсилання зловмисником повідомлень з метою крадіжки пароля користувача	Махінації (8)
	Несанкціонований доступ до ресурсів системи шляхом використання прав об'єкта (несанкціоноване використання NAT, підміна MAC-адреси)	Махінації (8)
0	Передача захищеного паролем архіву під час обміну відкритою інформацією в автоматизованій системі управління ЗС України "Дніпро"	Махінації (8)
1	Несанкціоноване використання ПЗ, що втручається в роботу комплексу засобів захисту	Махінації (8)
2	Порушення порядку використання ресурсів (використання не за призначенням, у несанкціонованих цілях), в тому числі обробка інформації в автоматизованій системі без створення комплексної системи захисту інформації з підтвердженою відповідністю, обробка інформації з обмеженим доступом в автоматизованій системі, що призначена для обробки відкритої інформації, передача інформації з обмеженим доступом в мережі Інтернет, в автоматизованій системі управління ЗС України "Дніпро", по відкритих телефонних мережах	Махінації (8)
3	Відсутність критичного оновлення безпеки ПЗ (прошивки телекомунікаційного обладнання)	Наявність, відомих вразливостей (9)
4	Функціонування автоматизованого робочого місця або сервера з порушенням вимог інструкції з організації антивірусного захисту в СЗКС МО України та ЗС України	Наявність відомих вразливостей (9)
5	Порушення порядку підключення автоматизованої системи до мережі Інтернет	Наявність відомих вразливостей (9)
6	Порушення встановлених правил розмежування доступу, в тому числі використання пароля (SNMP community, ключа шифрування системи цифрового радіозв'язку) понад встановлений термін або такого, що не відповідає визначеним вимогам безпеки	Наявність відомих вразливостей (9)
7	Використання свідомо уразливого протоколу, режиму роботи, налаштувань обладнання або ПЗ при	Наявність відомих вразливостей (9)

	Опис інциденту КБ	Назва категорії кіберінциденту (код)
	передачі паролів, іншої чутливої інформації	
8	Несанкціоноване використання ПЗ, що збільшує ризик порушення безпеки інформації, в тому числі отриманого з недостовірних джерел	Наявність відомих вразливостей (9)
9	Помилкові дії або бездіяльність користувача, що призводять до збільшення ризику порушення безпеки інформації цифрових систем радіозв'язку, а саме: робота передавача на випромінювання в період радіомовчання, робота радіозасобів без радіоданих під час переміщення ПУ (вузлів зв'язку), спотворення форми сигналу на виході передавача	Наявність відомих вразливостей (9)
0	Збирання інформації зловмисником про користувача, склад ІКС, існуючі вразливості, в тому числі нетехнічними засобами	Збір інформації зловмисником (3)
1	Масове розсилання небажаної кореспонденції (SPAM)	Зловмисна інформація (1)
2	Виявлення у відкритому доступі інформації, що здатна зашкодити інтересам МО України та ЗС України	Зловмисна інформація (1)
3	Виявлення шкідливого програмного засобу, що відбулося одночасно з його блокуванням/видаленням наявним антивірусним ПЗ за умови знаходження джерела розповсюдження шкідливого програмного засобу за межами ІКС ЗС України	Інше (10)

Розглядаючи нормативно-правову базу на загальнодержавному рівні, необхідно зазначити, що правову основу забезпечення КБ України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації.

Відповідно до Закону України “Про основні засади забезпечення кібербезпеки України” (Документ 2163-VIII) від 17.08.2022, Указу Президента України “Питання Головнокомандувача Збройних Сил України” від 27 березня 2020 року № 123/2020, вимог рішення Ради національної безпеки і оборони України від 14 травня 2021 р. “Про невідкладні заходи з кібероборони держави”, введеного в дію Указом Президента України від 26 серпня 2021 р. № 446 та у відповідності до вимог схваленого на засіданні Кабінету Міністрів України Плану організації виконання рішення Ради національної безпеки і оборони України від 14 травня 2021 р. “Про невідкладні заходи з кібероборони держави”, введеного в дію Указом Президента України від 26 серпня 2021 р. № 446 передбачено підтримання та нарощування спроможностей до застосування ЗС України, а також сил і засобів інших складових СО.

Як однією з похідних, розвитку та впровадження, зазначеної вище нормативно-правової бази, відбулась розробка та затвердження Міністром оборони України “Функціональних груп спроможностей Міністерства оборони України, Збройних Сил України та інших складових Сил оборони” від 26 листопада 2021 року. Паралельно з цим, робочою групою був розроблений “Єдиний перелік (каталог) спроможностей Міністерства оборони України, Збройних Сил України та інших складових Сил оборони”, який було затверджено Міністром оборони України 31 грудня 2021 року. Так, Розділом 7. ЗВ’ЯЗОК ТА ІНФОРМАЦІЙНІ СИСТЕМИ (COMMUNICATION&INFORMATION SYSTEMS – CIS), на Командування військ зв’язку та кібернетичної безпеки ЗС України (2CIS-5.1) покладається

“Створення і забезпечення захищених інформаційно-телекомунікаційних послуг (сервісів) для ОВУ та розгортання ПУ на рухомій базі” – код спроможності 2CIS-5. Зазначений розділ переліку охоплює спроможності СО з організації (забезпечення) зв’язку та обміну інформацією в інформаційних системах.

Переліком визначено ряд базових вимог до носіїв спроможності, одним з яких є здатність створення і забезпечення захищених інформаційно-телекомунікаційних послуг (сервісів) для ОВУ та розгортання ПУ на рухомій базі у відповідності до матриці надання мінімально необхідних сервісів оперативному складу (службовим особам) ПУ оперативної (оперативно-тактичної, тактичної) ланок управління [25]. Встановлено, що організація розгортання, здійснення управління, забезпечення функціонування єдиної системи захисту інформації та кіберзахисту в ІКС МО України і ЗС України покладається на Генеральний штаб ЗС України. При цьому розгортання та забезпечення функціонування технологічної інфраструктури кіберзахисту ЗС України здійснюється силами військових частин та підрозділів захисту інформації та КБ Командування Військ зв’язку та КБ ЗС України [26]. Порядок організації доступу телекомунікаційних вузлів ПУ до мережі Інтернет та електронної комунікаційної мережі ЗС України визначається старшим ОВУ у відповідному бойовому розпорядженні (розпорядженні зі зв’язку). Транзит трафіку ЕКМ ЗС України між ІТВ ЗС України здійснюється виключно в зашифрованому вигляді згідно з вимогами законодавства у сфері технічного та криптографічного захисту інформації.

Для надання оперативному складу ПУ базових, функціональних сервісів, доступу до мережі Інтернет спеціалісти зв’язку телекомунікаційних вузлів розгортають локальні мережі різного призначення, вживають відповідних технічних та організаційних заходів для забезпечення їх цілісності, безперервності надання електронних комунікаційних послуг, недопущення несанкціонованого доступу до розгорнутих мереж. Різні за призначенням (умовами доступу до інформації, що обробляється) мережі відокремлюються одна від одної на фізичному (шляхом використання окремого обладнання для різних мереж) або на логічному (шляхом використання технології VLAN тощо) рівні. Налаштування локальних мереж для підключення кінцевого (термінального) обладнання, яке використовується без створення комплексної системи захисту інформації (особисті засоби електронних комунікацій оперативного складу ПУ тощо), повинно забезпечувати ізоляцію обладнання таких мереж одне від одного та від локальних мереж іншого призначення. Ізоляція може бути реалізована шляхом відокремлення портів комутаційного обладнання мережі (технологія Private VLAN), налаштуванням спеціального режиму роботи точок безпроводового доступу (Guest Network) тощо.

Під час розгортання локальних мереж має використовуватися обладнання, ПЗ (прошивка) яке ліцензійно підтримується виробником. Вкрай важливо передбачити своєчасне оновлення ПЗ (прошивки) обладнання в разі виявлення його критичної вразливості яке покладається на адміністратора мережі. Розгортання, модернізація, припинення експлуатації, згортання відповідних інформаційно-комунікаційних систем (мереж) ПУ вноситься адміністратором в SIEM. Обладнання ЕКМ розгортається таким чином, щоб фізичний доступ до нього був обмежений лише персоналом польових ТВ, в обов’язки якого входить експлуатація (обслуговування) зазначеного обладнання. Доступ адміністраторам до адміністрування обладнання ЕКМ повинен надаватися виключно з IP-адрес робочих станцій, які визначені для адміністрування ЕКМ. Рекомендовано розміщення робочих станцій адміністраторів в окремій локальній мережі (Management VLAN). Доступ до управління технічними засобами електронних комунікацій має надаватися користувачам та адміністраторам в межах визначених їм прав доступу тільки після успішного проходження процедури автентифікації. Використання для адміністрування технічних засобів електронних комунікацій незахищених протоколів передачі даних (HTTP, Telnet тощо) забороняється. При цьому паролі облікових записів користувачів та адміністраторів технічних засобів електронних комунікацій мають відповідати вимогам парольної політики у ЗС України.

