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

ВІЙСЬКОВИЙ ІНСТИТУТ
КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

ЗБІРНИК НАУКОВИХ ПРАЦЬ

ВІЙСЬКОВОГО ІНСТИТУТУ КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ ІМЕНІ ТАРАСА ШЕВЧЕНКА

Виходить 4 рази на рік

№ 73

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 – 2021

УДК621.43
ББК 32-26.8-68.49
Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. К.: ВІКНУ, 2021. № 73. 132 с.

Редакційна колегія прагне до покращення змісту та якості оформлення видання і буде вдячна авторам та читачам за висловлювання зауважень та 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 16.12.21р., протокол № 9.

Відповідальні за макет:
Ряба Л.О., Солодєєва Л.В.

Адреса редакції: 03189, м. Київ, вул. Ломоносова,81 тел./факс +38 (044) 521 – 33 – 82
Наклад 300 прим.
Ел.адреса редактора: lenkov_s@ukr.net
Офіційний сайт журналу: http://miljournals.knu.ua/

ЗМІСТ

ВІЙСЬКОВА ТЕХНІКА І ТЕХНОЛОГІЇ ПОДВІЙНОГО ПРИЗНАЧЕННЯ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

CONTENTS

MILITARY EQUIPMENT AND TWO-DESTINATION TECHNOLOGIES

INFORMATION TECHNOLOGIES

UDK 351.74

D.Sci. Tech. **Babiy Yu.A.** (NASBGSU)
PhD **Polishchuk V.V.** (NASBGSU)
Martinyuk V.P. (NASBGSU)
Martinyuk A.V. (NASBGSU)
Chernousov D.A. (NASBGSU)

DOI: https://doi.org/10.17721/2519-481X/2021/73-01

ESTABLISHMENT OF BORDER SECURITY AS A COMPONENT OF NATIONAL SECURITY OF UKRAINE

An analysis of recent scientific publications and special literature on national security issues shows that approaches to the methodological aspects of research in this area are currently in place. The problem of delimitation of certain components of national security, in particular border security, remains relevant. However, its key concepts are not clearly defined, which complicates the definition of the subject of research, accurate analysis and preparation of appropriate recommendations for its implementation. As a result, the issue of border security is currently not deeply studied, in particular, insufficient attention is paid to geopolitical realities, external and internal factors that affect its state. This can be confirmed by a number of scientific publications that demonstrate simplified views of the state border. It is perceived simply as a physical line of demarcation of the territory of states, draws conclusions about the "blurring" of borders between European states and questions the need to protect them in the era of globalization. At the same time, the competence and tasks of the border institution are limited only to checking the documents of travelers across the border at checkpoints and control of its area outside them.

Taking into account the main trends and consequences of deep transformations of geopolitical and geoeconomic space, today there is a need for thorough research in the field of border security of Ukraine as a component of national security, as well as defining a clear place and role of its guarantee. functions, especially with the emergence of new types of threats, in particular: the temporary occupation by the Russian Federation of part of Ukraine - the Autonomous Republic of Crimea and the city of Sevastopol, Russia's incitement to armed conflict in the eastern regions of Ukraine, the threat of its spread through the territory of our state, but also aimed at destroying the system of world and regional security and the principles of international law.

We consider it necessary to substantiate the structure and content of the border security model as the basis for further development of the State Border Guard Service of Ukraine, which is the basis for the formation and implementation of modern European border policy, including bringing Ukrainian border legislation to European law.

Key words: risk, threat, national security, border security, border security model.

Introduction. For Ukraine, the issue of border security, given the course of Euro-Atlantic integration, and one of the main requirements for the accession of new countries to the Schengen Union is to ensure border security, is certainly relevant and a priority. Thus, the recent enlargement of the European Union, the geopolitical position of Ukraine determine the fact that the borders of our country play an important and universally recognized role in shaping the system of European security. It should be noted that the interests of Ukraine and the European Community in the management of common borders, of course, coincide. This is to ensure reliable protection of long sections of the state border of Ukraine; unimpeded legal crossing of the border by citizens and vehicles at checkpoints along with a high level of control procedures; proper management of migration flows; effective counteraction to the manifestations of organized cross-border crime.

Formulation of the problem. Our state supports the creation of a fundamentally new system of European security, which is based on non-power (political, economic, social, energy, environmental, information, etc.) aspects. Thus, it is necessary to substantiate the structure and content of the model of border security, which is the basis for the formation and implementation of modern border policy

of the European model, in particular, bringing border legislation of Ukraine to European law; ensuring the readiness of human resources; technical re-equipment; achieving the current state of state border infrastructure; information integration; qualitatively new level of cross-border cooperation. Analysis of recent research and publications.

Analysis of research and publications. According to the analysis of the theoretical foundations of the study of the problem of national security of Ukraine, to date, there are well-established approaches to the methodological aspects of research in this area. Basic concepts such as "risk", "challenge", "threat", "security", "danger", "national security", etc. are defined [1]. At the same time, the problem of delimitation of certain components of the national security system remains relevant, in particular the selection and theoretical understanding of such an element as border security [2, 3]. The key concepts of border security have not yet been clearly defined. This complicates the definition of the subject of research, its accurate analysis and preparation of relevant recommendations [4, 5]. Therefore, given the main trends and consequences of deep transformations of the geopolitical and geoeconomic space of the end of the last and the beginning of the present century, there is a need for thorough research in the field of border security. Based on the official definition of national security, given in the Law of Ukraine "On Fundamentals of National Security of Ukraine" [2], the official point of view adopted in scientific circulation [6, 7], border security can be defined as the protection of vital interests of the individual, society and the state in its border area, in which society, state and individual are not harmed, but on the contrary, create conditions for their interests related to freedom of movement across the state border [5], offenses are promptly detected and stopped, threats to national security at the border are countered and systematic activities are carried out to eliminate the causes of their occurrence.

Thus, border security must be considered an integral part of national security. It should include the following elements: scientific theory, concept, policy, strategy and tactics, a set of state and public institutions and organizations that ensure border security, means of ensuring it. The purpose of the article is to reveal the structure and content of the border security model as the basis for further development of the State Border Guard Service of Ukraine, which is the basis for the formation and implementation of modern European border policy.

Mane part. In our opinion, the formation and functioning of the border security system is based on certain laws. This is primarily the dependence of its construction on the nature of threats, and efficiency and effectiveness - on the economic potential of the state. The real perception and analysis of threats and risks, their correct classification and assessment are a must. The border security system must be flexible, change quickly depending on external and internal factors, their magnitude and dynamics of change. The formation and effective implementation of border policy is crucial in achieving the appropriate level of border security. It should be noted that in 2002, in pursuance of the decision of the National Security and Defense Council of Ukraine, an interdepartmental working group developed a draft Concept (basics) of border policy and security of Ukraine [8]. The concept proposed to consider border policy as a set of measures aimed at ensuring the sovereignty, inviolability and integrity of the territory, the implementation and protection of national interests and security of the state in its border area. It was determined that it is implemented through purposeful and coordinated activities of public authorities and local governments in accordance with their powers and responsibilities in this area. For some reason, the concept was not approved. However, after the adoption of the Law "On the Fundamentals of National Security of Ukraine" and the approval by the Presidential Decree of the National Security Strategy of Ukraine, the proposed approaches need further study and development in scientific and theoretical terms. To this end, it is important to analyze the approaches to the formation and implementation of border policy, building the border security system of Ukraine in 1991–2008, which allows us to draw the following conclusions [9]: first, with Ukraine's independence, its border policy was aimed at ensuring territorial integrity, creating its own border security system, organizing border protection around the perimeter (about 7,000 km, of which 1,300 km is a sea area) and protection exclusive (maritime) economic zone (about 82 thousand sq. km); secondly, the formation of the border security system was influenced by a number of factors, including: Ukraine's location in the east of the united Europe and the passage of

Eurasian transport corridors through its territory; the presence of "frozen" conflicts in the regions bordering Ukraine; illegal migration and smuggling activities that have become organized across borders; the absence of any border infrastructure on two thirds of the border (more than 4.5 thousand km), which were not defined in the legal contract and were not protected, the need for significant resources for its development, etc. thirdly, the process of formation and implementation of border policy in this period can be divided into four stages [9]: the first – 1991–1993; the second – 1994–1999; the third – 2000–2005; the fourth – 2006–2015. This division is made in view of the adoption and implementation of relevant regulations, concepts and programs (state, target, etc.), which determined the main directions of the formation of border security and the mechanism of their implementation. At the first stage, the main efforts were aimed at determining (establishing) the legal status and ensuring the inviolability of the state border, developing a basic legal basis in the field of border security, approaches to creating a national border institution and building border infrastructure. The key to the formation of the border security system at that time were the first official acts: "Declaration of State Sovereignty of Ukraine", "Act of Independence of Ukraine", Laws "On Succession of Ukraine" and "On the State Border of Ukraine", which determined that the USSR , which separates the territory of Ukraine from other states, and the border between the USSR and BSSR, RSFSR, RM as of July 16, 1990 is the state border of Ukraine, it is inviolable and any border violations are decisively stopped [10]. Depending on the existing conditions and potential threats, the share of border security in the national security system changes. During this period, it was particularly large and had significant political significance. At the end of 1993, state approaches to border development were developed and reflected in the Comprehensive Program approved by the President of Ukraine [11]. It was implemented during the second stage. At the same time, the basic regularity in the field of border security is clearly traced, namely: resolving the contradictions between threats on the one hand and the economic potential of the state on the other. That is why the main forces and resources were aimed at building the Ukrainian-Moldovan border. This decision was influenced by the Transnistrian conflict and, consequently, the threats that arose in this area [12].

At the same time, on the border with Russia and Belarus (until 1998) the main efforts were aimed at carrying out control functions in temporarily equipped checkpoints and operational cover of the "green border". The analysis of the third stage allows us to define it as a stage of active reforms. The implementation of state policy in the field of border security was carried out through the adoption of the second program [13] and a number of legislative acts. They not only identified measures to improve legal regulation, but also stimulated serious reforms of the main institution that implements border policy. During this period, the border agency demonstrates unprecedented openness of action and strategic planning. An example of this is a number of international conferences, starting with the first in Brussels (2002), public discussion of the draft basic law on the State Border Guard Service of Ukraine, attracting the help of international experts and more. This Law and other normative legal acts, adopted in 2003, created a legal basis for reforming the border institution from military to law enforcement [13 - 15]. Thus, the analysis of the third stage allows us to draw the following conclusions: First, it is currently impossible to use old methods effectively in a rapidly changing world. Despite the fact that external threats have acquired mostly non-military forms, they are no less painful for society and national security. These conclusions were made by the leadership of the border agency, after which its reform began, which was preceded by an understanding of the need for profound change and a thorough study of European experience. Secondly, at the third stage a number of transformations were successfully carried out, which affected all spheres of activity of the border agency: powers, structure, systems of staffing and training, forms and methods of service. Significant steps have been taken to develop the border infrastructure, technical re-equipment, and establish cooperation with the state authorities of the border regions, including the arrangement of the border. Third, the demarcation of the first new section of the border (Ukrainian-Moldovan) and its marking unilaterally in other non-demarcated areas has begun. Fourth, border security measures have acquired a new quality at the international level, both bilaterally and multilaterally. In particular, a number of joint projects with the EU and the US are being successfully implemented. A new form of cooperation related to the activities of the European Commission Mission on the Ukrainian-Moldovan border has

been introduced. The fourth stage began in 2006 after the President of Ukraine approved the Concept of Development of the State Border Guard Service of Ukraine for the period up to 2015. In developing the provisions of the Concept, the Government approves the State Targeted Law Enforcement Program "Arrangement and Reconstruction of the State Border of Ukraine" for the period up to 2015 (state customer and main executor of the State Border Guard Service of Ukraine). These strategic documents envisage not only significant changes in the organization of the border department, construction of a modern integrated border protection system and protection of Ukraine's sovereign rights in its exclusive (maritime) economic zone, but also improvement of the border security system as a whole [15, 16]. Based on the analysis of the first four years of the fourth stage (2006-2009), evaluation of the results of actions and effectiveness of border security policy, the following conclusions can be drawn:

First, there is every reason to assess actions in the field of border security as progressive, balanced and appropriate. They included a range of activities: legislative and regulatory regulation; contractual and legal registration of the border; conclusion of international treaties and agreements; development of the border institution (structural changes; reorganization of the management system; introduction of risk management and criminal analysis systems; reform of the Maritime Guard; transition to full staffing on a contract basis; reform of the training system; optimization of the logistics system; technical re-equipment of border units according to law enforcement needs etc). Secondly, the level of protection of national interests at the state border is further increased, in particular: measures to implement the provisions of the Schengen Borders Code [17], streamlining checkpoints and visa liberalization have contributed to the growth of passenger and transport flows; There is a steady trend to increase the effectiveness of combating modern threats – arms smuggling, drug trafficking, illegal migration. Thus, according to joint estimates with the border services of neighboring EU countries in 2004 - 2009, there has been a gradual decline in the activity of illegal migration on the border of Ukraine with the European Union. This trend is strengthened by strengthening the protection of the common border with the EU, eastern and northern areas, cooperation with other law enforcement agencies to detect and stop organized criminal groups that smuggle people across the border, preventive measures to prevent potential migrants to Ukraine, strict implementation of readmission agreements, expulsion of foreign offenders outside Ukraine. Third, the development of approaches to improving border security continued at the highest state level in the framework of the Comprehensive Security Sector Review and the development of the draft Conceptual Framework for Law Enforcement Reform. The analysis of more than three years of work shows state support for the initiatives of the border agency, its approaches to the development of the border security system. Fourth, an adequate level of border security is supported by joint action on at least both sides of the border. Adherence to this principle is especially characteristic of the fourth stage. Examples include measures to establish joint controls at checkpoints, joint patrols at the Green Border and the Danube, the establishment of joint consultation points, the development of cooperation between operational bodies and information exchange, joint operations, including in the framework of the European Agencies, management of operational cooperation at the external borders of EU member states (FRONTEX). Fifth, the development of approaches to the development of the border security system (short, medium and long term) should take into account the experience of new EU member states in preparing for accession to the European Union and accession to the Schengen Agreement. In particular, this process involves the development of a joint strategy to build the future external border of the community - the implementation of which is regularly monitored by the evaluation mission. Not only border institutions are subject to this assessment, but also all government agencies related to border security. During the assessment, special attention is paid to the consolidation and clear delineation of tasks related to the protection of national interests at the border; fulfillment of international obligations in the field of border security; creation of simple but effective departmental and interdepartmental mechanisms of interaction. In some cases, the assessment mission's findings that the candidate country was not ready to protect the new external border became an obstacle to the decision to join the EU. In general, the policy of the European Union in the field of border security is quite flexible, promptly modernized in the light of existing and potential threats,

aimed at continuous development, the use of the latest technology and information technology. It provides for close cooperation at national level in the Member States and throughout the EU, in particular through FRONTEX, as well as with third countries on a bilateral and multilateral basis. In recent years, the EU has developed a number of concepts for action in the field of border security, which are mandatory both in the Community and in each Member State (including candidate countries). A number of concepts have already been implemented (reflected in the relevant regulations, instructions, recommendations, etc.), and others are under implementation. They concern, in particular, integrated border management; risk management systems, criminal analysis, technical surveillance; European patrol network; national focal points; information collection centers; information systems and technologies etc.

The main EU document in this area is the Instruction on the Integrated Border Management System (IPM). It must ensure a balance between effective border protection, prevention of modern threats and maintaining the openness of borders for legitimate cross-border activities and travelers. This Instruction identifies three levels of IPM implementation (development): 1. Interdepartmental cooperation within the national services responsible for border management tasks at the vertical and horizontal levels. 2. Interagency cooperation and coordination between different national services responsible for specific border management tasks at the border. 3. International cooperation, in particular, bilateral cooperation with neighboring countries and multilateral cooperation. The key areas of focus within these three levels are the legal and regulatory framework, the institutional system, procedures, human resources, education and training, information and communication exchange, infrastructure and equipment. The practice of European countries involves the development of a national strategic action plan in the field of border management with a number of measures at all three levels above. Given the perspective, the experience of European countries needs to be carefully studied, as the Ukrainian situation can be assessed as unprecedented. Unlike, for example, Poland, Slovakia, Hungary and Romania, which jointly guard the EU's new eastern land border of about 2,000 km, Ukraine's land border, which could become the EU's external border after Ukraine's accession, is 1.5 times larger. In addition, it is a new, unregulated border. Its construction is not yet complete, especially at checkpoints. It is also necessary to take into account the factors that affect and will have an impact on the state of border security. In particular, external factors include: the presence of 1,400 km of common border with the EU, the accession of Poland, Slovakia and Hungary to the Schengen Agreement and the future accession of Romania; measures for the development of international transport corridors passing through Ukraine; holding the European Football Championship in Ukraine and Poland in 2012; activity of European structures on monitoring (evaluation) of the effectiveness of protection of Ukrainian borders, in particular the Ukrainian-Moldovan one; the entry into force of a readmission agreement with the EU in the near future; incomplete legal registration of the border with Belarus and Russia, the central part of the border with Moldova, delimitation of exclusive (maritime) economic zones with Romania and Russia; unresolved Transnistrian conflict; projected activity of cross-border (transnational) criminal groups on human smuggling, trafficking in drugs and other contraband items, economic smuggling, etc. The internal factors include: unresolved (including legal) a number of issues in the field of migration management, anti-smuggling, etc.; lack of material resources for the arrangement of the border, construction of checkpoints across the border (including for small border traffic), renewal of the ship and boat composition of the Marine Guard, border aviation; unresolved issues regarding the allocation of land for the development of border infrastructure; a large set of tasks that need to be done in the framework of Ukraine's development as a maritime state; the need for significant reforms to achieve ambitious goals for Ukraine's integration into the European Union.

Conclusions. Taking into account these and other factors in security, migration, economic, environmental and other spheres, depending on specific conditions, the priorities of Ukraine's border policy should be differentiated, their hierarchy, range of subjects and objects and their functions, the role of adjacent territories within positive cross-border interaction. These are crucial state tasks that require theoretical elaboration, systematic research, and the search for ways to resolve the problems and contradictions that exist in this area, which we will consider in the future.

REFERENCES:

1. Sytnyk H. P. (2004). *Derzhavne upravlinnia u sferi zabezpechennia natsionalnoi bezpeky Ukrainy: teoriia i praktyka* [Public administration in the field of national security of Ukraine: theory and practice]. Extended abstract of candidate's thesis. Kyiv, p. 36. [in Ukrainian]
2. Law of Ukraine on the basics of national security of Ukraine № 964/IV. (2003, June 19). *Vidomosti Verkhovnoyi Rady Ukrayiny,* 39. [in Ukrainian]
3. Decree of the President of Ukraine on the National Security Strategy of Ukraine № 349/2020 (2003, September 14). [in Ukrainian]
4. Pyrozhenko V. A. (2020) *Metodolohiia operatsionalizatsii osnovnykh poniat natsionalnoi bezpeky: humanitarna skladova* [Methodology of operationalization of basic concepts of national security: humanitarian component]. *Ukrainskyi tsentr politychnoho menedzhmentu*. Retrieved from : http://www.politik.org.ua. [in Ukrainian]
5. *Protokol № 4 do Konventsii pro zakhyst prav i osnovnykh svobod liudyny* (2000) [Protocol 4 to the Convention for the Protection of Human Rights and Fundamental Freedoms]. *Zbirka dohovoriv Rady Yevropy*. Kyiv: Parlamentske vydavnytstvo, p. 52. [in Ukrainian]
6. Horbatenko V. P. (2000). *Politolohichnyi entsyklopedychnyi slovnyk* [Political science encyclopedic dictionary]. Kyiv : Heneza, 736 p. [in Ukrainian]
7. Bondarenko V. A., Vasilenko A. I. & Tepechin V. I. (2001). *Pogranologiya: metodologicheskie voprosyi* : monografiya [Borderology: methodological issues: monograph]. Moskva: MVI FPS Rossii, 198 p. [in Russian]
8. Shysholin P. A., Mykheienko M. M. (2002). *Prykordonna bezpeka Ukrainy: kontseptualni zasady* [Border security of Ukraine: conceptual principles]. *Naukovyi visnyk Derzhavnoi prykordonnoi sluzhby*, № 1, p. 23. [in Ukrainian]
9. *Stratehichnyi biuleten prykordonnoi bezpeky Ukrainy* [Strategic Bulletin of Border Security of Ukraine] (2008). Kyiv : Administratsiia Derzhprykordonsluzhby Ukrainy, p. 123. [in Ukrainian]
10. Law of Ukraine on the succession of Ukraine (September, 12 1991) № 1543-XII : *Vidomosti Verkhovnoi rady Ukrainy*, № 46. [in Ukrainian]
11. Decree of the President of Ukraine on the comprehensive program for the development of the state border of Ukraine (1993, December 16) № 596/1993. [in Ukrainian]
12. Decree of the President of Ukraine on measures to protect the state border of Ukraine with the Republic of Moldova (1992, March 17) № 158/1992. [in Ukrainian]
13. Decree of the President of Ukraine of program of actions aimed at maintaining the state border regime of Ukraine and the border regime, the development of Border Troops and customs authorities for the period up to 2005 (2000, November 16), № 1241. [in Ukrainian]
14. Law of Ukraine on the State Border Guard Service of Ukraine (2003, April 3) № 661 – IV. *Vidomosti Verkhovnoi rady Ukrainy*, № 27. [in Ukrainian]
15. Law of Ukraine on Amendments to Certain Legislative Acts of Ukraine in Connection with the Adoption of the Law of Ukraine "On the State Border Guard Service of Ukraine" (2003, April 3) № 662 - IV. *Vidomosti Verkhovnoi rady Ukrainy*, № 27. [in Ukrainian]
16. Resolution of the Cabinet of Ministers of Ukraine on approval of the State Targeted Law Enforcement Program "Arrangement and Reconstruction of the State Border of Ukraine" for the period up to 2015 (2007, June 13), № 831. [in Ukrainian]
17. Order of the European Parliament and the Council of the EU on the implementation of the Schengen Borders Code (2006, Martch 15), № 562/2006. [in Ukrainian]

д.т.н. Бабій Ю.О., к.військ.н. Поліщук В.В., Мартинюк В.П., Мартинюк О.В., Черноусов Д.О.

СТАНОВЛЕННЯ ПРИКОРДОННОЇ БЕЗПЕКИ ЯК СКЛАДОВОЇ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Аналіз останніх наукових публікацій та спеціальної літератури щодо проблематики в галузі національної безпеки показує, що на сьогодні усталені підходи до методологічних аспектів дослідження у цій сфері. Актуальною залишається проблема розмежування окремих складових національної безпеки, зокрема прикордонної. Разом з тим її ключові поняття чітко не окреслені, що ускладнює визначення предмету дослідження, проведення точного аналізу та підготовку відповідних рекомендацій стосовно її реалізації. Як наслідок, питання прикордонної безпеки на разі глибоко не вивченні, зокрема не достатньо враховуються геополітичні реалії, зовнішні та

внутрішні фактори, які впливають на її стан. Підтвердженням цьому може слугувати низка наукових публікацій, що демонструють спрощені погляди на державний кордон. Його сприймають просто як фізичну лінію розмежування території держав, роблять висновки щодо „розмиття" кордонів між європейськими державами і піддають сумніву необхідність їх охорони в епоху глобалізації. Водночас компетенція та завдання прикордонної інституції обмежуються лише перевіркою документів у подорожуючих через кордон в пунктах пропуску та контролі його ділянки поза ними.

Беручи до уваги основні тенденції і наслідки глибинних трансформацій геополітичного та геоекономічного простору, на сьогодні виникла потреба у проведенні ґрунтовних досліджень у сфері забезпечення прикордонної безпеки України, як складової національної безпеки, а також визначення чіткого місця і ролі суб'єктів її гарантування в ході реалізації зазначеної функції, особливо з появою нових видів загроз, зокрема: тимчасова окупація Російською Федерацією частини території України - Автономної Республіки Крим і міста Севастополя, розпалювання Росією збройного конфлікту в східних регіонах України, що обумовлюють не лише дестабілізацію політичної та економічної ситуації в Україні, розвиток тероризму та загрозу його поширення територією нашої держави, але й спрямованні на руйнування системи світової та регіональної безпеки і принципів міжнародного права.

Необхідним вважаємо – обґрунтування структури та змісту моделі прикордонної безпеки, як основи подальшого розвитку Державної прикордонної служби України, що є основою формування та реалізації сучасної прикордонної політики європейського зразка, зокрема приведення прикордонного законодавства України до норм європейського права.

Ключові слова: ризик, загроза, національна безпека, прикордонна безпека, модель прикордонної безпеки.

UDC 623.618.5

D.Sci.Tech. **Barabash O.V.** (NDU)
PhD **Open'ko P.V. (**NDU)
PhD **Kireienko V.V. (**NDU**)**

DOI: https://doi.org/10.17721/2519-481X/2021/73-02

PROSPECTS OF DEVELOPMENT OF ANTIAIRCRAFT MISSILE TROOPS TECHNICAL SUPPORT SYSTEM

In article considers the state and prospects of development of logistics to anti-aircraft missile forces, identifies areas for further development in the application of information technology for intelligent life cycle of military products. Theoretical bases of material and technical maintenance from the point of view to models of their life cycle are opened. Modern approaches to logistics are analyzed, considerable attention is paid to information technologies, tools that support this approach, and in particular process management according to the technical condition. It is noted that the main area of improvement should be the use of intelligent management of operation of technical condition and restoration of military products, which will allow during the life cycle of the sample on armaments and military equipment using projected indicators of its technical condition, determine the frequency and scope of maintenance, repair and providing them with military and technical property. There is an objective need to equip troops with an automated control system for dynamic analysis and effective planning of the life cycle of equipment. The advantages of forming a mobility park on the basis of the modular principle are highlighted. It is shown that during the operation of intelligent systems, solving the problem of providing military products, there are a large number of limitations that must be taken into account during its development. Recommendations for improving the logistics of armaments and military equipment, developing a methodology to ensure a higher quality of the life cycle of military products and effective life cycle management, which will achieve maximum performance of these types of military products. Theoretical bases of material and technical maintenance from the point of view of models of their life cycle are opened.