Налаштування обладнання ЕКМ має забезпечувати реєстрацію та передачу в SIEM даних щонайменше про такі події: вхід користувачів та адміністраторів; невдалі спроби

входу користувачів та адміністраторів; зміна конфігураційних налаштувань. Налаштування обладнання, що служить для з'єднання локальної мережі з іншими мережами (маршрутизатор або міжмережевий екран), повинно забезпечувати політику пропуску трафіку та передачу даних про нього в SIEM з метою аналізу на предмет виявлення ознак кібератак.

Політика пропуску трафіку (правила фільтрації) визначає обмеження на пропуск трафіку між взаємоз'єднаними мережами на основі критеріїв дозволених та заборонених служб, протоколів, портів, станів взаємодії (statefulness), мережевих адрес, вебсайтів тощо. До проведення налаштування передачі даних про трафік у SIEM повинно забезпечуватись локальне зберігання зазначених даних не менше 30 діб та передача їх в електронному вигляді за запитом командира (заступника) військової (их) частин та підрозділів захисту інформації та КБ Командування Військ зв'язку та кібербезпеки ЗС України для аналізу.

Налаштування шлюзу між локальними мережами і мережею Інтернет має, крім того, забезпечувати автоматичне застосування встановлених правил обробки мережевого трафіку, у тому числі блокування кібератак у разі виявлення ознак відомих кіберзагроз.

Зазначені вимоги реалізуються міжмережевими екранами (ММЕ). У разі відсутності ММЕ, необхідно здійснити відповідні налаштування маршрутизаторів мережі. Оновлення даних про кіберзагрози в системі централізованого управління міжмережевими екранами забезпечується силами військових частин та підрозділів захисту інформації та КБ Командування Військ зв'язку та кібербезпеки ЗС України шляхом управління ліцензіями (підписками на джерела даних про кіберзагрози виробника ММЕ) та інтеграції з MISIP. У разі якщо умови роботи ЕКМ не дозволяють проходження трафіку через міжмережеві екрани, то для виявлення кіберзагроз налаштовується передача на міжмережеві екрани копії трафіку (технологія Traffic Mirroring).

Для забезпечення належного функціонування ЕКМ необхідно створювати систему резервування копій конфігурацій обладнання ЕКМ та інформаційних ресурсів/даних об'єктів критичної інфраструктури СЗКС СО. Передбачити оперативний доступ до ресурсів/даних зазначених систем, як на мобільних так і на стаціонарних резервних платформах, пунктах, центрах. Резервні копії повинні зберігатися у зашифрованому вигляді на окремих змінних (зовнішніх) носіях, віртуальних серверах або в зашифрованому вигляді на хмарних ресурсах та/або в центрах обробки даних, розташованих за межами України [27].

В рамках підготовки оперативного складу щодо коректного налаштування та підтримки політик ІБ та КБ, необхідно передбачити залучення їх до відповідних навчальних курсів з базових заходів КБ, що підтверджуються відповідними сертифікатами.

Оперативний склад ПУ експлуатує базові і функціональні сервіси, при цьому доступ до мережі Інтернет має виключно через кінцеве (термінальне) обладнання, підключене до локальних мереж ІТВ (польових ВЗ). Використання інших мереж електронних комунікацій, у тому числі операторів мобільного зв'язку, на ПУ забороняється.

У комунікаційних мережах ПУ необхідно забезпечити контроль доступу до сервісів обміну електронними поштовими повідомленнями. При цьому доступ до захищених сервісів домену mil.gov.ua надається оперативному складу ПУ без обмежень, а доступ до сервісів обміну електронними поштовими повідомленнями в інших доменах надається для окремих пристроїв у разі необхідності, про що вказується в заявці на підключення кінцевого обладнання структурного підрозділу з відповідним обґрунтуванням.

Доступ оперативному складу ПУ до локальних мереж має надаватись з використанням індивідуальних даних автентифікації (логін, пароль, сертифікат тощо) за протоколом контролю доступу і автентифікації IEEE 802.1x. У разі неможливості використання протоколу IEEE 802.1x пристроям оперативного складу ПУ при їх підключенні до локальних мереж мають видаватися незмінні (постійні) IP-адреси. У такому разі IP-адреса пристрою закріплюється за його MAC-адресою та видається за протоколом DHCP. Безпроводовий доступ до локальних мереж пристроям, MAC-адрес яких немає в переліку дозволених, має бути заблокований налаштуванням точок безпроводового доступу, комутаційного

обладнання тощо. Ведення обліку IP-адрес, виданих пристроям оперативного складу ПУ, покладається на ІТВ [28].

Пристрої електронних комунікацій (комп'ютери, мобільні комунікаційні пристрої тощо, у тому числі особисті), що підключаються до ЕКМ, мають відповідати таким вимогам:

- встановлена операційна система та ПЗ, які дозволено використовувати у ЗС України, повинно технічно підтримуватись виробником та мати відповідні ліцензії;

- оновлення ПЗ у разі виявлення його критичної вразливості (при цьому пристрої необхідно підключити до системи виявлення і протидії кіберзагрозам, у тому числі комп'ютерним вірусам);

- налаштування політик безпеки, виконання зазначеного заходу унеможливорює доступ до змінних (зовнішніх) пристроїв та носіїв інформації, ідентифікаторів яких немає в списку дозволених;

- користувачі та адміністратори повинні отримати доступ до пристроїв в межах визначених їм прав доступу тільки після успішного проходження процедури автентифікації.

Вимоги до автоматизованих робочих місць або інших пристроїв, що підключаються до ІКС, визначаються комплексною системою захисту інформації (методикою розгортання) таких ІКС.

Оперативним складом ПУ мають створюватися (оновлюватися) резервні копії власних інформаційних ресурсів з періодичністю, достатньою для їх відновлення у разі пошкодження або знищення внаслідок кіберінцидентів та кібератак. Резервні копії повинні зберігатися на окремих змінних (зовнішніх) носіях, які не використовуються для перенесення інформації між автоматизованими робочими місцями та виконання інших завдань.

Отже, проведене дослідження дозволило сформулювати вимоги з кіберзахисту інформаційно-комунікаційних систем та сервісів зв'язку під час їх розгортання та експлуатації на ПУ складовими СО.

В науковій праці побудовано алгоритм базових дій з налаштування політики безпеки як на програмному так і на технічному рівні основного обладнання зв'язку яке розгортається на ПУ для оперативної роботи особового складу.

Наведені пропозиції забезпечать заходи безпеки на ПУ різних ланок управління з захисту інформаційно-телекомунікаційних та інших електронно-комунікаційних систем та інформації, яка зберігається, обробляється чи передається в цих системах із додержанням доступності, цілісності, автентифікації, конфіденційності та ідентифікації відправника/отримувача.

Висновки. Виходячи з викладеного, можливо зробити наступні висновки:

1. СО спільно використовують інформацію в рамках єдиного інформаційного простору із запровадженням та супроводженням реєстру інформаційних ресурсів, електронних баз даних інформації та інформаційного менеджменту.

2. Архітектура та масштабованість ІКС і їх сервісів на ПУ різних ланок управління розгортається та експлуатується відповідно до документу Ради штабу НАТО з консультацій, командування та управління AC/322-D (2018) 0020. Alliance C3 Strategy – Part 1, 27 April 2018.

3. Існує ряд кіберзагроз та їх модифікації спрямовані на порушення захисту інформації, що носять вірогідний та імовірний характер впливу на стале функціонування ПУ різних ланок управління СО.

4. В рамках наведених пропозицій є вкрай важливим реалізувати на ПУ СО вимоги, щодо кіберзахисту ІКС та сервісів зв'язку під час їх розгортання та експлуатації.

ЛІТЕРАТУРА:

1. Черниш Р.Ф., Ігнатюк М.В. Протидія деструктивному інформаційному впливу в Україні: правові та організаційні аспекти [Електронний ресурс] – Режим доступу: http://lsej.org.ua/1_2022/54.pdf.
2. Доктрина зв'язок та інформаційні системи, введена в дію Головнокомандувачем Збройних Сил України від 20 червня 2020 року, ВКП 6-00(01).01.
3. Живилю Є.О., Черноног О.О. Стратегія кібероборони України // Збірник наукових праць ВІТІ № 4 – 2017 [Електронний ресурс] – Режим доступу: http://www.viti.edu.ua/files/zbk/2017/4/4_4_2017.pdf.
4. Закон України “Про національну безпеку України” від 21.06.2018 р. № 2469-VIII // Законодавство України [Електронний ресурс] – Режим доступу: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>.
5. Закон України “Про основні засади забезпечення кібербезпеки України” від 05.10.2017 р. № 2163-VIII // Законодавство України [Електронний ресурс] – Режим доступу: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.
6. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” [Електронний ресурс] – Режим доступу: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>.
7. Закон України “Про розвідку” від 17.09.2020 № 912-IX [Електронний ресурс] – Режим доступу: <https://zakon.rada.gov.ua/laws/show/912-20#Text>.
8. Закон України “Про Національну програму інформатизації” від 04.02.1998 р. № 74/98-ВР // Законодавство України [Електронний ресурс] – Режим доступу: <https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80#Text>.
9. Закон України “Про ратифікацію Конвенції про кіберзлочинність” від 10.03.2006 р. № 2163-VIII // Законодавство України [Електронний ресурс] – Режим доступу: <https://zakon.rada.gov.ua/laws/show/2824-15#Text>.
10. Про Державну службу спеціального зв'язку та захисту інформації : Закон України від 23.02.2006 р. [Електронний ресурс] – Режим доступу: <https://zakon.rada.gov.ua/laws/show/3475-15#Text>.
11. Закон України “Про державну таємницю” від 21 січня 1994 № 3855-XII (зі змінами) [Електронний ресурс] – Режим доступу: <https://zakon.rada.gov.ua/laws/show/3855-12#Text>.
12. Закон України “Про доступ до публічної інформації” від 13 січня 2011 р. № 2939-VI. [Електронний ресурс] – Режим доступу : <https://zakon.rada.gov.ua/laws/show/2939-17#Text>.
13. Закон України “Про захист персональних даних” від 01.06.2010 р. № 2297-VI [Електронний ресурс] – Режим доступу: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>.
14. Закон України “Про оборону України” від 06.12.1991 р. № 1932-XII // Законодавство України [Електронний ресурс] – Режим доступу: <https://zakon.rada.gov.ua/laws/show/1932-12#Text>.
15. Закон України України “Про інформацію” № 2938-VI. [Електронний ресурс] – Режим доступу: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>.
16. Закон України “Про Збройні Сили України” від 6 грудня 1991 року № 1934-XII (зі змінами) // Законодавство України [Електронний ресурс] – Режим доступу: <https://zakon.rada.gov.ua/laws/show/1934-12#Text>.
17. Стратегія національної безпеки України, введена в дію Указом Президента України від 14 вересня 2020 року № 392/2020 Про рішення Ради національної безпеки і оборони України], від 14 вересня 2020 року Про Стратегію національної безпеки України [Електронний ресурс] – Режим доступу: <https://www.president.gov.ua/documents/3922020-35037>.
18. Стратегія кібербезпеки України, введена в дію Указом Президента України від 26 серпня 2021 року № 447/2021, – Режим доступу <https://www.president.gov.ua/documents/4472021-40013>.
19. Стратегія воєнної безпеки України, введена в дію Указом Президента України від 25 березня 2021 року № 121/2021 Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року Про Стратегію воєнної безпеки України [Електронний ресурс] – Режим доступу: <https://www.president.gov.ua/documents/1212021-37661>.
20. Указ Президента України №473/2021 від 17 вересня 2021 року №473/2021 Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року “Про Стратегічний оборонний бюлетень України” [Електронний ресурс] – Режим доступу: <https://www.president.gov.ua/documents/4732021-40121>.

21. Указ Президента України №27/2020 28 січня 2020 року Про внесення змін до Указів Президента України від 27 січня 2015 року № 37 та від 7 червня 2016 року № 242 [Електронний ресурс] – Режим доступу: <https://zakon.rada.gov.ua/laws/show/27/2020#Text>.

22. Стратегія інформаційної безпеки України, введена в дію Указом Президента України від 28 грудня 2021 року № 685/2021 Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року Про Стратегію інформаційної безпеки України [Електронний ресурс] – Режим доступу: <https://www.president.gov.ua/documents/6852021-41069>.

23. Живилю Є.О. Сервіси зв'язку об'єднаної мережі за стандартами країн НАТО // Електронна бібліотека Нац. ун-т ім. Ю. Кондратюка, 82 с. – 2023. [Електронний ресурс] – Режим доступу: <http://lib.nupp.edu.ua/elcat/alog?tab=b961c4f53c15ad9d36d3fa0351b68eb0>.

24. Живилю Є.О. Ситуаційний центр Міністерства оборони України – модель завчасного виявлення та аналізу кризових ситуацій сектору безпеки держави // Збірник наукових праць ХНУ ім. В. Н. Каразіна №1 (60) – 2022 [Електронний ресурс] – Режим доступу: <https://periodicals.karazin.ua/apdu/article/view/21125/19764>.

25. Єдиний перелік (каталог) спроможностей Міністерства оборони України, Збройних Сил України та інших складових Сил оборони, затверджено Міністром оборони України 31 грудня 2021 року.

26. Лісаконов В. Багатошарові кібератаки Росії не знають меж, 2019 [Електронний ресурс] – Режим доступу: <https://concordium.com/articles-and-blogs/>.

27. Центр обробки даних контейнерного типу [Електронний ресурс] – Режим доступу: https://it-integrator.ua/sites/default/files/imce/prezentaciya_rishennya_v_umovah_voyennogo_chasu.pdf.

28. Живилю Є.О., Докіль В. М. Модель методики оцінювання спроможностей військ зв'язку та кібербезпеки Збройних Сил України щодо виконання завдань з відбиття воєнної агресії в кіберпросторі // Сучасні інформаційні технології у сфері безпеки та оборони № 1 (46)/2023: – НУОУ, Київ, 2023. – С. 32-40.

REFERENCES:

1. Cherny`sh R.F., Ignatyuk M.V. Proty`diya destrukty`vnomu informacijnomu vply`vu v Ukrayini: pravovi ta organizacijni aspekty` [Elektronny`j resurs] – Rezhy`m dostupu: http://lsej.org.ua/1_2022/54.pdf.

2. Doktry`na zv'yazok ta informacijni sy`stemy`, vvedena v diyu Golovnokomanduvachem Zbrojny`x Sy`l Ukrayiny` vid 20 chervnya 2020 roku, VKP 6-00(01).01.

3. Zhy`vy`lo Ye.O., Chernonog O.O. Strategiya kiberoborony` Ukrayiny` // Zbirny`k naukovy`x prac` VITI # 4 – 2017 [Elektronny`j resurs] – Rezhy`m dostupu: http://www.viti.edu.ua/files/zbk/2017/4/4_4_2017.pdf.

4. Zakon Ukrayiny` “Pro nacional`nu bezpeku Ukrayiny`” vid 21.06.2018 r. # 2469-VIII // Zakonodavstvo Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>.

5. Zakon Ukrayiny` “Pro osnovni zasady` zabezpechennya kiberbezpeky` Ukrayiny`” vid 05.10.2017 r. # 2163-VIII // Zakonodavstvo Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.

6. Zakon Ukrayiny` “Pro zaxy`st informaciyi v informacijno-telekomunikacijny`x sy`stemax” [Elektronny`j resurs] – Rezhy`m dostupu: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>.

7. Zakon Ukrayiny` “Pro rozvidku” vid 17.09.2020 # 912-IX [Elektronny`j resurs] – Rezhy`m dostupu: <https://zakon.rada.gov.ua/laws/show/912-20#Text>.

8. Zakon Ukrayiny` “Pro Nacional`nu programu informaty`zacyi” vid 04.02.1998 r. # 74/98-VR // Zakonodavstvo Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: <https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80#Text>.

9. Zakon Ukrayiny` “Pro raty`fikaciyu Konvenciyi pro kiberzlochy`nnist” vid 10.03.2006 r. # 2163-VIII // Zakonodavstvo Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: <https://zakon.rada.gov.ua/laws/show/2824-15#Text>.

10. Pro Derzhavnu sluzhbu special`nogo zv'yazku ta zaxy`stu informaciyi : Zakon Ukrayiny` vid 23.02.2006 r. [Elektronny`j resurs]. – Rezhy`m dostupu: <https://zakon.rada.gov.ua/laws/show/3475-15#Text>.

11. Zakon Ukrayiny` “Pro derzhavnu tayemny`cyu” vid 21 sichnya 1994 # 3855-XII (zi zminamy`) [Elektronny`j resurs]. – Rezhy`m dostupu: <https://zakon.rada.gov.ua/laws/show/3855-12#Text>.