Keywords*: *technical support system, air defense weapons, management of operation, technical state and recovery of a military product, CALS / IPV technology.

Introduction. Modern information and intellectual technologies allow to change approaches to the organization of preparation, use and comprehensive support of combat, to increase efficiency and substantiation of the made decisions, in particular concerning support set level of serviceability and technical readiness of the surface-to-air missile systems (SAM-systems) during operation [1].

Modern samples of antiaircraft missile armament (AMA) are complex technical systems with hierarchically branched structure. The AMA samples combine components of different physical execution and appointment.

Technical support is organized for the maintenance of combat readiness of Antiaircraft missile troops (AMT) by support them of armament and military equipment (AME), missiles, ammunition, military and technical facilities, their maintenance in constant readiness for employment, recovery (repair) of AME in case of damages (breakages) and to return them to an operation.

The main actions of technical support are: provision of troops by AME, missiles, ammunition, military and technical facilities; preparation of AME for combat use; organization of AME operation; carrying out maintenance and replacement of the AME blocks, units, nodes which completed the specified life resource , repair of the damaged (faulty) AMA samples and return them to an operation; control of technical support; the greatest possible attraction of local industrial base for carrying out of AME repair [2].

Formation of the problem. The existing system of technical support which remained from the Soviet Union envisages use of the regulated strategy of maintenance and repair (M&R) of AMA samples and provides carrying out of all types of planned repairs in a network of repair plants of the USSR Ministry of Defense. Such system does not correspond the existing opportunities of the plants of defense industry complex and state of the Ukraine economy. The made stores, spare part kit, tools and accessories (SPTA) do not provide carrying out a complex of actions concerning maintenance (or recovery) an operating (serviceable) condition of AMA samples.

Analysis of previous studies. Now operation of samples of AME is carried out on the basis of the decision on continuation of the assigned reliability indexes. The decision is accepted on the basis of an estimation of the current technical state of its radio-electronic means (REM) [3]. The perspective direction of maintenance and recovery of an operable (serviceable) condition of AMA is introduction of adaptive strategy of maintenance and repair of AMA samples. For example, the strategy of maintenance and repair according to state [4,5] which provides the appointed reliability indexes the REM of SAM-complexes and cost decrease of their operation.

Introduction of strategy of M&R for a state in process of operation of AME demands performance of procedures of technical diagnosing by means of built in (or external) the automated test systems (control of technical state). The existing automated test systems (control of technical state) are ineffective and do not meet the requirements of present time. The assessment of indicators of reliability of products by results of operational supervision is significantly complicated because of impossibility of the accounting of conditions and modes of operation of concrete accessories in structure REM of SAM-complexes, lack of statistics of the moments of transitions of SAM-complexes and their REM in a limit state demands from experts of technical ensuring use of rather difficult mathematical apparatus.

Main part. The efficiency of realization of adaptive M&R strategy, substantially, depends on existence built in (or external) the automated diagnostic systems (monitor of technical state) of products, fitness of monitor objects to diagnosing (monitor of technical state), a technique of diagnosing (monitor of technical state), possibilities of timely detection of the transition moments of REM of AMA samples in a limit state.

In the leading countries of the world adaptive M&R strategy are introduced in the form of the relevant systems of the life cycle (LC) support of complex technical systems.

The system of Continuous Acquisition and Life cycle Support (CALS) covers all LC of a product, from development of tactical and technical requirements of a perspective AMA samples to its write-off and utilization. Development of perspective AMA samples is carried out according to the CALS standards. The M&R system of AMA samples, which a long time are in operation, is brought into step with the CALS standards. The subsystem of the integrated logistic support (ILS) is one of components of the CALS system. In the similar way the system of intellectual support of life cycle of the knowledge-intensive products (ISLC) in the Russian Federation provides all LC stages of military products [6].

Now ideas of CALS / ISLC are documentary realized by IPV in the form of the ISO standards, national (state) standards and normative documents of branches and the separate enterprises [7] on the basis of which the concept of increase of operational reliability of difficult technical systems which allows to consider in real time a lag effect of information processes and intensity of use of the appointed operational resource is formulated and to provide information support of difficult industrial products and samples of AME [8-10].

Basis of systems of intellectual support of LC of the knowledge-intensive products are databases about products where statistical data, arrived from military units with AMA sample, is saved. Results of processing this statistical data and developments of recommendations of further operation of AMA sample and other data arrays about a product [11] are kept in these databases.

In work the option of structure of technical support system of AME of the Air Force of Ukraine is offered. The structure provides control of operation, technical state and recovery of military products in a common information space.

Basis of information support system is the AME database of Ukraine (AME the Air Force of Ukraine) which is created at a development stage and scientific and technical maintenance of the corresponding AMA sample. The database is stored and refined during production, operation, combat use, write-off, utilization. It comprises all technical information about a military product and its components, with obligatory use of the database of the Logistic of the Armed Force of Ukraine concerning existence and the movement of stores. Correctly organized database allow to includes new data which come during the operation of military products, to accumulate and process big data arrays, to calculate necessary reliability indexes of products. At the same time for AMA samples that

already for a long time are in operation, it is expedient to build databases by creation of electronic operation and maintenance documentation with use of electronic copies of paper operation and maintenance documentation.

Information communication between the AME databases of Ukraine with all subscribers is provided by the specialized network created with application of elements of an electronic network of a unified automated control system of Armed Force of Ukraine.

The Control Center of operation, technical state and recovery of military products (analog of the center of logistic support of life cycle of complex technical products) is created in the Logistic of the Air Force Command. The main tasks of the Control Center are: collecting and the analysis of technical data on a state, service conditions and resource expenses of AMA samples, types and causes of failures, level of readiness of attending personnel; elaboration of the nomenclature of military and technical facilities and the set of spare parts, tools and accessories which is contained in storehouses of military units of AMT; determination of work amounts, use of repair bodies and use of military and technical facilities during intermediate and capital repairs of AMA samples (as necessary), big interval maintenance of AMA samples, maintenance (scheduled works / preventive maintenance) of anti-aircraft guided missiles, monitor and recovery works on AMA samples which are subject of transfer to operation on technical state, control of a limit condition of AMA samples which are operated on technical state; support applications for repair (replacement) of knots, blocks, subblocks, units with the plant facilities, repair bodies, support centers of the Logistic of Ukraine, storehouses, bases and arsenals of Arms of Ukraine.

Devices for monitor and diagnostic of technical state of a military product are one of basic elements of perspective technical support system of AME of the Air Force of Ukraine. Elements of these means as a part of the automated test system have to be constantly in AMA samples and provide timely receiving, processing and transfer of data about the product technical state for formation of control decisions with use of the AME databases of Ukraine and support system of decision-making (SSDM) of the person which makes the decision [12].

In the offered SSDM the estimation of a military products state is carried out by the following indexes: total number of AME and completeness of military unit taking into account regular requirements and the appointed readiness degrees, including stores of the center; completeness of military storehouses and storehouses of the center by missiles, ammunition, military and technical facilities; technical state of AME park of different types (on serviceability, a resource left and an obsolescence); the predicted indexes of a state of AME park for a certain period (on serviceability, a resource left and an obsolescence); degrees of compliance of the existing AMA samples (complexes, systems) to foreign analogs; degrees of compliance of potential efficiency of the existing AMA samples to modern and perspective requirements to the task performance levels [13,14].

In the offered system of technical support of AME of Ukraine the M&R strategy for a state, in particular, in the conditions of incomplete basic data about military products reliability (about reliability of an AMA sample, about statistics of random processes of its parameters changes, about accumulation of faults, etc.) is used. At the same time the control acts on a military product which is in operation is formed taking into account additional information on technical state of a product which comes during the monitor and diagnostic of the corresponding parameters at operation.

Technical realization of the offered structure of technical support of AME of Ukraine requires the solution of the following tasks:

the choice of information characteristics of military products which will allow to provide formation of basic data about objects of control with the set reliability and accuracy;

development of requirements to structure and program information support of control devices and diagnostics of technical state of military products of the test system;

justification and the choice of a method of creation of the database and a method of data processing of military products during formation of the AME Armed Force of Ukraine only database of Ukraine;

justification and the choice of a method (methods) of forecasting of indicators of technical state of military products, including in the conditions of incomplete basic data about reliability of objects

of control;

development of algorithm of the solution of a problem of management of operation, technical state and recovery of military products which will provide essential decrease in temporary, labor, material and cost expenses on maintenance of operating state and the set level of their reliability;

improvement of system of technical support AMT Air Force Armed Force of Ukraine to the level which provides management of operation, technical state and recovery of military products by introduction of CALS / IPV of all stages of LC of objects of control.

Conclusions. Thus, as a result of the analysis of the existing condition of system of technical support AMT and systems of support of life cycle of difficult technical products realized in the leading countries of the world the general structure of perspective system of technical support AMT is offered. Requirements to the database of system, an order of interaction of components of system and SSDM and problematic issues which solution will provide a possibility of realization of the offered structure of technical support antiaircraft rocket troops are formulated. Existence of advanced system of technical support AMT Air Force Armed Force of Ukraine raises potential opportunities of AME park and provides maintenance of operating state and the set level of reliability of military products during operation.

The results of the solution of the given tasks received in Control center of operation, technical state and recovery of military products with use of the listed basic data are intended for use in Command of Air Force during justification of sets of AME necessary for the solution of settlement fighting tasks and sets of utilities which promote their performance.

REFERENCES:

1. Kryzhnyi A.V., Openko P.V. Prediction of the advancement of the fleet of antiaircraft missile complexes (systems) per hour of operation for the technical camp // Nauka i oborona. – K., 2012. – № 1. – P. 50–54.

2. Toropchyn A. M., Romanenko I. O., Danyk Yu. H., Pashchenko R. E. et al. Handbook of Air Defense. Kharkiv, Ukrainy, 2003. – 366 p.

3. Kryzhnyi, A.V., Openko P.V. Prospects for the application of information technology in the study of the reliability of complex technical systems. Povysheniye kachestva, nadezhnosti i dolgovechnosti tekhnicheskikh sistem i tekhnologicheskikh protsessov: materialy XII Mizhnarodnoyi naukovo-tekhnichnoyi konferentsiyi. – Khmel′nytskyy 2014. – № 5 P. 62–64.

4. Lanetskyi B.N., Lukianchuk V.V. Adaptive management of the technical condition and reliability of complex technical systems under resource constraints. Systemy ozbroyennya i viys′kova tekhnika, Kharkiv 2011. – №2(26).– P.149-151.

5. Hryb D.A., Lanetskyi B.N., Lukianchuk V.V. Improving methods of technical operation and repair as a basis for maintaining the combat readiness of anti-aircraft missile weapons in modern conditions // Nauka i oborona. – K., 2012. – № 3. P. 55-63.

6. Solomentsev Y.M., Mytrofanov V.H., Pavlov V.V., Rybakov A.V. Information - computing systems in mechanical engineering, CALS – technologies. Moscow. Nauka. 2003. P.354.

7. Demidov, V.A. “Sistemnaja metodologija planirovanija razvitija, predproektnyh issledovanij i vneshnego proektirovanija vooruzhenija i voennoj tehniki” [System methodology of development planning, pre-project research and external design of weapons and military equipment], 2011 Stilos, Kyiv, P. 464.

8. Musiienko A.P. Diahnostychna model bezdrotovoi sensornoi merezhi na osnovi vzaiemnykh perevirok elementiv merezhi / I.V. Pampukha, O.V. Barabash, A.P. Musiienko, M.O. Koval // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. – K.: VIKNU, 2017. – Vyp. 57. – P. 160 – 168.

9. Kireienko V.V., Barabash O.V., Salanda I.P (2021) Methods and algorithms of ensuring of functional persistence of subsystem of information exchange in the system of airspace control Natural and Technical Sciences, IX(31), pp. 1776-1779.

10. Barabash O.V., Musienko A.P., Sobchuk V.V., Lukova-Chuiko N.V., Svynchuk O.V. (2021) Distribution of Values of Cantor Type Fractal Functions with Specified Restrictions. Chapter in Book “Contemporary Approaches and Methods in Fundamental Mathematics and Mechanics”. Editors VictorA.Sadovnichiy, Michael Z. Zgurovsky. Publisher Name: Springer, Cham, Switzerland AG pp. 433 – 455.

11.Barabash O., Laptiev O., Tkachev V., Maystrov O., Krasikov O., Polovinkin I. (2020) The Indirect

method of obtaining Estimates of the Parameters of Radio Signals of covert means of obtaining Information. International Journal of Emerging Trends in Engineering Research (IJETER). Volume 8. No. 8, pp. 4133 – 4139.

12.Barabash O., Laptiev O., Kovtun O., Leshchenko O., Dukhnovska K. and Biehun A. (2020) The Method dynavic TF-IDF. International Journal of Emerging Trends in Engineering Research (IJETER). Vol.8, No. 9, pp. 5712 – 5718.

13.J. Boiko, I. Pyatin, O. Eromenko, O. Barabash, (2020). Methodology for Assessing Synchronization Conditions in Telecommunication Devices. Advances in Science, Technology and Engineering Systems Journal (ASTESJ), 2020, Vol. 5, No 2. ISSN: 2415-6698. pp. 320 – 327.

14.Berkman L., Barabash O., Tkachenko O., Musienko A., Laptiev O. and Salanda I. (2020) The Intelligent Control System for infocommunication networks. International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 8, No. 5. pp. 1920 – 1925.

д.т.н., проф. Барабаш О.В., к.т.н., ст. досл. Опенько П.В., к.військ.н. Кіреєнко В.В.

ПЕРСПЕКТИВИ РОЗВИТКУ СИСТЕМИ ТЕХНІЧНОГО ЗАБЕЗПЕЧЕННЯ ЗЕНІТНИХ РАКЕТНИХ ВІЙСЬК

У статті розглянуто стан та перспективи розвитку матеРріально-технічного забезпечення зенітних ракетних військ, визначено напрями подальшого розвитку щодо застосування інформаційних технологій інтелектуального забезпечення життєвого циклу військової Зазначається, що основним напрямком удосконалення має бути застосування інтелектуального забезпечення управління експлуатацією за технічним станом та відновленням військової продукції, що дозволить протягом життєвого циклу зразка озброєння та військової техніки з використанням прогнозованих показників його технічний стан, визначати періодичність і обсяги робіт з технічного обслуговування, ремонту та забезпечення їх військово-технічним майном. Наведена об'єктивна потреба щодо оснащення військ автоматизованою системою управління для динамічного аналізу і ефективного планування життєвого циклу техніки. Висвітлені переваги щодо формування парку рухомості на базі модульного принципу. Показано, що під час функціонування інтелектуальних систем, розв'язанні завдань забезпечення військової продукції, діє велика кількість обмежень, які необхідно враховувати під час її розробки. Запропоновані рекомендації щодо удосконалення матеріально-технічного забезпечення озброєння та військової техніки, розробки методології забезпечення більш високої якості життєвого циклу військової продукції та ефективного управління життєвим циклом, яке забезпечить досягнення максимальних показників експлуатаційної ефективності зазначених типів військової продукції. Розкрито теоретичні основи матеріально-технічного забезпечення з точки зору моделей їх життєвого циклу.

Ключові слова: система технічного забезпечення, озброєння протиповітряної оборони, керування експлуатацією, технічний стан та відновлення військового виробу, технологія CALS/IPV.

UDC 004.021

D.Sci. Tech. **Zaslavskyi V.A.** (TSNUK)
Pushkarenko Yu.V. (TSNUK)

DOI: https://doi.org/10.17721/2519-481X/2021/73-03

PRINCIPAL CURVE TRAJECTORY ANALYSIS

Increasing availability of probe data sources gives an opportunity to use the data in automatic map creation process, refine the shape of existing maps as well as potential for generating source of truth (i.e., ground truth data) in military as well as for civil aspects. That is needed for confirming the quality of existing maps as well as compilation them from different sources to achieve the comprehensive result of creating very high-definition maps. The main reason is to compile the resulting map not only from satellite imageries but also using another source of compilation or confirmation. We don't do deep dive in map compilation process itself but concentrating on map-matching problematic from perspective of GPS Probes trajectories which is very noisy by nature. The present paper proposes an analyzing of methods based on principal curve trajectory collected from raw GPS positions. Probes positions itself from phone inside a car are noisy, they don't necessarily match the actual position of the car for a given moment. Assuming the car drives on a street according to regulations, the raw position can be matched to street locations by means of a map matching algorithm. Using a series greatly improves the stability and plausibility of the map matched positions, especially when probes samples are noisy or sparse and different roads are close together (e.g. crossings, bridges, tunnels, slip roads) it could be useful for creating bi-directional road geometry from sparse probes. The resulting road segments in the road network graph enable conflation with existing map data to identify map changes including base maps.

Trajectory analysis and related algorithms have recently attracted substantial attention, thanks to technological advances in navigation and mapping systems. Nevertheless, some fundamental concepts are still lacking a thorough study. The identification of a middle (representative) trajectory in a bundle of trajectories is one of them. Without conscious reasoning, a middle trajectory is a trajectory that lies in the middle of a collection of trajectories. However, this definition is far from being comprehensive.

This research work is focused on the concept of finding a principal curve trajectory among a bundle of trajectories with specific source and destination points. The main idea is to use the timing information associated with trajectories to improve existing methods for trajectory analysis. We investigate the concept of a principal curve related to timing information, we give a review of algorithms for all existing methods, analyze the worst-case running time, and show that under certain assumptions methods such as timing can be implemented efficiently.

Key words: Map-Matching, Geo-Spatial Analysis, Computational Geometry, Cluster Analysis, Probe Data, Road Geometry Extraction, Road Maps, Spatial Data Mining.

Introduction. A formal definition of trajectory is specified in [1] as a time-stamped path taken by a moving entity, represented by a sequence of n tuples of points and time stamps (p_0, t_0), $(p_1, t_1), \dots, (p_{n-1}, t_{n-1})$. Points have spatial and temporal components. The spatial component typically represents a two or three dimensional space. Here, we assume that the space is two dimensional. A bundle of m distinct trajectories $T_0, \dots, T_{m-1}$ with the same start and ending points, therefore results in an input size of $\theta(nm)$.

In an ideal situation, the time stamps of all trajectories in the bundle are exactly the same, but this is usually not the case. Generally, trajectories are collected with different or irregular sampling rates, at different times, and data can be missing as well. In between time stamps, we have no information about the actual movement path of the entity. The standard assumption can be that the entity moves with constant velocity from a time-stamped point to the next time-stamped point in a straight line. This assumption leads to an approximation of the actual data, which becomes more inaccurate when sampled at longer intervals. As a result, the path of a trajectory is considered as a polygonal curve with n edges that can self-intersect, and can have repeated vertices at the same location if the entity stands still. The number of points defining a trajectory is usually much larger than the number of trajectories in a bundle $n \gg m$.

Analysis of previous studies. Various methods for trajectory analysis have been developed in different fields of science including computational geometry and data mining. Trajectory data sets can be analyzed in a variety of ways. They are usually clustered into a collection of subsets that have a high similarity regarding (a) certain property(-ies), such as location. Nevertheless, processing large amounts of trajectory data is a challenge. Trajectory data compression can be regarded as a solution to address this problem, particularly for the trajectories with huge sampled data points to improve the efficiency of computations. This compression can be carried out for individual trajectories, but in most applications, the data contains similar bundle of trajectories in terms of space and/or time, and as such, an alternative method would be to compress a trajectory bundle to represent similar trajectories with a single representative trajectory. We call this representative trajectory a middle trajectory without loss of generality. Furthermore, using a single representative trajectory enables processing data in a simple, robust and more predictive way. As an example, a representative trajectory for an specific route can be used to predict where a vehicle will be at a certain time. Alternative applications of middle trajectories include clustering and visualizations. As an example, a middle trajectory can act as the medoid in $k - medoid$ clustering. In the context of visualization, instead of showing a large collection of trajectories, one may identify subsets of similar ones, and replace them by a middle trajectory whose width is determined by the size of the subset.

Formation of the problem. Given a set of m trajectories $T = \{T_0, \dots, T_{m-1}\}$ with the same source and destination points s and d, we want to find a representative trajectory T_r that minimizes a defined distance function to all trajectories $T_i, 0 \leqslant \mathrm{i} < \mathrm{m}$ in the set and T_r contains points from input trajectories. In case not specified otherwise, the distance function is defined as the Euclidean distance between trajectories.

A representative trajectory has to be in the middle of all trajectories in the bundle. However, we first have to define what is considered middle. There are two main types of interpretations of what a middle trajectory is for a set of input trajectories: *median* and *mean* trajectory [2]. They can produce a trajectory that is in the middle, regarding space or time, or both. There could be different interpretations for the definitions of mean and median here compared to the standard arithmetic definitions of these parameters, however the general intuition remains the same. The main difference between a mean and a median trajectory is that the latter uses only points of the input trajectories. An alternative definition for a median trajectory is to use only the edges of the trajectories present in the input set, or parts of the edges, and switch at intersections [1]. Both mean and median trajectories have their own applications. Mean trajectory which is based on the spatial component of the input trajectories looks more accurate compared to a trajectory that is restricted to one of the inputs. Nevertheless, there can be a strong reason why one prefers a median trajectory over the mean one. A typical example would be for moving objects that have to avoid obstacles. The same property should also hold for the middle trajectory. If no information about the obstacles is known in advance, then the only way to ensure that the representative trajectory crosses no obstacle is to use parts of the original input trajectories. On the other hand, if such information is known, then it may also be possible to use this information and make the mean path go around the obstacles. Fig. 1 shows examples of mean and median trajectories. The median one follows the existing trajectories and thus avoids potential obstacles if any is defined. The mean trajectory does not necessarily follow the input trajectories and may pass through obstacles. One major disadvantage for mean trajectory is its sensitivity to outliers. Data sets of input trajectories containing substantially diverging measurements will influence a calculated mean trajectory. Fig. 2 shows an example of this phenomenon.

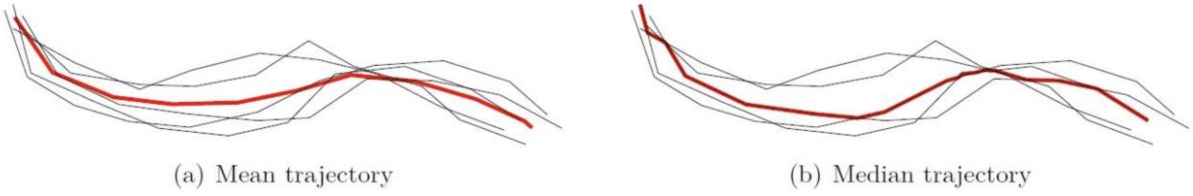


Figure 1 - Examples of (a) Mean trajectory (b) Median trajectory

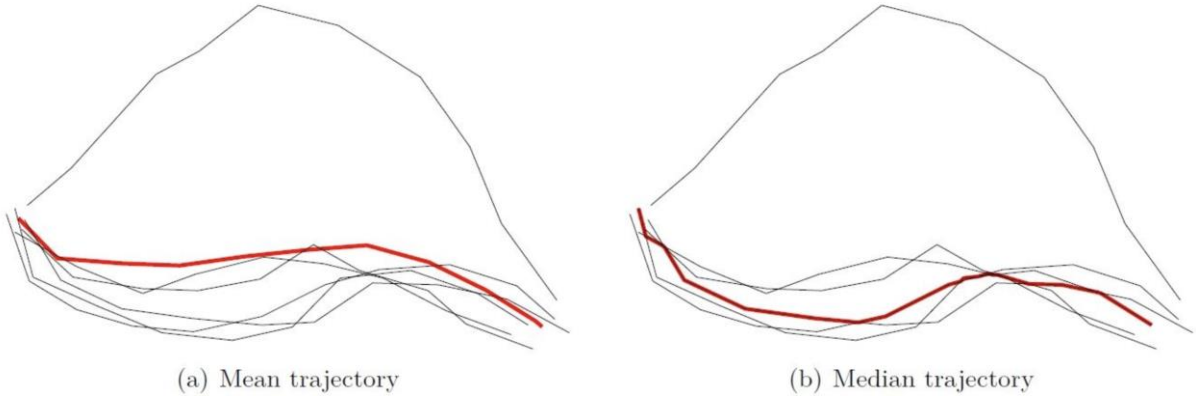


Figure 2 - Effects of outliers on (a) Mean trajectory (b) Median trajectory

Trajectory data usually include a temporal component in addition to an spatial component, however in most cases the temporal component plays no role in computation of the middle trajectory. The reason is that it would be difficult to utilize this information in an efficient way due to inconsistencies between data points that is mostly present in a trajectory bundle. As an example, suppose the trajectories are from different vehicles on a specific route. The data could be collected on different days and times, as a result, we cannot directly use the temporal component. Even if vehicles had exactly the same starting and ending locations and take more or less the same path, we cannot simply align the starting times of the travels, because one vehicle may have been held up due to traffic conditions which distorts the time correspondence that we set up at the starting point. Thus, in many situations, a middle trajectory is solely processed based on the spatial component and considers the path (shape) of the trajectories.

Main Part. So far several properties have been proposed for a representative trajectory in literature. Nevertheless, most of these properties are not well defined, but rather intuitively assumed to hold for a representative trajectory. Here is a list of these properties:

- continuous: a contiguous curve from a source to a destination without interruptions
- central: locally central within the bundle regarding the positions of the input trajectories
- comparable length: its length should be more or less the same as the input trajectories
- comparable angular change: its total angular change should be more or less the same as input trajectories
- comparable vertices: its total number of vertices should be more or less the same as input trajectories
- maintain edge direction: for every edge of input trajectories included, the direction should be retained accordingly
- follow the majority: should visit regions only if most of the input trajectories do
- consist of input trajectories: should be composed of points of input trajectories

It addition it is desirable that a representative trajectory be robust against outliers and special cases and there will be efficient algorithms for its computation.