12. Zakon Ukrayiny` “Pro dostup do publichnoyi informaciyi” vid 13 sichnya 2011 r. # 2939-VI. [Elektronny`j resurs] – Rezhy`m dostupu : <https://zakon.rada.gov.ua/laws/show/2939-17#Text>.

13. Zakon Ukrainy "Pro zaxyst personal'nyx danyx" vid 01.06.2010 r. # 2297-VI [Elektronnyj resurs] – Rezhy'm dostupu: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>.
14. Zakon Ukrainy "Pro oboronu Ukrainy" vid 06.12.1991 r. # 1932-XII // Zakonodavstvo Ukrainy [Elektronnyj resurs] – Rezhy'm dostupu: <https://zakon.rada.gov.ua/laws/show/1932-12#Text>.
15. Zakon Ukrainy Ukrainy "Pro informaciyu" # 2938-VI. [Elektronnyj resurs] – Rezhy'm dostupu: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>.
16. Zakon Ukrainy "Pro Zbrojni Syly Ukrainy" vid 6 grudnya 1991 roku # 1934-XII (zi zminamy) // Zakonodavstvo Ukrainy [Elektronnyj resurs] – Rezhy'm dostupu: <https://zakon.rada.gov.ua/laws/show/1934-12#Text>.
17. Strategiya nacional'noyi bezpeky Ukrainy, vvedena v diyu Ukazom Prezydenta Ukrainy vid 14 veresnya 2020 roku # 392/2020 Pro rishennya Rady nacional'noyi bezpeky i oborony Ukrainy, vid 14 veresnya 2020 roku Pro Strategiyu nacional'noyi bezpeky Ukrainy [Elektronnyj resurs] – Rezhy'm dostupu: <https://www.president.gov.ua/documents/3922020-35037>.
18. Strategiya kiberbezpeky Ukrainy, vvedena v diyu Ukazom Prezydenta Ukrainy vid 26 serpnia 2021 roku # 447/2021, – Rezhy'm dostupu <https://www.president.gov.ua/documents/4472021-40013>.
19. Strategiya voyennoyi bezpeky Ukrainy, vvedena v diyu Ukazom Prezydenta Ukrainy vid 25 bereznia 2021 roku # 121/2021 Pro rishennya Rady nacional'noyi bezpeky i oborony Ukrainy vid 25 bereznia 2021 roku Pro Strategiyu voyennoyi bezpeky Ukrainy [Elektronnyj resurs] – Rezhy'm dostupu: <https://www.president.gov.ua/documents/1212021-37661>.
20. Ukaz Prezydenta Ukrainy #473/2021 vid 17 veresnya 2021 roku #473/2021 Pro rishennya Rady nacional'noyi bezpeky i oborony Ukrainy vid 20 serpnia 2021 roku "Pro Strategichnyj oboronnyj byuletyn Ukrainy" [Elektronnyj resurs] – Rezhy'm dostupu: <https://www.president.gov.ua/documents/4732021-40121>.
21. Ukaz Prezydenta Ukrainy #27/2020 28 sichnia 2020 roku Pro vnesennya zmin do Ukaziv Prezydenta Ukrainy vid 27 sichnia 2015 roku # 37 ta vid 7 chervnia 2016 roku # 242 [Elektronnyj resurs] – Rezhy'm dostupu: <https://zakon.rada.gov.ua/laws/show/27/2020#Text>.
22. Strategiya informacijnoyi bezpeky Ukrainy, vvedena v diyu Ukazom Prezydenta Ukrainy vid 28 grudnya 2021 roku # 685/2021 Pro rishennya Rady nacional'noyi bezpeky i oborony Ukrainy vid 15 zhovtnia 2021 roku Pro Strategiyu informacijnoyi bezpeky Ukrainy [Elektronnyj resurs] – Rezhy'm dostupu: <https://www.president.gov.ua/documents/6852021-41069>.
23. Zhyv'lo Ye.O. Servisy zv'yazku ob'yednanoyi merezhi za standartamy krayin NATO // Elektronna biblioteka Nacz. un-t im. Yu. Kondratyuka, 82 s. – 2023. [Elektronnyj resurs] – Rezhy'm dostupu: <http://lib.nupp.edu.ua/elcat/alog?tab=b961c4f53c15ad9d36d3fa0351b68eb0>.
24. Zhyv'lo Ye.O. Sytuacijnyj centr Ministerstva oborony Ukrainy – model' zavchasnogo vy'yavleniya ta analizu kry'zovy'x sy'tuacij sektoru bezpeky derzhavy // Zbirnyk naukovy'x prac' XNU im. V. N. Karazina #1 (60) – 2022 [Elektronnyj resurs] – Rezhy'm dostupu: <https://periodicals.karazin.ua/apdu/article/view/21125/19764>.
25. Yedy'nyj perelik (katalog) spromozhnostej Ministerstva oborony Ukrainy, Zbrojny'x Sy'l Ukrainy ta inshy'x skladovy'x Sy'l oborony, zatverdzheno Ministrom oborony Ukrainy 31 grudnya 2021 roku.
26. Lisakonov V. Bagatosharovi kiberatomy Rosiyi ne znayut' mezh, 2019 [Elektronnyj resurs] – Rezhy'm dostupu: <https://concordium.com/articles-and-blogs/>.
27. Centr obrobky dany'x kontejnernogo ty'pu [Elektronnyj resurs] – Rezhy'm dostupu: https://it-integrator.ua/sites/default/files/imce/prezentaciya_rishennya_v_umovah_voyennogo_chasu.pdf.
28. Zhyv'lo Ye.O., Dokil V. M. Model' metody'ky' ocinyuvannya spromozhnostej vijs'k zv'yazku ta kiberbezpeky Zbrojny'x Sy'l Ukrainy shhodo vy'konannya zavdan' z vidby'ttya voyennoyi agresiyi v kiberprostorii // Suchasni informacijni tekhnologiyi u sferi bezpeky ta oborony # 1 (46)/2023: – NUOU, Ky'yiv, 2023. – C. 32-40.

**REQUIREMENTS FOR CYBER PROTECTION OF INFORMATION AND
COMMUNICATION SYSTEMS AND COMMUNICATION SERVICES DURING THEIR
DEPLOYMENT AND OPERATION AT THE CONTROL POINTS OF THE COMPONENTS OF
THE DEFENSE AND SECURITY FORCES**

The relevance of this work is due to the fact that in recent years the communication forces have been constantly developing and equipped with the latest digital means of communication, which allows them to successfully perform their assigned tasks. Today, information and communication systems that are deployed at the control points of various branches of management ensure the implementation of priority tasks for the management of troops. Functionally, the communication system and information systems are deployed at control points as a single information and communication environment based on the implementation of the latest information and communication technologies, information exchange protocols, complexes, systems and means of communication, which ensures the exchange of all types of information between bodies military management (management bodies) and control points at all levels of management. An active communication system ensures the exchange of information with guaranteed security in a single information space as a set of material functions (including personnel and other resources) that combine to perform a certain task.

In turn, information systems, as a set of equipment, methods and procedures, and, if necessary, personnel organized to perform information processing functions operate in accordance with a defined structure, namely:

- services, in the context of communication and information systems;*
- architecture, in the context of communication and information systems;*
- functions in the context of service-oriented architecture;*
- interoperability;*
- information protection and cyber protection.*

It is clear that the more important the object of management, the more capacious flow of information can be directed to it. This allows the adversary/attacker to identify the most important targets and direct other types of information to them or suppress them in various ways. Thus, in the interests of ensuring cyber protection of electronic information resources, communication and technological systems of the control points of the Armed Forces of Ukraine, the technological infrastructure of cyber protection of the Armed Forces of Ukraine has been deployed and is functioning, which is a component of the unified system of information protection and cyber protection in the information and communication systems of the Ministry of Defense and the Armed Forces of Ukraine. In these conditions, to solve the tasks of preventing unwanted interventions, disruption of the stable functioning of the information and communication environment at control points, counterweights in obtaining confidential information, data theft, and other minimally necessary components of the cyber protection infrastructure are deployed. The main components of the relevant technological infrastructure of cyber protection are the security information event management system (SIEM), the threat information exchange platform (Malware Information Sharing Platform & Threat Sharing, MISP), the centralized management system of inter-network screens and the system for detecting and countering cyber threats. including computer viruses on end equipment.

Therefore, solving the tasks of ensuring cyber protection in the course of deployment and operation of electronic communication networks and communication services at the control points of various branches of management turns out to be quite a serious and urgent task.