Several approaches have been used to identify a representative trajectory for a set of clustered trajectories. Buchin et al. [1] present two different methods to construct a median trajectory for a set of input trajectories. The first method is based on simple definition of mean level in an arrangement of lines while the second method uses the concept of homotopy with respect to sufficiently large faces in the arrangement formed by input trajectories. Both methods produce a trajectory that consists of pieces of the input and ignore the temporal component of trajectories. The simple median trajectory starts on the middle trajectory and always switches to another trajectory at an intersection point. If all the m input trajectories are ordered based on the starting point s (in the outer face of the arrangement of curves) with the first and last trajectories adjacent to the outer face, then the middle trajectory starts

from the $\left[\frac{m}{2}\right]$ -nd edge in the order. It is shown that under certain conditions, such a median is always in the middle. They prove that the median trajectory satisfies the property that for any point p must cross to reach the unbounded face (including the one(s) on which p lies) is $\left[\frac{m+1}{2}\right]$. In presence of outlier trajectories, they shall be excluded from the total number of trajectories. The simple median trajectory has a upper bound time complexity of $O((nm)^2)$ because of the total $n.m$ line segments that should be processed, where m is the number of input trajectories and n is the maximum number of data points for any trajectory. For practical situations, the time complexity is improved to $O((nm + k)a(nm)\log(nm))$, where a is the inverse Ackerman function and k is a number of edges in the output trajectory.

The main problem with this approach is that it will most probably fail to find a representative trajectory when the trajectories are self-intersecting. An example is shown in Fig. 3. All the three input trajectories go through a loop but the median one does not follow a similar path. The problem happens because at some intersection, an edge is selected which is not a part of the direct continuation of the path, rather part of a trajectory on the way proceeding the loop. A similar problem can even emerge when the trajectories are not self-intersecting. As shown in Fig. 4, the usual path of the majority of the input trajectories is not followed accordingly. In this example, two of the input trajectories make a kinda detour, while a third one takes a straight path towards the destination. The median trajectory follows the unwanted straight one.

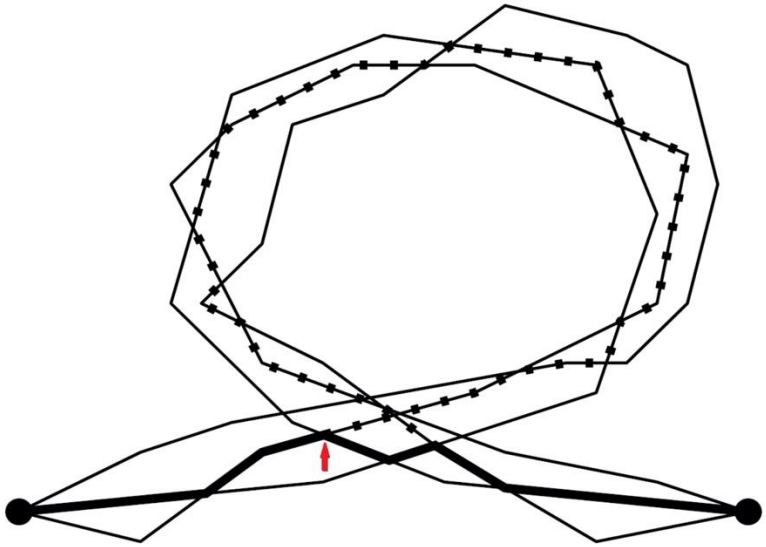


Figure 3 - Self-intersecting trajectories can perform undesirable for the computation of the median trajectory

Unlike the simple median trajectory, the homotopic median does not necessarily switch at every intersection points. When trajectories self-intersect, a point p is placed in the face(s) around which it loops. Switching trajectories is only done if the median calculated up to the switching point is of the right homotopy type, determined by the signature of the (sub)trajectory. This signature is the intersection of the trajectory with the vertical line through each point p and side of the intersection (i.e. above or below

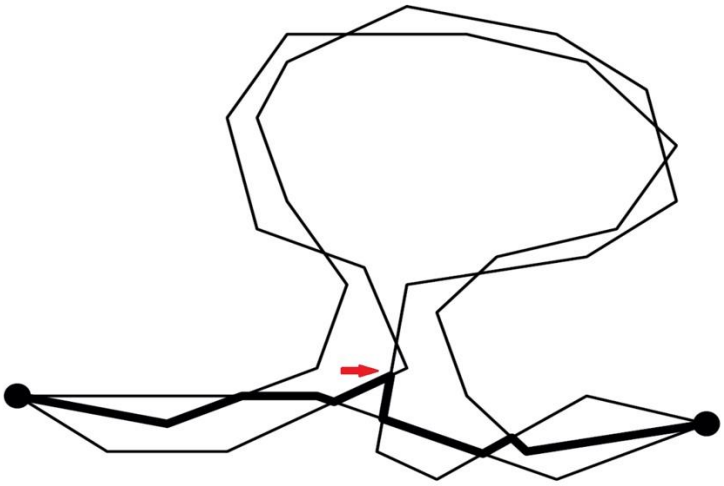


Figure 4 - The median trajectory can miss part of the path of the input trajectories with no self-intersections

Unlike the simple median trajectory, the homotopic median does not necessarily switch at every intersection points. When trajectories self-intersect, a point p s placed in the face(s) around which it loops. Switching trajectories is only done if the median calculated up to the switching point is of the right homotopy type, determined by the signature of the (sub)trajectory. This signature is the intersection of the trajectory with the vertical line through each point p and side of the intersection (i.e. above or below p with the values p^+ and p^-, respectively). Fig. 5 shows two examples of input trajectories and their corresponding homotopic types.

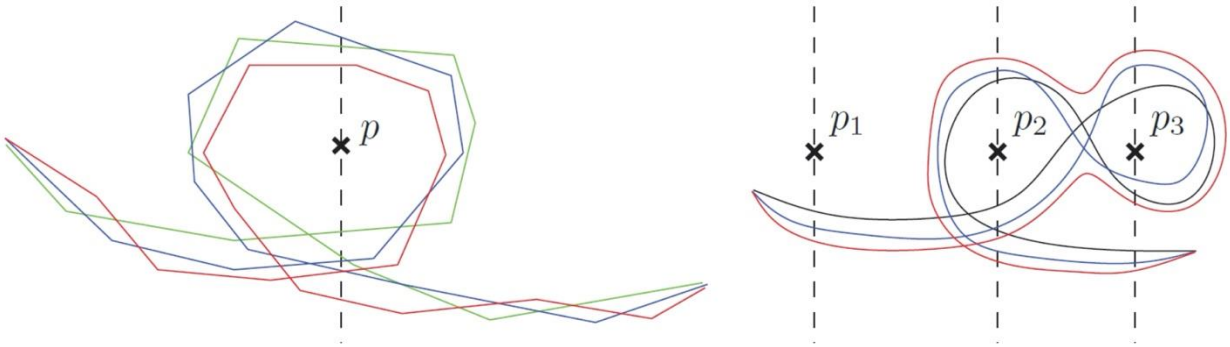


Figure 5 - (a) three input trajectories that loop around a face of the subdivision in which p is placed. All three trajectories have the signature $p^- p^+ p^-$. (b) two trajectories that are homotopic, with signature $p_1^- \; p_2^- \; p_3^+ \; p_3^- \; p_2^+ \; p_2^- \; p_3^-$

An example of seven input trajectories is shown in Fig. 6 (a). Most of the trajectories follow the path numbered from 1 to 14. Five trajectories skip point 7 and six skip point 11. One trajectory skips points 5–8. One expects the representative trajectory to follow what most input trajectories do, and consecutively go from 1 towards 2, 3, 4, 5, 6 = 8, 9, 10 = 12, 13, and 14. The simple and homotopic median trajectories are marked in Fig. 6(b). As seen in the figure, the homotopic median (red) appears to give a more appropriate middle trajectory compared to the simple median one (green).

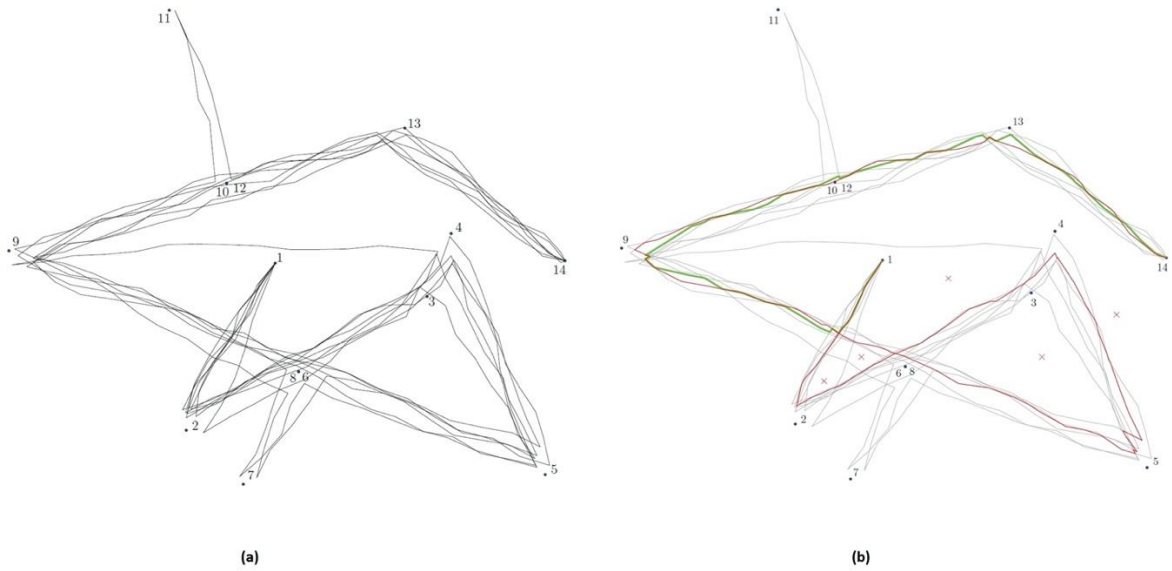


Figure 6 - **(a)** A set of input trajectories, generally following the numbered points excluding 7 and 11, **(b)** The simple median trajectory is marked with green and the homotopic median is marked with red

Although homotopic median appears to give intuitive median trajectories in many situations, there are two clear cases where it fails to identify a suitable representative trajectory. In [3], van Kreveld and Wiratma give examples where the homotopic median trajectory fails. In one case, if all trajectories make a detour that is back-and-forth over the same path, then no relatively large face is present to place a point in. Such a detour is incorrectly ignored by the homotopic approach. Fig. 7 illustrates this situation. Another case is when all trajectories are of a different homotopy type (e.g., when no large subset of homotopically equivalent trajectories exists), which results in one of the input trajectories being the median. Using a single input trajectory as the median might result in the computed trajectory to include regions that are visited only by a single input trajectory. This situation is illustrated in Fig. 8.

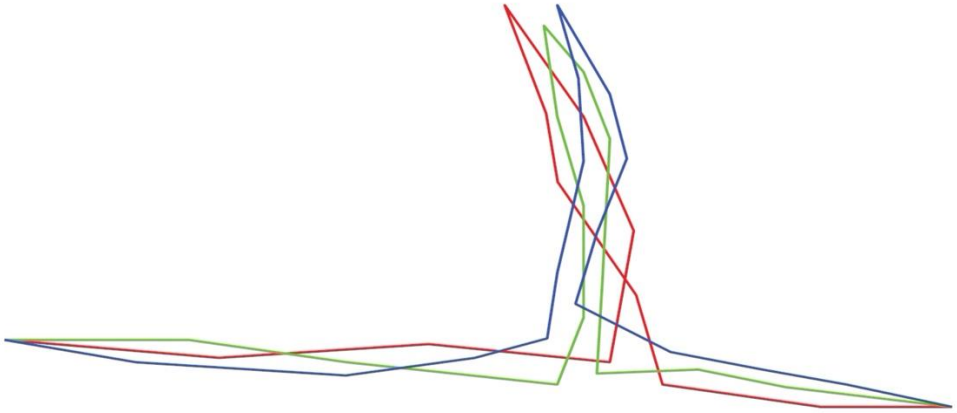


Figure 7 - The homotopic median approach will fail to make the detour because there is no large enough face to place a point

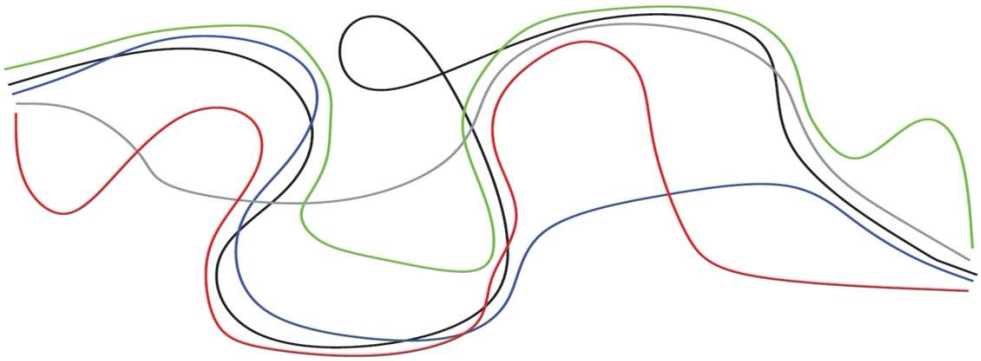


Figure – 8 Input trajectories with different homotopic types make the identification of a representative trajectory fail. There is no typical set of homotopically equivalent trajectories, thus one of the inputs would be identified as a median trajectory

The time complexity of computing homotopic median trajectory is: $O((nm)^{2+e}), e > 0$.

In [3], van Kreveld and Wiratma present a completely different method that computes median trajectories as an alternative to overcome the aforementioned drawbacks for simple and homotopic trajectories. This method is based on the idea that not all segments (edges) in T are suitable to be a part of the median trajectory T_r in case they are not close to the majority of trajectories in T. This implicitly implies that the edges which lie somehow in the middle of a bundle of trajectories are more eligible to be included in the median trajectory. As seen in Fig. 9, based on the majority definition, the dark green edges are most likely to be selected as part of the median trajectory, while red eges having the least chance.

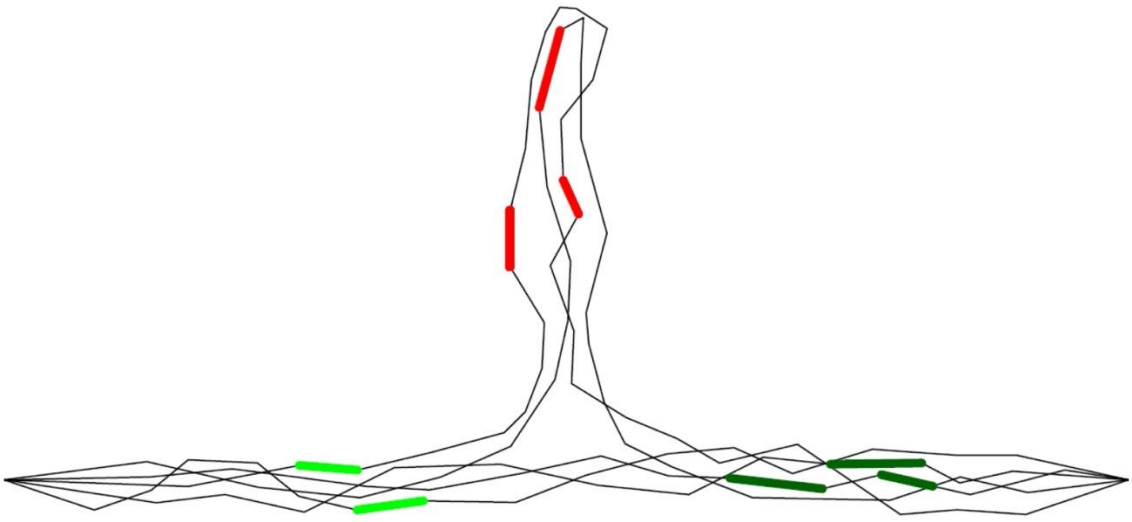


Figure 9 - Red edges are not good candidates to be part of a median trajectory; dark green ones are suitable due to their positions (close to the majority and somehow in the middle); being on the outside border of the bundle, the light green ones are less suitable compared to the dark green segments

In the proposed algorithm, aka *buffer median* algorithm [4], an edge e is called *useful* if a buffer of size δ around intersects with at least half of the total number of trajectories (the majority). Only if an edge e is considered useful then it is allowed to be part of the median trajectory, and subsequently an attempt is made to include e or some other edge in its neighborhood in the median trajectory. A rough high-level description of the majority median algorithm is that all the edges that are not useful

are deleted initially and for all the remaining useful edges an investigation is carried out to determine whether or not they can be part of the median trajectory. To this end, suppose that a directed planar graph φ is constructed with all vertices of the trajectories T plus all intersection points of the edges of the trajectories. The edges in φ are edges or sub-edges (intersections are also included) from the trajectories in T. The direction of the edges in φ are identical to the directions of edges in T. For simplicity, it is assumed that all trajectories of T start in a common vertex s, the source, and they all end in a common vertex d, the destination. As mentioned previously, this restriction can easily be removed by introducing two dummy vertices if needed. The median trajectory is assumed to be some directed path in φ from s to d only containing useful edges, but not all of the useful edges. To find such a path, all edges of φ that are determined not useful are removed initially. Then, the shortest path from s to d in φ is computed as the first (tentative) median. Given a median, a useful edge is called happy if it is in the median or within distance at most 2δ from an edge in the median. As long as there are unhappy useful edges, a better median may be constructed by including more unhappy useful edges. A useful edge that is "most unhappy" (the one that is furthest from the median) is selected (edge e), and let $S(e)$ be the set of edges of φ within distance δ from e. The shortest paths from s to all endpoints of edges in $S(e)$, and shortest paths from these endpoints to d, are computed and they are combined to find an overall shortest path from s to d that uses some edge of $S(e)$. If such a path exists, then this is the new median and e and all edges in $S(e)$ must be happy. If such a path does not exist, then it is not possible to make e happy when using only useful edges for the median. Hence, e and all other edges in $S(e)$ are ignored. The algorithm stops when all useful edges are happy or ignored. Whether or not a new median is computed, there may still be not ignored, unhappy edges elsewhere, so to proceed, the most unhappy edge for the latest median is located, and the same procedure is followed to try to include it in the median.

The median trajectory is supposed to pass through a sequence of sets of endpoints $P_1, P_2, \dots, P_k$ between s and d, where each P_i corresponds to the endpoints of some set $S(e)$ of edges in the algorithm. The order $P_1, P_2, \dots, P_k$ is determined incrementally during the algorithm using a voting strategy, which is robust against deviations, shortcuts and noise. Once the order of $P_1, P_2, \dots, P_k$ is settled, a shortest path is computed between s and d, using Dijkstra's algorithm in an iterative manner for all the intermediate endpoints. The final shortest path from s to d visits at least some node of each of $P_1, P_2, \dots, P_k$ in the specified order. The details of the algorithm and its pseudo-code is described in [4].

The time complexity of the algorithm is polynomial regarding the input size $m \times n$. Nevertheless, the worst-case running time is rather high. A worst-case analysis does not characterize the actual running time well because it would refer to hypothetical cases where all edges of a trajectory intersect all edges of all other trajectories. Under assumption that any edge of any trajectory intersects with constant number of edges of other trajectories (i.e. there are $O(nm)$ edge-edge intersections in total), the worst-case time complexity would be $O(n^3 m^3 log(nm))$. This assumption leads to a size of the graph that is linear in the input size, $O(nm)$, and it also implies that the computed median has at most $O(nm)$ vertices [3].

The majority median trajectory for the bundle of trajectories depicted in Fig. 6(a) is shown in Fig.10. The extra paths regarding points 7 and 11 are skipped by majority of trajectories. The homotopic median (depicted in Fig. 6(b)) and the majority median both have identical global shape that respects the majority of input trajectories. It is worth noting that the homotopic median is based on only four trajectories because three do not have the same homotopy type. Consequently, the homotopic median does not always lie in the middle. Furthermore, the homotopic median demonstrates an artifact close to point 5. It is common for homotopic medians to experience extra angles especially near sharper bends. This is not the case with the majority median.

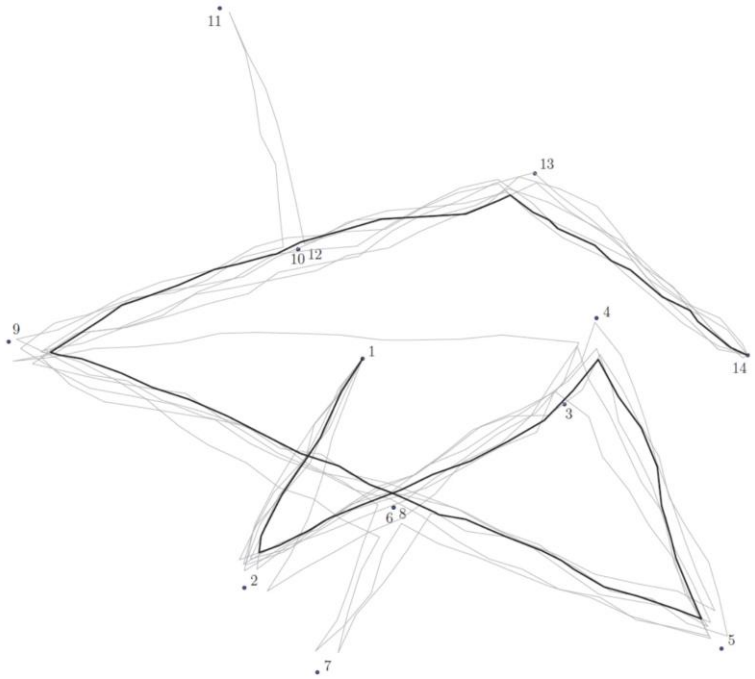


Figure 10 - The majority median trajectory (the black) for a bundle of input trajectories

The majority median satisfies most of the properties described in Section 1.4 for a representative trajectory. However, the median trajectory will not necessarily be locally centered since the focus is on the shortest path and not being in the center. In order to address this issue and improve the quality of the computed median, an alternative version of the majority median algorithm is also presented in [4]. The improved version differs only in assigned weights for edges when Dijkstra's algorithm is applied. In the original algorithm, the weight of an edge is just its Euclidean length. In the improved version, the weight of an edge is its Euclidean length times the size of the buffer needed for that edge to become useful (i.e. to have at least $\frac{m}{2}$ trajectories intersect the buffer). As a result, the alternative version gives preference to edges that are in dense areas because they are cheaper, and thus it outputs a median that is often more in the middle of the input trajectories.

Fig. 11 shows an example of a bundle of seven input trajectories, which were generated synthetically with a variation probability of 20% [3]. The trajectory generator creates trajectories that deviate on a larger scale utilizing three types of global variations with a certain probability. These include 1) skipping a point in a sequence of points, 2) visiting an extra, random point between two consecutive points in a sequence, 3) visiting an extra point from halfway between two consecutive points, and then going back to the halfway position to continue following the sequence. The markers with no numbers attached are the additional points used due to the variations, and they are used by some trajectories only. For example, three out of seven trajectories use the marker halfway between points 2 and 3 to go up and back to the marker between points 5 and 6. The homotopic median misses points 2 and 3, because the faces in this part of the input were considered too small to place a special point (poles). This can be resolved by choosing special points in smaller faces too, but then fewer trajectories are homotopically equivalent which has other negative consequences. The majority median and its alternative have the right global shape, but the majority median does not stay in the middle when the trajectories are close, for example near point 7. The alternative majority median is slightly better, although it has artifacts in the dense region left of the middle.

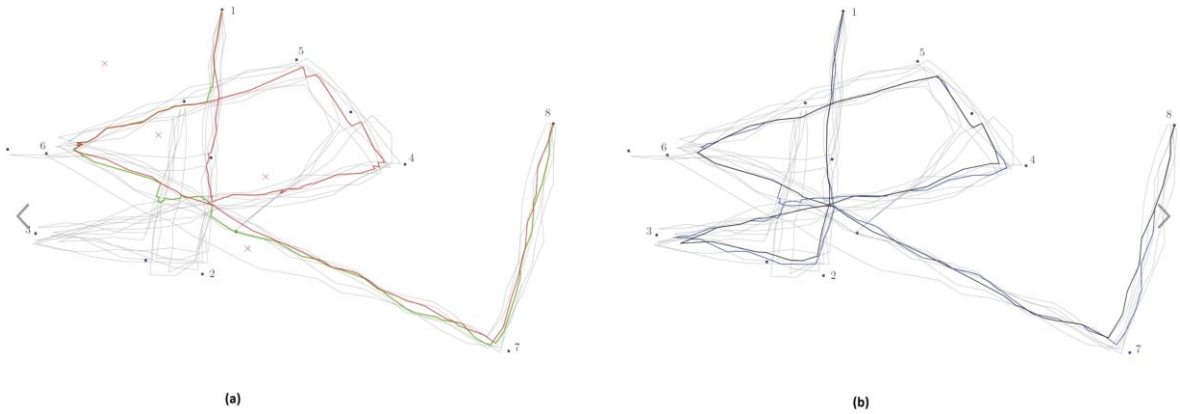


Figure 11 - Median trajectory for a bundle of seven input trajectories: (a) Simple median (green) and homotopic median (red), (b) Majority median (black) and alternative majority median (blue)

In general, the majority median and its alternative are supposed to slightly outperform the homotopic median. Nevertheless, the performance has to be defined based on the importance of the properties of the median. It is shown that the majority medians make fewer global errors (the correct shape of input trajectories are preserved) and have fewer artifacts, while the homotopic median is more in the middle when the trajectories are not deviating substantially [3]. There are several cases where the homotopic median performs better than the majority median [4]. An example in shown in Fig. 12. Although the majority median preserves and follows the overall path of input trajectories, it misses point number 4, because that area is already covered by another part of the median. On the other hand, the homotopic median is closer to point 4 and the result is better than the majority median in that part, even though it still misses the narrow space between points 2 and 3.