Keywords: control point, information and communication environment, cyber space, cyber threat, cyber security, cyber defense.

Дані про авторів

Бармак Олександр Володимирович, доктор технічних наук, професор, Завідувач кафедри комп'ютерних наук Хмельницького національного університету.

Батрак Євгеній Олександрович, кандидат технічних наук, доцент кафедри Інформаційних систем та технологій ФІОТ КПІ ім. Ігоря Сікорського, ORCID – 0000-0003-3027-4507.

Боровик Дмитро Олегович, студент Хмельницького національного університету.

Боровик Олег Васильович, доктор технічних наук, професор Заступник начальника відділу організації освітньої та наукової діяльності управління професійної підготовки Адміністрації Державної прикордонної служби України.

Георгадзе Олександр Аміранович, кандидат військових наук, доцент, заступник начальника кафедри керівництва військами (силами) в мирний час Національний університет оборони України. ORCID ID: 0000-0002-9306-6660.

Городнов В'ячеслав Петрович, доктор військових наук, професор, професор кафедри тактико-спеціальної підготовки Національної академії Національної гвардії України. ORCID ID: 0000-0001-8593-8871.

Дружинін Віталій Світозарович, ад'юнкт, Військова академія (м. Одеса). ORCID ID: 0000-0001-8254-1836.

Живилю Євген Олександрович, кандидат наук з державного управління, доцент кафедри військової підготовки Військового інституту телекомунікацій та інформатизації імені Героїв Крут (м. Київ), ORCID: 0000-0003-4077-7853.

Жиринов Геннадій Борисович, кандидат технічних наук, старший науковий співробітник, доцент кафедри радіотехніки та радіоелектронних систем, Київський національний університет імені Тараса Шевченка Scopus ID:57193847167 ORCID ID: 0000-0001-7648-7992

Заверуха Григорій Валентинович, старший викладач кафедри Військового інституту танкових військ Національного технічного університету Харківський політехнічний інститут, (Харків, Україна), ORCID - 0000-0001-7447-2033.

Злобін Кирило Вячеславович, начальник Військового коледжу сержантського складу Військового інституту телекомунікацій та інформатизації імені Героїв Крут (м. Полтава), ORCID: 0009-0003-4608-9506.

Кароль Дмитро Анатолійович, викладач кафедри організації розвідувально-інформаційної роботи та технічних засобів розвідки, Військова академія (м. Одеса). ORCID ID: 0009-0002-1649-3770.

Касім Намір Хашім, кандидат технічних наук, доцент, доцент кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва і архітектури, ORCID 0000-0002-7283-0594.

Ключак Оксана Миколаївна, старший науковий співробітник кафедри керівництва військами (силами) в мирний час Національного університету оборони України. ORCID ID: 0000-0003-3422-3379.

Ковальов Ігор Вікторович, кандидат військових наук, доцент кафедри тактико-спеціальної підготовки Національної академії Національної гвардії України. ORCID ID: 0000-0002-7359-5776.

Кондратюк Сергій Миколайович, старший викладач кафедри тилового забезпечення Національний університет оборони України. ORCID ID: 0000-0001-8705-8966.

Кононенко Артем Андрійович, магістр 2-ого року навчання, кафедри радіотехніки та радіоелектронних систем, Київський національний університет імені Тараса Шевченка.

Корчак Олександр Володимирович, доктор філософії з галузі знань Електроніка та телекомунікації, начальник військово-мобілізаційного підрозділу (відділу) Київського національного університету імені Тараса Шевченка ORCID ID: 0000-0003-0801-2340.

Кривцун Володимир Іванович, кандидат технічних наук, старший науковий співробітник, докторант Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, (Львів, Україна), ORCID - 0000-0002-3907-5320.

Кузь Владислав Сергійович, старший викладач циклової комісії експлуатації військових засобів зв'язку Військового коледжу сержантського складу Військового інституту телекомунікацій та інформатизації імені Героїв Крут (м. Полтава), ORCID: 0009-0003-4608-9506.

Купріненко Олександр Миколайович, доктор технічних наук, старший науковий співробітник, професор кафедри Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, (Львів, Україна), ORCID - 0000-0001-6692-0959.

Лаврінченко Владислав, національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського». ORCID ID: 0009-0008-4914-5805.

Ленков Сергій Васильович, доктор технічних наук, професор, Заслужений діяч науки і техніки України, Лауреат, Державної премії України в галузі науки і техніки, головний науковий співробітник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка, ORCID ID: 0000-0001-7689-239x.

Літвіненко Наталія Ігоревна, кандидат технічних наук, старший науковий співробітник науково-дослідного центру, Військового інституту Київського національного університету імені Тараса Шевченка.

Максименко Юрій Анатолійович, кандидат технічних наук, начальник кафедри організації розвідувально-інформаційної роботи та технічних засобів розвідки, Військова академія (м. Одеса). ORCID ID: 0000-0002-1227-2009.

Маляганов Володимир Вікторович, викладач кафедри управління діями підрозділів військової розвідки та сил спеціальних операцій, Військова академія (м. Одеса). ORCID ID: 0000-0001-8294-5531.

Маміч Віктор Володимирович, кандидат технічних наук, доцент, доцент кафедри організації розвідувально-інформаційної роботи та технічних засобів розвідки, Військова академія (м. Одеса). ORCID ID: 0000-0001-5574-0901.

Мірошніченко Олег Вікторович, кандидат технічних наук, старший науковий співробітник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка.

Міщенко Ярослав Сергійович, кандидат технічних наук, доцент, доцент кафедри Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, (Львів, Україна), ORCID - 0000-0002-0231-2361.

Муженко Віктор Миколайович, кандидат військових наук, провідний науковий співробітник Центрального науково-дослідного інституту Збройних Сил України, Київ. ORCID ID: 0000-0002-5023-6463.

Нагачевський В'ячеслав Йосипович, кандидат технічних наук, доцент, начальник кафедри Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, (Львів, Україна), ORCID - 0000-0003-3362-5210.

Пекуляк Роман Олександрович, доктор філософії, старший дослідник, старший науковий співробітник Центрального науково-дослідного інституту Збройних Сил України, Київ. ORCID ID: 0000-0002-1916-211X.

Пехота Сергій Григорович, кандидат військових наук, професор кафедри керівництва військами (силами) в мирний час Національний університет оборони України. ORCID ID: 0000-0002-5175-449X.

Резніков Михайло Ігорович - кандидат технічних наук, доцент, завідувач кафедри теоретичних основ високих технологій Навчально-наукового інституту високих технологій Київського національного університету імені Тараса Шевченка Scopus ID: 57206141858 ORCID ID: 0000-0002-0946-9871.

Скрипник Тетяна Казимирівна, старший викладач кафедри комп'ютерних наук Хмельницького національного університету.

Степанов Михайло Миколайович, доктор технічних наук, старший науковий співробітник, професор кафедри прикладної радіоелектроніки Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського". ORCID ID: 0000-0001-6376-4268.

Тарасюк Дмитро Мефодійович, асистент кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва і архітектури, ORCID ID: 0009-0002-3916-9121.

Трояновська Аліна Олегівна, студентка кафедри Інформаційних систем та технологій ФІОТ КПІ ім. Ігоря Сікорського, ORCID ID: 0009-0002-8702-711X.

Фелінський Георгій Станіславович - доктор фізико-математичних наук, доцент, професор кафедри квантової радіофізики ННІ високих технологій, Київський національний університет імені Тараса Шевченка Scopus ID: 15519293700 ORCID ID: 0000-0001-9377-6227

Фтемов Юрій Олександрович, кандидат технічних наук, старший науковий співробітник, професор кафедри Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, (Львів, Україна), ORCID - 0000-0003-1709-5395.

Хлапонін Юрій Іванович, доктор технічних наук, професор, завідувач кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва і архітектури, ORCID ID: 0000-0002-9287-0817.

Цибізов Андрій Леонідович, кандидат військових наук, старший дослідник, старший науковий співробітник Центрального науково-дослідного інституту Збройних Сил України, м. Київ. ORCID ID: 0000-0001-6555-5005.

Цюпа Наталія Володимирівна, кандидат технічних наук, доцент кафедри Інформаційних систем та технологій ФІОТ КПІ ім. Ігоря Сікорського, ORCID ID: 0000-0002-3215-0711.

Чайковська Олена Євгенівна, старший викладач кафедри керівництва військами (силами) в мирний час Національний університет оборони України. ORCID ID: 0000-0002-0656-9105.

Чорномаз Олексій Олександрович, старший науковий співробітник Центрального науково-дослідного інституту Збройних Сил України. ORCID ID: 0000-0003-2355-3006.