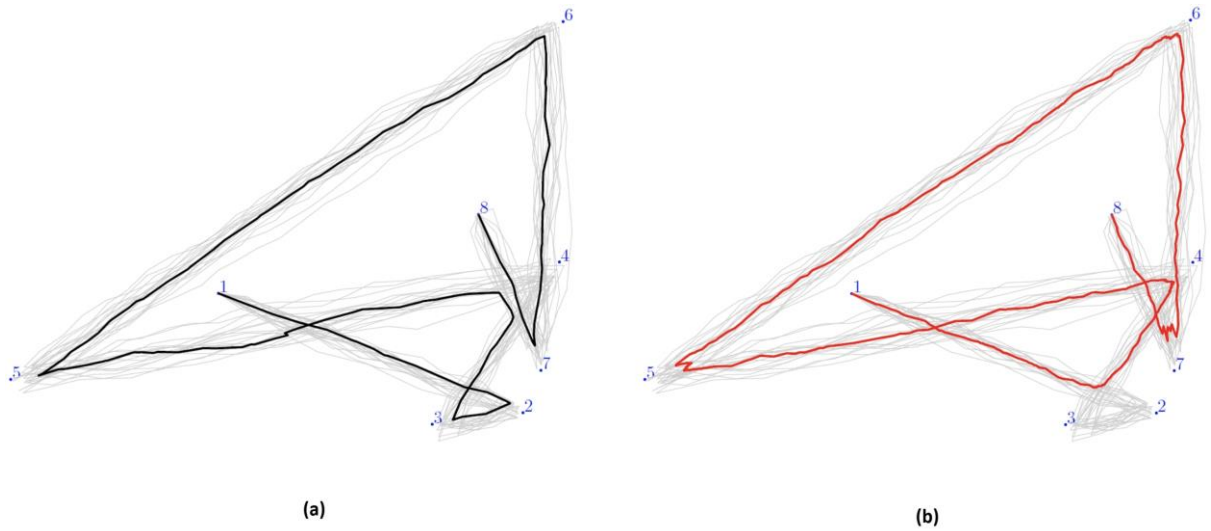


Figure 12 - The homotopic median trajectory outperforms the majority median: **(a)** Majority median misses' part of the path from point 3 to 4, **(b)** Homotopic median correctly follows the path from point 3 to 4

Conclusions. Most of the existing solutions to the problem of finding a middle trajectory do not take the temporal component into account. For some applications the time correspondence can not be clearly defined or it is logical just to ignore it. For example if we want to find a middle trajectory for several tourists taking a similar route. Due to different preferences, we can not use the

temporal information directly as they can take different paths on different times. If we include the temporal component, then we might find a completely different trajectory that is not irrelevant and pointless. Even following the same route, it can be that they have to stop at different locations. In this application, the temporal information is not relevant and can be simply ignored. However, in another application, it can be quite different. Suppose, we are not only interested in the route taken by most of the tourists but also the time it takes to complete an ordinary walking tour of a district. This can be difficult to compute because we have to ignore the stop incidents (visit tourist attraction, rest, eat, taking photos, etc.), which can be at different locations or can have different lengths. In this case we have to find a way to normalize the routes with regards to the timing information.

The methods that deal with temporal information of middle trajectories fall into two categories: 1) methods that are based on the notion of equal time slices, in which a middle trajectory is computed by finding a middle (representative) point for each time slice, 2) methods that assign timing data as a post processing step to a middle trajectory.

In addition to the properties described in Section 1.4, using temporal information for a representative trajectory, additional properties may be considered. These properties shall utilize the timing data in a way, e.g., the duration and speed of a middle trajectory should be comparable to the input trajectories in a bundle. The calculations of these properties is not straightforward and can be troublesome. One might define the duration of a trajectory as the time difference between the first and the last data points taking into account the stay points, or opt to exclude them from the calculation. Measuring the speed of a trajectory can also be done using the minimum, maximum or average speed, though it can be meaningless and not representative at all if several different scenarios and obstacles exist on the path.

The way the speed is determined for a middle trajectory influences its duration as well. If the calculation of the speed is based on the speed(s) of the input bundle, then the total duration of the middle trajectory can be a lot lower (similar speeds in combination with a shorter distance, which normally happens for the middle trajectory). A drawback would be that the middle trajectory can not be used to determine at what time a certain location will be visited. On the other hand, if the calculation is based on the total duration of the middle trajectory, then the middle trajectory can not be used to determine the speed in between the points. Hence, in this case, the middle trajectory should only be seen as a series of points where the time stamps represent the time at which the location will be visited, without having any information for what happens between two points. Regardless of the method that is used, we can set an upper bound on the speed that is based on the highest speed in the input. If this bound is exceeded, the result is most likely not a realistic representation of the input and either needs to be refined or rejected as a usable result. An example of such a scenario causing a trajectory to exceed speed bounds is when a trajectory spans great distances in a really short time [2].

Assuming that similar moving objects following the same itinerary behave in a similar way and move along an optimized main route (middle trajectory), Etienne et al. [5] proposed an approach to analyse the trajectories of these objects in order to infer several spatio-temporal patterns and then, to qualify their behavior by comparing their trajectories to these patterns. They first present a method to extract and filter trajectories of moving objects following a similar itinerary. This is done in several steps:

1. Formalizing the concepts of zones and itineraries, trajectories of same type of objects moving along the same path of an itinerary are extracted (a set of homogeneous bundle of trajectories).

2. Trajectories with an important gap between two consecutive positions or erroneous positions are filtered from the bundle in order to improve subsequent statistical analysis.

3. Filtering out starting and ending positions of trajectories within the departure and arrival zones in order to compute trajectories for which departure and arrival positions are independent from time of transmission (spatial shifting of trajectories). Without this filtering, measurements can be biased in the spatio-temporal patterns defined later.

4. Indexing and simplifying trajectories using a spatio-temporal variant of Douglas & Peucker filter to optimize subsequent computations by retaining only significant positions of trajectories while keeping information about both speed and heading changes.

5. Computing a relative timestamp for each position of a trajectory to ease distance and time comparison between trajectories. Timestamps of positions are useful to compute speed and order each position within a trajectory. The relative timestamp for each position of a trajectory indicates the time duration since the starting position of the trajectory.

6. Normalizing the timestamps of all the trajectories of a bundle to avoid spatial distortions introduced by slightly different speeds of moving objects. To compute this relative normalized timestamps, first of all, the median duration (D_m) of the bundle is calculated. Using this duration, a normalization process is applied to all positions so that each trajectory in the bundle begins at a time 0 and ends at (D_m).

After the initial phase of selecting and extracting the similar trajectories in a homogeneous bundle, the middle trajectory is computed by statistical analysis [6]. Considering the normalized timestamps previously, for each position of each trajectory in the bundle, positions of other trajectories are interpolated using their normalized timestamps. Then, at each normalized timestamp, a median position is selected using the median value of coordinates (latitudes and longitudes) of each position subset [7]. This creates a subset of positions for the whole trajectories in the bundle. Note that only meaningful positions that were selected by the spatio-temporal Douglas & Peucker algorithm are considered, so that the computation process is only applied on sub-parts of trajectories where mobile object behavior changes. Subsequently, the computed median positions are ordered according to their normalized time to create the middle trajectory for the bundle. Finally, this middle trajectory is also filtered using the spatio-temporal Douglas & Peucker algorithm. Listing 1 presents an outline of the algorithm for the computation of the middle trajectory.

```
for each trajectory Tr of the HGT_AIT do
    Delete erroneous trajectories
    Spatial shifting of starting and ending positions
    Douglas_Peucker_ST(Trajectory Tr)
    Temporal normalization using median duration t_m
end for
Algorithm Main_Route_Computation(HGT_AIT)
for each trajectory Tr_i of the HGT_AIT do
    for each position P_i of Tr_i do
        Let tn_i be the normalized time of P_i
        for each other trajectoiries Tr_j of the HGT_AIT do
            Interpolate the positions P_j at normalized time tn_i
            Add P_j to the subset of positions EP_i
        end for
        Compute median position P_med of EP_i
        Add P_med to the main route R_IT at normalized time t_ni
    end for
end for
return Douglas_Peucker_ST(Trajectory R_IT)
```

Listing 1 - The outline of the algorithm described in [5] for computing the middle trajectory in a bundle using the temporal information

Fig. 13 (a) depicts an example of a homogeneous trajectory bundle composed of 506 trajectories plotted in black. Looking at the figure shows that same-type moving objects with the same itinerary globally follow a main route (the middle trajectory) [8]. The cloud of dark dots shown in Fig. 13 (b) represents the subset of positions at a normalized timestamp, the large white dot indicates the median position of the whole subset. All these median positions ordered by theirs normalized timestamps compose the middle trajectory plotted in white in Fig. 13(a).

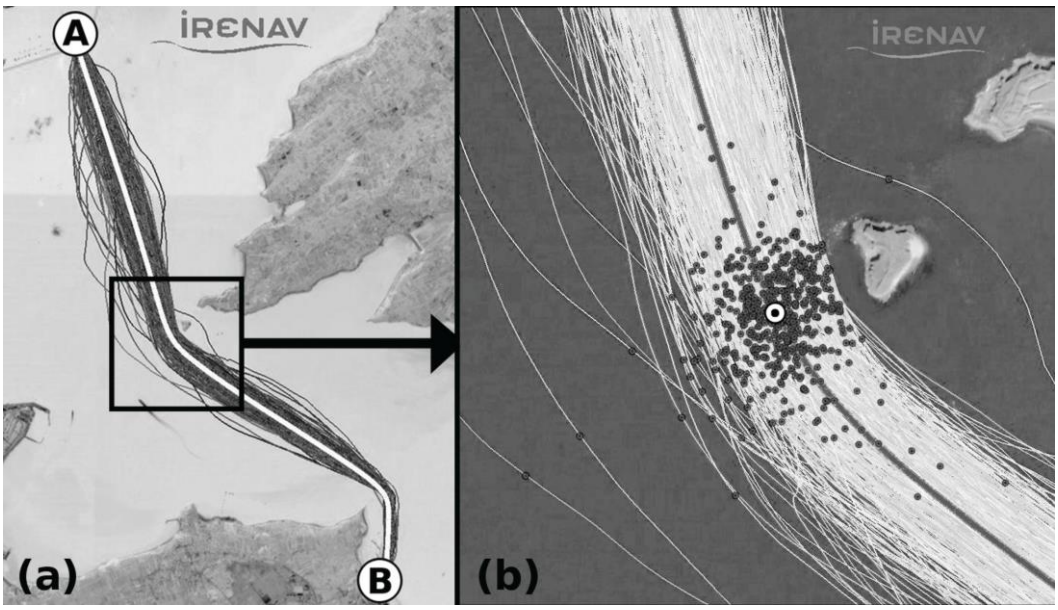


Figure 13 - A homogeneous bundle of trajectories and the computed middle trajectory

The main computational part of the algorithm described in listing 1 does not seem to the most efficient way of solving this problem in practice, however the asymptotic time complexity of the algorithm seems to be intact for more efficient alternative implementations. Another issue would be that for real world data, it is unlikely to identify exact locations known for all (equal) timestamps. For each input trajectory, in the worst case, there are $O(nm)$ data points to process because there are n timestamps and m trajectories, each of which might contain unique timestamps. This gives for a total running time of $O(nmT(m))$ for the main part of the algorithm, where $T(m)$ is the time it takes to process m points of equal time.

REFERENCES:

1. Buchin, K., Buchin, M., van Kreveld, M., Löffler, M., Silveira, R., Wenk, C., Wiratma, L. (July 2013), Median Trajectories**,** *Algorithmica* 66(3), pp. 595–614.

2. Vermeulen, T. (October 2013) Algorithms for finding a middle trajectory, Master's Thesis, TU Eindhoven.

3. Van Kreveld, M., Wiratma, L. (November 2011), Median trajectories using well-visited regions and shortest paths, In Proceedings of the 19th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems, pp. 241-250.

4. Wiratma, L. (2010), Following the Majority: A New Algorithm for Computing a Median Trajectory, Master's Thesis, Department of Information and Computing Sciences, Utrecht University.

5. Etienne, L., Devogele, T., Bouju, A. (2012), Spatio-temporal trajectory analysis of mobile objects following the same itinerary, In Advances in Geo-Spatial Information Science, 10, pp. 47–57.

6. Biagioni, J., Eriksson, J. (2012) Inferring road maps from global positioning system traces: Survey and comparative evaluation. Transportation Research Record: Journalofthe Transportation Research Board 2291, pp. 61-71.

7. Y.Chen, J. Krumm (2010) "Probabilistic modeling of traffic lanes from GPS traces", Proceeding soft the 18th SIGSPATIAL International Conference on Advancesin Geographic Information Systems, ACM, pp. 81-88.

8. B. Xu, M. Stroila, J. MacFarlane (2014) "A Before and After Study for Travel Time of Unconventional Intersections Using Probe Data", Proceedings of ACMSIGSPATIAL International Workshopon Computational Transportation Science.

д.т.н., проф. Заславський В.А., Пушкаренко Ю.В.