Шаршаткін Данило Юрійович, старший викладач кафедри організації розвідувально-інформаційної роботи та технічних засобів розвідки, Військова академія (м. Одеса). ORCID ID: 0000-0002-3362-2469.

Алфавітний покажчик

Бармак О. В.	98	Кононенко А. А.	59	Пехота С. Г.	14
Батрак Є. О.	87	Корчак О. В.	59	Резніков М. І.	59
Боровик Д. О.	98	Кривцун В. І.	36	Скрипник Т. К.	98
Боровик О. В.	98	Кузь В. С.	118	Степанов М. М.	7
Георгадзе О. А.	14	Купріненко О. М.	36, 72	Тарасюк Д. М.	91
Городнов В. П.	25	Лавріненко В. С.	7	Трояновська А. О.	87
Дружинін В. С.	25	Лєнков С. В.	72	Фелінський Г. С.	59
Живило Є. О.	118	Літвіненко Н. І.	72	Фтемов Ю. О.	36, 72
Жиров Г. Б.	59	Максименко Ю. А.	45	Хлапонін Ю. І.	91
Заверуха Г. В.	36	Маляганов В. В.	45	Цибізов А. Л.	51
Злобін К. В.	118	Маміч В. В.	45	Цьопа Н. В.	87
Кароль Д. А.	45	Мірошніченко О. В.	72	Чайковська О. Є.	14
Касім Н. Х.	91	Міщенко Я. С.	36	Чорномаз О. О.	14
Ключак О. М.	91	Муженко В. М.	51	Шаршаткін Д. Ю.	45
Ковальов І. В.	14	Нагачевський В. Й.	51		14
Кондратюк С. М.	25	Пекуляк Р. О.	51		44

РЕДАКЦІЙНА ПОЛІТИКА ТА ЕТИЧНІ НОРМИ

ПРИНЦИПИ ФОРМУВАННЯ ТА ДОСТУП ДО ЗМІСТУ «ЗБІРНИКА ВІКНУ»

Редакційна політика «Збірника ВІКНУ» заснована на принципах об'єктивності та неупередженості при відборі статей для публікації; високих вимог до якості наукових досліджень; обов'язковості та конфіденційності рецензування статей; додержання колегіальності при відборі до публікації статей; доступності та оперативності у спілкуванні з авторами; суворого дотримання авторських і суміжних прав. Запобігання протизаконним публікаціям є відповідальністю кожного автора, редактора, рецензента, видавця.

До друку приймаються оригінальні рукописи, які не опубліковано раніше, не було відправлено до інших редакцій та які повністю відповідають вимогам щодо оформлення та порядку подання статей.

У «Збірнику ВІКНУ» сформовані наступні рубрики: військова техніка і технології подвійного призначення, інформаційні технології, загальні питання.

Редакція підтримує політику відкритого доступу та принципи вільного поширення наукової інформації. Примірники збірників знаходяться у Національній бібліотеці України ім. В.І. Вернадського, науковій бібліотеці ім. М. Максимовича, у бібліотеці Військового інституту та інших бібліотеках України. Електронна версія розміщена на сайті інституту, на сайтах наведених бібліотек та на сайтах «Збірника ВІКНУ»: <http://miljournals.knu.ua/index.php/zbirnuk>; <http://mil.univ.kiev.ua/page/lib/31>

ЕТИКА ПУБЛІКАЦІЙ

Редакційна колегія журналу вимагає від авторів наслідувати формальним та етичним правилам підготовки і публікації наукових робіт, що вони подають до редакції журналу. Ці норми зумовлено стандартами якості наукових статей, прийнятими у світовому науковому співтоваристві, зокрема публікаційними принципами Publishing Ethics Resource Kit (PERK), рекомендаціями Elsevier, Комітету з етики публікацій (Committee on Publication Ethics, COPE), етичним кодексом вченого України, а також досвідом роботи іноземних та українських професіональних спільнот, наукових організацій, редколегій та редакцій видань.

ЕТИЧНІ ЗОБОВ'ЯЗАННЯ РЕДАКЦІЙНОЇ КОЛЕГІЇ ЖУРНАЛУ

Редакційна колегія у своїй діяльності:

- керується принципами неупередженості, наукової етики рецензування, захисту – інтелектуальної власності,
- несе відповідальність за рівень наукового наповнення журналу,
- виступає проти фальсифікації, плагіату, направлення автором одного рукопису до кількох журналів, багаторазового копіювання тексту статті в різних місцях, введення громадськості в оману щодо реального внеску кожного автора в опубліковану наукову роботу;
- залишає за собою право направити рукопис на розгляд сторонньому рецензенту, у тому числі ретельний відбір через «сліпе» рецензування, відхилити статтю або повернути її на доопрацювання;
- може відхилити рукопис, якщо вважає, що він не відповідає профілю журналу, чи не відповідає етиці та правилам оформлення,
- має право вилучити вже опубліковану статтю в разі виявлення порушення будь-чиїх прав або загальноприйнятих норм наукової етики, про даний факт вилучення статті редакція повідомляє як автору статті, так і організації, де було виконано дослідження та повідомляє про це у наступному номері.

Співробітники редакції не надають іншим особам інформації, пов'язаної із змістом рукописів, що перебувають на розгляді, крім осіб, які беруть участь у її фаховій оцінці

Згідно з міжнародним законодавством щодо додержання авторського права на електронні інформаційні ресурси, матеріали сайту, електронного журналу або проекту не можуть бути відтворені повністю або частково в будь-якій формі (електронній чи друкованій) без попередньої письмової згоди редакції журналу. При використанні опублікованих матеріалів у контексті інших документів обов'язково необхідними є посилання на першоджерело.

ЕТИЧНІ ЗОБОВ'ЯЗАННЯ АВТОРА

Автор:

- несе відповідальність за новизну і достовірність наведених у статтях результатів, тактико-технічних та економічних показників, коректність висловлювань а також за те, що в матеріалах не міститься інформація з обмеженим доступом;

- повинен цитувати ті публікації, які мали визначальний вплив на суть викладеного у статті, а також ті, які можуть швидко ознайомити читача з більш ранніми працями, важливими для розуміння цього дослідження, необхідно також належним чином вказувати джерела принципово важливих матеріалів, використаних у даній роботі, якщо вони не були отримані самим автором;

- забезпечує недопустимість плагіату та подання до публікації раніше надрукованих матеріалів, у випадку виявлення зазначених фактів відповідальність несе автор поданих матеріалів.

Співавторами статті мають бути всі особи, що зробили вагомий науковий внесок у подану роботу і поділяють відповідальність за отримані результати. Автор, який подає рукопис до публікації, відповідає за те, щоб до списку співавторів були включені тільки ті особи, які відповідають критерію авторства, і бере на себе відповідальність за згоду інших авторів статті на її публікацію в журналі.

УВАГА!

Для авторів статей дещо доопрацьовані вимоги щодо особистих даних.

Ці данні подаються українською та англійською мовами в такій послідовності:

Прізвище _____
Ім'я _____
По батькові (за бажанням) _____
Науковий ступінь та вчене звання _____
Місце роботи та посада _____
ORCID 0000-0001-3215-4400
SCOPUS ID 57193059215 (при наявності)
Індекс DBLP 10 (при наявності)
e-mail: _____
моб. телефон _____

Надсилати скановані рисунки, формули та таблиці не допускається.

Вся стаття оформлюється одним шрифтом **Times New Roman** вказаними нижче розмірами, зверніть увагу на формули, таблиці та рисунки.

РЕДАКЦІЙНА КОЛЕГІЯ «ЗБІРНИКА ВІКНУ» ЗДІЙСНЮЄ НЕЗАЛЕЖНЕ («СЛІПЕ») ЕКСПЕРТНЕ РЕЦЕНЗУВАННЯ НАДАНИХ ДО ДРУКУ РУКОПИСІВ ТА ПЕРЕВІРКУ ЇХ НА ПЛАГІАТ. РЕЦЕНЗУВАННЯ ЗДІЙСНЮЄТЬСЯ ЗА АНОНІМНОЮ ФОРМОЮ ЯК ДЛЯ АВТОРІВ, ТАК І ДЛЯ РЕЦЕНЗЕНТІВ.

ПОРЯДОК ПОДАННЯ І ОФОРМЛЕННЯ СТАТЕЙ ДО "ЗБІРНИКА НАУКОВИХ ПРАЦЬ ВІЙСЬКОВОГО ІНСТИТУТУ КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ ІМЕНІ ТАРАСА ШЕВЧЕНКА"

До друку приймаються оригінальні рукописи, які не опубліковано раніше, не було відправлено до інших редакцій та які повністю відповідають вимогам щодо оформлення та порядку подання статей.

Загальні вимоги до технічного оформлення статей:

Обсяг рукопису - рекомендується **не менше 12 повних аркушів** українською або англійською мовами.

Формат аркуша - **A4 (210 x 297 мм)**.

Розмір полів: верхнє, нижнє, правє, лівє - **2 см**.

Шрифт тексту - **Times New Roman №12**, через міжрядковий інтервал - **1,0**.

Абзац має становити **10 мм**.

Стаття повинна мати такі необхідні елементи:

УДК;

назва статті, яка лаконічно відображає зміст та новизну статті;

анотація та ключові слова;

вступ та постановка задачі чи проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями;

аналіз останніх досліджень і публікацій, в яких започатковано **розв'язання даної проблеми** і на які спирається автор, визначення невирішених раніше частин загальної проблеми, котрим присвячується означена стаття, формулювання мети статті;

виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів, практичних рішень та експериментів;

висновки з даного дослідження і перспективи подальшого розвитку у даному напрямку.

**список літератури,
References,
дані про авторів** двома мовами.

Анотація до статті виконується українською та англійською мовами загальний обсяг кожної не менш ніж **1800** знаків, включаючи ключові слова.

Вона повинна містити коротке повторення структури статті, що включає вступ, цілі і завдання, методи, результати, висновки.

Анотацію друкують курсивом, шрифт Times New Roman, №11. Після анотації розміщуються **ключові слова** (5–7 термінів).

Список літератури (References) повинен включати не менш 12 джерел, з яких 50 % видані за останні 10 років. При цьому не менш 25 % джерел повинно відноситися до іноземної періодики. Самоцитовання авторів у списку літератури повинно бути, як правило, не більш за 25 %.

Якщо основною мовою статті є українська, то оформлюються два списки літератури:

перший (список літератури мовою оригіналу джерела) – згідно наказу МОН від 12.01.2017 № 40 та відповідно до ДСТУ 8302:2015 «Інформація та документація. Бібліографічне посилання: загальні положення та правила складання»;

другий (REFERENCES) з урахуванням ДСТУ 8302:2015, наказу МОН від 12.01.2017 № 40 та міжнародного Гарвардського стилю BSI (British Standards Institution).

На адресу редколегії (03680. м. Київ, вул Ломоносова 81, тел.: +38 (044) 521 - 33 - 82) мають бути надіслані наступні матеріали:

експертний висновок, про можливість відкритого публікування, завірений печаткою, сканкопія надсилається на e-mail: lenkov_s@ukr.net

Відомості про авторів див.на стор.150.

Вимоги до оформлення References

References потрібно приводити окремим блоком, повторюючи послідовність попередньо наведеного Списку літератури. Джерела при цьому оформлюються за такими основними правилами (Harvard style оформлення BSI: British Standards Institution):

– запис завжди починається з прізвища автора, потім, через кому, ініціали (між ініціалами пропуски не ставляться), за якими в дужках вказується дата видання; два автори відокремлюються «and» без коми; кілька авторів розділяються комами, але останнє прізвище повинно бути відокремлено «and» без коми;

– витяги з публікацій, тобто назви статей журналів, глав в книгах наводять у "лапках";

– назва журналу або книги завжди виділяється курсивом;

– ім'я видавця вказується перед місцем видання;

– коми використовують для поділу елементів запису;

– для джерел українською або російською мовою, що наводяться у References, назви статей журналів, глав в книгах наводять латиницею (транслітерацією) у "лапках" та перекладом на англійську мову у квадратних дужках. Онлайн-конвертер з української мови для транслітерації: <http://translit.kh.ua/?passport>.

Приклади оформлення References за стилем Harvard British Standards Institution

Книга (ДСТУ 8302:2015)

Інформаційно-психологічна боротьба у війсьній сфері : монографія / Г.В. Певцов, А.М. Гордієнко, С.В. Залкін, С.О. Сідченко, А.О. Феклістов, К.І. Хударковський. Х. : Вид. Рожко С.Г., 2017. 276 с.

Книга (Harvard style BSI)

Pievtsov, H.V., Hordiienko, A.M., Zalkin, S.V., Sidchenko, S.O., Feklistov, A.O. and Khudarkovskyi, K.I. (2017), "Informatsiino-psykholohichna borotba u voiennoi sferi: monohrafiia" [The information and psychological struggle in the military sphere], Rozhko S.H., Kharkiv, 276 p.

Стаття із періодичного видання (ДСТУ 8302:2015)

Карпенко, Д.В. Стан та перспективи розвитку зенітного ракетного озброєння Повітряних Сил Збройних Сил України / Наука і техніка Повітряних Сил Збройних Сил України. 2017. № 2(27). С. 75–78.

Стаття із періодичного видання (Harvard style BSI)

Karpenko, D.V. (2017), "Stan ta perspektyvy rozvytku zenitnoho raketnoho ozbroiennia Povitrianykh Syl Zbroinykh Syl Ukrainy" [The state and perspectives of the development of anti-aircraft missile armaments in the Air Force of Ukraine], Science and Technology of the Air Force of Ukraine, No. 2(27), pp. 75–78.

Дисертація (ДСТУ 8302:2015)

Белозеров, И.В. Религиозная политика: дис. ... канд. ист. наук: 07.00.02; защищена 22.01.02; утв. 15.07.02 / Белозеров Иван Валентинович. К., 2002. 215 с.

Дисертація (Harvard style BSI)

Belozеров, I.V. (2002), "Relyhyoznaia polytyka: dissertation" [The religious policy: dissertation], Kiev, 215 p.

Джерела електронного ресурсу віддаленого доступу (ДСТУ 8302:2015)

Романов В. К вопросу о путях достижения национальной безопасности в условиях глобализации: проблемы теории и практики в контексте внешней политики России и Польши [Електронний ресурс] Безопасность и оборона, 2016. № 1(2), С. 7–15. Режим доступа до журн.: http://www.desecuritate.uph.edu.pl/images/De_Securitate_12_2016.pdf.

Джерела електронного ресурсу віддаленого доступу (Harvard style BSI)

Romanov, V. (2016), "K voprosu o putyakh dostizheniya natsionalnoy bezopasnosti v usloviyakh globalizatsii: problemy teorii i praktiki v kontekste vneshney politiki Rossii i Polshi" [To the question about the ways to achieve national security in the context of globalization: the problems of theory and practice in the context of the foreign policy of Russia and Poland], Security and Defence Journal, No. 1(2), pp. 7–15, www.desecuritate.uph.edu.pl/images/De_Securitate_12_2016.pdf (accessed 12 July 2017). (примітка: при наведенні URL "http: //" має бути виключено).

Більш детальну інформацію щодо оформлення бібліографічних посилань за стилем Harvard British Standards Institution можна знайти на сайті *Національної бібліотеки України імені В.І. Вернадського* та онлайн генератора посилань *Cite This For Me*.

Редакційна колегія: e-mail: lenkov_s@ukr.net

Шрифт

СХЕМА ОФОРМЛЕННЯ СТАТЕЙ У «ЗБІРНИКУ НАУКОВИХ ПРАЦЬ ВІКНУ»

УДК

науковий ступінь, вчене звання

ініціали та прізвище автора (співавторів)

Місце роботи автора (співавторів)

12 пт

УДК 32.973.202:07.681

д.т.н., проф. Степанов С.В. (ВІКНУ)

к.т.н., с.н.с. Українець О.В. (ВІКНУ)

к.т.н. Саленко В.Д. (ВІКНУ)

12 пт

жирний

КЕРУВАННЯ ЕЛЕКТРОННИМИ ПРИСТРОЯМИ ЗА ДОПОМОГОЮ ЖЕСТИВ

Анотація до статті виконується українською та англійською мовами (загальний обсяг кожної не менш ніж **1800** знаків, включаючи ключові слова).

11 пт

курсив,
жирний

Для керування електронними пристроями, для сучасного користувача важливими критеріями є такі, як: зручність та простота керування. Для того щоб надати користувачу такі можливості та зручності в використанні, є досить доцільною розробка системи, яка б надавала такі можливості. Керування системою, яка працює на основі жестів, є надзвичайно перспективним, та може суттєво полегшити користувачу роботу з нею, тому що, жести які потрібні для керування системою, можуть бути інтуїтивно зрозумілими користувачу, порівняно з іншими системами які працюють за допомогою комбінацій клавіш.

Для вирішення задач керування за допомогою жестів, пропонується програмно-апаратний комплекс, який побудований на основі різних модулів, кожен з яких в свою чергу виконує відповідну роль в системі, наприклад знаходить точку інтересу з множини чи вираховує глибину сцени. Також в системі є ядро, яке відповідає за аналіз модифікаторів та жестів. На основі даних модулів стає можливо створити систему, яка б працювала на основі жестів. Але для створення даної системи, потрібно вирішити певні задачі, такі як: сегментація, скелетизація, спостереження. Кожна з яких містить в собі відповідні математичні моделі та визначення. Запропонований програмно-апаратний комплекс для керування природними жестами. Суть програмно-апаратного комплексу полягає в тому, щоб забезпечити користувача таким інтерфейсом, щоб він виконував роботу знаходячись частково віддалено від робочого місця, чи маніпулював інструментами на відстані, тобто за допомогою жестів. Використання запропонованого програмно-апаратного комплексу дозволить покращити показники стерильності в операційних, підвищити технічну безпеку під час виконання безпосередньої роботи користувача з приладами.

Ключові слова: штучний інтелект, контролери, модулі, жести, глибина сцени, точка інтересу, аналіз модифікаторів, аналіз жестів, сегментація, скелетизація, спостереження.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ СТАТТІ

12 пт

НЕОБХІДНІ ЕЛЕМЕНТИ СТАТТІ: вступ та постановка проблеми (задачі) у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями; аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми і на які спирається автор, виділення невирішених раніше частин загальної проблеми, яким присвячується дана стаття, формулювання цілей статті (постановка завдання), виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів; їх практичного значення та результатів експерименту чи впровадження; висновки з даного дослідження і перспективи подальших досліджень у даному напрямку. Література. References.

УВАГА! Таблиці і рисунки друкують після посилань. Якщо у статті кілька таблиць чи рисунків - їх нумерують. Заголовки таблиць і рисунків необхідно

розмішувати по центру, а нумерацію таблиць праворуч від таблиці (стиль **normal**, шрифт – **Times New Roman № 12**). **Рисунки** повинні бути виконані за допомогою редактора **Word**, згруповані і являти собою один графічний об'єкт. **Формули** та позначення по тексту обов'язково набирати за допомогою **Equation Editor** - редактора формул **Word**, а не у текстовому режимі. У редакторі формул мають бути встановлені такі параметри - розміри: загальний – **12 pt**. великі індекси – **10 pt** , малі індекси – **7 pt**, великі символи – **14 pt**. малі символи – **10 pt**: стиль: текст, функції, змінні, матриці-вектори, числа – шрифт **Times New Roman**, для решти стилів – шрифт **Symbol**, при цьому: строк. грецькі – прямі. Великі за розміром вирази та рівняння необхідно записувати у кілька рядків.

ЛІТЕРАТУРА

Перший (список літератури на мові оригіналу джерела) – згідно наказу МОН № 40 від 12.01.2017 та відповідно до ДСТУ 8302:2015 «Інформація та документація. Бібліографічне посилання: загальні положення та правила складання»;

другий (REFERENCES) з урахуванням ДСТУ 8302:2015, наказу МОН № 40 від 12.01.2017 та міжнародного Гарвардського стилю BSI (British Standards Institution).

ЛІТЕРАТУРА:

11 пт

ЗРАЗОК

1. Ленков С.В., Толлок І.В., Цицарев В.М., Ленков Є.С. Моделювання процесів витрачання та поповнення ресурсу угруповання технічних об'єктів. *Системи озброєння і військова техніка*. Харків. 2018. Вип. 1(53). С. 155 – 162.

2. Жиров Г.Б., Ленков Є.С., Цицарев В.М., Проценко Я.М. Моделювання процесу відмов об'єктів, що відновлюються з ієрархічною конструктивною структурою. *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка*. Київ. 2017. Вип. 55. С. 30-39.

REFERENCES:

11 пт

ЗРАЗОК

1. Lienkov, S.V., Tolok, I.V., Tsytsarev, V.N. and Lenkov, Ye.S. (2018), "Modeliuvannia protsesiv vytrachannia ta popovnennia resursu uhrupuvannia tekhnichnykh obiektiv" [Modeling of processes of expenditure and resource replenishment grouping of technical objects], *Systems of Arms and Military Equipment*, No. 1(53), pp. 155-162.

2. Zhyrov, G.B., Lenkov, Je.S., Cycarjev, V.M. and Procenko, Ja.M. (2017), "Modeljuvannja procesu vidmov ob'ektiv, shho vidnovljujut'sja z ijerarhichnoju konstruktyvnoju strukturoju" [Simulation of the process of failure of objects that are restored with a hierarchical constructive structure], *Zbirnyk naukovykh prac' Vijs'kovogo instytutu Kyi'vs'kogo nacional'nogo universytetu imeni Tarasa Shevchenka*, No. 55, pp. 30-39.

Prof. Stepanov S.V., Ph.D. Ukrainets O.V., Ph.D. Salenko V.D.

CONTROL ELECTRONIC DEVICES USING GESTURES

11 пт

курсів,
журний

For management of electronic devices, for today's user important criteria are: convenience and ease of management. In order to provide the user with such opportunities and usability to use, it is quite reasonable to develop a system that would provide such opportunities. Managing a gesture-based system is extremely promising, but can greatly facilitate the user to work with it, because the gestures that are needed to manage the system can be intuitive to the user, compared to other systems that operate using keyboard shortcuts. To solve the problems of managing using gestures, a software-hardware complex is proposed that is based on different modules, each of which in turn plays an appropriate role in the system, for example, finds a point of interest from a plurality or calculates the depth of a scene. Also, the system has a kernel that is responsible for analyzing modifiers and gestures. Based on the data of the modules it becomes possible to create a system that would work on the basis of gestures. But for the creation of this system, it is necessary to solve certain problems, such as: segmentation, skeletalization, observation. Each of them

contains the corresponding mathematical models and definitions. Proposed hardware and software complex for management of natural gestures. The essence of the software and hardware complex is to provide the user with such an interface that he was performing work while being partially remote from the workplace, or manipulating tools at a distance, that is, using gestures. The use of the proposed software-hardware complex will improve the sterility parameters in the operating system, increase the technical safety during the direct work of the user with the devices.

Keywords: *artificial intelligence, controllers, modules, gestures, depth of the scene, point of interest, analysis of modifiers, gesture analysis, segmentation, skeletonization, observation.*

Дані про авторів див.стор.150

ЗРАЗОК

11 пт

Степанов Сергій Вікторович, доктор технічних наук, професор, Заслужений діяч науки і техніки України, Лауреат Державної премії України в галузі науки і техніки, головний науковий співробітник Військового інституту Київського національного університету імені Тараса Шевченка, ORCID – 0000-1202-6512-1234, ORCID ID 0000-0001-3215-4400, SCOPUS ID 57193059215 (при наявності), індекс DBLP 10 (при наявності), e-mail:stepanov@ukr.net, тел. 068 652 26 62.

Українець Олексій Васильович, кандидат технічних наук, старший науковий співробітник, провідний науковий співробітник Військового інституту Київського національного університету імені Тараса Шевченка, ORCID – 0000-1204-6512-1235, ukr@ukr.net, 073 556 6776. SCOPUS ID 57193059215 (при наявності), індекс DBLP 10 (при наявності), e-mail:stepanov@ukr.net, тел. 068 652 26 62.

Саленко Володимир Дмитрович, кандидат технічних наук, науковий співробітник Військового інституту Київського національного університету імені Тараса Шевченка, ORCID – 0000-1201-6512-1236, salenko@ukr.net, 0938763423. SCOPUS ID 57193059215 (при наявності), індекс DBLP 10 (при наявності), e-mail:stepanov@ukr.net, тел. 068 652 26 62.

Stepanov Sergij, doctor of technical sciences, professor, Chief Researcher of the Military Institute of Kiev National Taras Shevchenko University (Kiev, Ukraine)

Ukrainets Oleksij, candidate of Technical Sciences, Senior Researcher, Leading Researcher of the Military Institute of Kyiv National Taras Shevchenko University (Kiev, Ukraine)

Salenko Volodymyr, candidate of engineering sciences, Researcher of the Military Institute of Kiev National Taras Shevchenko University (Kiev, Ukraine).

Наукове видання



ЗБІРНИК НАУКОВИХ ПРАЦЬ

Військового інституту

**Київського національного університету
імені Тараса Шевченка**

№ 80

Усі матеріали надруковані в авторській редакції

Підписано до друку 25.01.24 р.
Авт. друк. арк. 18. Формат 60х90/8
Безкоштовно. Замовлення № 2-24

Надруковано у навчальному картографічному комплексі ВІКНУ

03189, Київ, вул. Ю. Здановської, 81

т. 521-32-89