АНАЛІЗ ТРАЕКТОРІЇ ГОЛОВНОЇ КРИВОЇ

Збільшення доступності джерел даних геолокацій дозволяє використовувати їх в процесі автоматизації створення карт, корегувати зміст існуючих карт, а також надає потенціал для створення джерел істини (тобто ground truth) як у військовому, так і в цивільному аспектах. Це необхідно для підтвердження якості існуючих карт, а також для їх публікації з використанням різних джерел для досягнення комплексного результату створення мап надвисокої чіткості. Основна ідея полягає в тому, щоб формувати кінцеву карту не тільки базуючись на супутникових знімках, а й використовувати інші джерела і в тому числі дані геолокацій. Ми не заглиблюватимемось в сам процес формування карт, а зосереджуємось на проблематиці зіставлення карти з точки зору траєкторій отриманих з GPS, оскільки власне сам процес отримання за своєю природою є дуже спотворений завадами. В даній роботі здійснюється аналіз методів, заснованих на формуванні траєкторії головної кривої, сформованої з "сирих" даних GPS-локацій. Яскравим прикладом може бути геолокація яка отримана з телефону всередині автомобіля та є «зашумленою», тобто локація не обов'язково збігається з фактичним географічним положенням автомобіля у певний момент часу. Якщо припустити, що автомобіль їде вулицею згідно з правилами, то такі дані геопозицій на великій виборці можна зіставити з розташуванням вулиць за допомогою алгоритмів зіставлення карт. Використання серії покращень на великій виборці такими алгоритмами стабілізує і узгоджує положення об'єктів на карті, особливо коли дані локацій «спотворені завадами» або неповні, такими прикладами є різнотипність доріг, розташованість або близькість одна до одної (перехрестя, мости, тунелі, з'їзди).

Одним із таких підходів та пов'язані з ним алгоритми - є аналіз траєкторії головної кривої (або компоненти). Аналіз траєкторій головних кривих останнім часом привертає значну увагу завдяки технологічним досягненням у навігаційних і картографічних системах. Тим не менш, деяким фундаментальним концепціям все ще бракує ретельного вивчення. Ідентифікація середньої (репрезентативної) траєкторії в низці траєкторій є такою фундаментальною проблемою. Якщо не заглиблюватись у сутність судження, середня траєкторія - це траєкторія, яка лежить всередині сукупності траєкторій. Втім, дане твердження є далеким від вичерпності.

Ця дослідницька робота зосереджена на концепції знаходження траєкторії головної кривої серед низки траєкторій із конкретними точками відправлення та призначення. Основна ідея полягає у використанні інформації про час, пов'язаної з траєкторіями, для покращення існуючих методів аналізу траєкторій. Ми досліджуємо концепцію головної кривої, пов'язану з інформацією про час, також даємо огляд алгоритмів щодо всіх існуючих методів, аналізуємо час роботи в найгіршому випадку та показуємо, що за певних припущень такі методи, як хронометраж, можуть бути реалізовані ефективно.

Ключові слова: Узгодження карт, геопросторовий аналіз, обчислювальна геометрія, кластерний аналіз, дані геопозицій, виокремлення геометрії доріг, дорожні карти, аналіз просторових даних.

УДК 355. 53

к.військ.н., доц. **Зайцев Д.В.** (ВІКНУ)
к.пед.н., доц. **Прохоров О.А.** (ВІКНУ)
д.т.н., с.н.с. **Сєлюков О.В.** (КНУБіА)
Семеха С.М. (ВІКНУ)
Солодєєва Л.В. (ВІКНУ)

DOI: https://doi.org/10.17721/2519-481X/2021/73-04

ЗАГАЛЬНІ ПОЛОЖЕННЯ ПОРЯДКУ УПРАВЛІННЯ ПІДРОЗДІЛАМИ (TLP)

У статті розкриваються основи управління підрозділами й обґрунтовується системність планування та підготовки до виконання поставлених завдань командирами механізованих підрозділів за стандартами НАТО.

Визначена процедура управління підрозділами, початок управлінських функцій (діяльності) командира взводу після отримання попереднього бойового розпорядження, бойового розпорядження чи бойового наказу від старшого командира до завершення завдання. Після отримання нового (уточненого) завдання процес управління підрозділами починається з початку, згідно визначених та обґрунтованих 8 кроків процедури управління підрозділами. При цьому, загальний алгоритму дій командира взводу – планування, розрахунок часу, оцінювання обстановки, підготовка підрозділу, виконання завдання тощо залишається сталим та будуть розкриті в основній частині статті. Підкреслено, що порядок управління підрозділами включає послідовність дій, що допомагає командирам ефективно використовувати доступний час для видачі наказів та виконання завдань за призначенням. Порядок управління підрозділами за процедурою TLP (troop leading procedures) не є жорстким зводом правил, які виконуються у певній послідовності. Деякі дії можуть виконуватися одночасно чи в порядку, який відрізняється від того, що вказаний у викладенні основного матеріалу. Порядок управління підрозділами є процедурою, що застосовується відповідно до ситуації, тактичної обстановки, бойового досвіду командира взводу та командирів відділень, наявності часу на прийняття рішення, погодними умовами тощо. Завдання, пов`язані з деякими діями (такими як початок виконання завдання, відання попереднього наказу, проведення розвідки (рекогносцирування)) у процесі виконання можуть повторюватися декілька разів.

Прийняття рішення, як остаточно обраного варіанту дій командиром підрозділу з переліку можливих, зазвичай здійснюється на найближчому до ведення бойових дій місці – пункті управління (командно-спостережному пункті) після чіткого, однозначного усвідомленням ситуації. Процес управління підрозділами починається тоді, коли командиру взводу відповідним наказом старшого командира повідомляють про майбутнє завдання та здійснюється постійно зі стаціонарного або рухомого ПУ. Заключний етап – контроль та перевірка плану відбувається в ході виконання завдання командиром. Поточна інформація щодо порядку управління підрозділами обробляється в умовах обмеженого часу. Всі кроки мають бути виконані, навіть у скороченій формі. Таким чином, запропоновані кроки процедури управління підрозділами спрямована на допомогу командиру швидко розробити і видати бойовий наказ.

Ключові слова: порядок управління підрозділами; управління підрозділами за процедурою TLP; попереднє бойове розпорядження; кроки процедури управління підрозділами; бойовий наказ.

Вступ. Порядку управління підрозділами у всіх ланках управління за стандартами НАТО передуватиме: розробка концепції операції (бою, тактичних дій) (далі – бою); розподіл обов’язків та завдань між підлеглими, які необхідно виконати негайно; опис варіантів дій, їх підготовка; розроблення схеми (макету) в тактичній ланці у спрощеному вигляді.

Концепція бою описує, як командир передбачає його розвиток від початку до завершення. Концепція бою описує взаємозв'язок між діями, подіями та завданнями й пояснює, яким чином ці завдання приведуть до виконання місії. Концепція лише допомагає командирам у управлінні і не повинна розглядатися як жорсткий сценарій. Так, концепцією наступальних дій є зосередження в районі, тактичне приміщення на визначені рубежі (позиції), дії на об’єкті, нарощування зусиль та зміна бойових порядків. Для оборонних дій – інженерне обладнання місцевості перед своїми позиціями та своїх позицій, оборонні дії, проведення

контратаки з метою відновлення втраченого положення, нарощування зусиль, зміна бойових порядків, відновлення боєздатності [1-3].

Розробляючи концепцію бою, командир усвідомлює та обирає для себе найкращий спосіб використання рельєфу та місцевості, враховує сильні сторони свого підрозділу, слабкі сторони підрозділу противника. Усвідомлення, зокрема, включає запит старшого командира на застосування артилерії для здійснення вогневої підготовки, підтримки атаки та забезпечення всіх видів маневру. Потім він розробляє заходи контролю за маневром, щоб «як зрозуміліше довести його намір, поглибити розуміння схеми маневру, попередити ведення дружнього вогню та уточнити завдання і цілей вирішальної, формуючої та підтримуючої операцій» [2,3,6]. Командир також визначає аспекти всебічного забезпечення розробленого варіанту бою (тактичних дій).

Розподіл обов'язків. Командир розподіляє відповідальність за кожне завдання між підлеглими. Проте, незалежно від існуючого командного ланцюжка, розподіл обов'язків не повинен порушувати структуру виконання завдання. Командир повинен бути впевненим, що всі підрозділи, які знаходяться під його безпосереднім керівництвом, додані та підтримуючи підрозділи були залучені до виконання операції (бою) в якості підрозділів першого (другого) ешелонів або резерву, все обладнання і військово-технічне майно розподілено між підрозділами залежно від його ролі в бою й головне, щоб до кожного підрозділу під час підготовки до виконання завдання був доведений бойовий наказ (розпорядження) або інша відповідна команда. Командир повинен уникати зайвих складних командних структур та підтримувати цілісність підрозділів, де це можливо.

Опис варіантів дій та підготовка їх схеми (макету). Командири невеликих підрозділів для опису концепції бою в основному використовують опис варіанту своїх дій та макет місцевості. Ці два елементи – основа для 3 пункту бойового наказу (OPORD – Operations Order). Варіант дій визначає, як підрозділ буде виконувати місію (завдання) в певний проміжок часу самостійно або у взаємодії з сусідами.

Опис варіанту дій містить докладну інформацію про те, як часткове завдання підрозділу забезпечить виконання операції старшого командира; вирішальний момент операції і чому він є вирішальним; вид оборони; вид маневру під час наступу; район її проведення.

Схема (макет) варіантів дій (за бойовим статутом механізованих військ ЗС України – схема взводного опорного пункту) це один або декілька аркушів креслень, які допомагають командиру описати хід бою. Схема дає уявлення про порядок маневрених дій і допомагає командиру описати завдання в контексті бойового статуту. Опис варіантів дій та їх схема зосереджуються на вирішальному моменті. В описі варіантів дій вказується [1-3]:

- вирішальний момент і що робить його вирішальним;
- форма маневру або вид оборонної місії;
- завдання і мету штатних, підтримуючих та доданих підрозділів;
- пріоритети застосування резерву;
- найважливіші завдання при веденні бойових дій;
- кінцевий результат.

Схема варіантів дій повинна визначити, яким чином підрозділ має намір сконцентрувати свою бойову потужність у вирішальний момент. Після накладання на карту місцевості (за бойовим статутом механізованих військ ЗС України – робоча карта командира), схема варіантів дій стає для підрозділу планом виконання завдання.

Аналіз останніх досліджень. Аналіз першоджерел [1,3], перекладів та публікацій [2,4,5], керівних документів ГШ ЗС України [6,7], матеріалів науково-практичної конференції [8] свідчить, що впровадження порядку управління підрозділами за процедурою TLP як елементу переходу на стандарти НАТО є не чим іншим як щоденною, плановою роботою у військах. Для освітнього процесу – сьогоднішня задача уточнення (внесення змін) у тематичні плани підготовки курсантів, громадян, які навчаються за програмою підготовки офіцерів запасу й набуття практичних навичок офіцерами тактичної ланки в управлінні підрозділами після вивчення теоретичного матеріалу.

Військовий інститут імені Тараса Шевченка як один з провідних військових ВВНЗ України є в авангарді підготовки курсантів за процедурою TLP і саме цей досвід повинні врахувати в освітньому процесі викладачі, що здійснюють підготовку офіцерів запасу на факультеті післядипломної освіти.

Метою статті є: визначення порядку управління підрозділами тактичної ланки за процедурою TLP; стисла характеристика 8-х кроків процедури управління підрозділами, обґрунтування необхідності внесення змін до тематичних планів модулів навчання розділу ІІІ «Тактична та тактико-спеціальна підготовка» навчальної дисципліни «Військова підготовка» у Військовому інституті Київського національного університету імені Тараса Шевченка за всіма військово-обліковими спеціальностями.

Виклад основного матеріалу. Порядок управління підрозділами за процедурою TLP включає 8 кроків [1 - 3]:

Отримання завдання.

Видача попереднього бойового розпорядження.

Розробка попереднього плану.

Початок руху (виконання завдань).

Проведення розвідки (рекогносцирування).

Завершення складання плану.

Видача бойового наказу.

Контроль та перевірка плану.

Кроки 1,2 виконуються по порядку, а кроки 3-8 можна виконувати не дотримуючись жорсткої послідовності. Також можна виконувати одночасно декілька кроків. В умовах бою командир може не мати достатньо часу для детального виконання кожного кроку, але необхідно *застосовувати дану процедуру,* щоб бути впевненим що нічого не залишилося поза увагою. Кількість часу, яка є в розпорядженні командира, буде впливати на кількість деталей, які приймаються до уваги на кожному кроці процедури. У разі отримання нової інформації план необхідно обновите та скоригувати.

Після отримання завдання, час завжди обмежений, тому його необхідно використати розумно. З усіх доступних ресурсів лише час не можливо повернути назад. Необхідно використати не більше 1/3 доступного часу на планування і видачу Бойового наказу. Підлеглому особовому складу потрібно надавати 2/3 часу, на складання плану та підготовки їхньої частини завдання. Цей процес відомий як «правило 1/3, 2/3». Щоб добре розподілити час, необхідно використовувати протилежне, або зворотне планування (відштовхуючись від часу проведення атаки або початку виконання завдання).

Крок 1 – отримання завдання. Командири визначають завдання для своїх підрозділів і встановлюють час на його виконання. Вони можуть провести попередній (загальний) аналіз наказу використовуючи METT-TC (Mission, Enemy, Terrain and Weather, Troops Available, Time, Civilian Considerations – бойове завдання, противник, свої війська, місцевість, час, цивільна складова). Детальний аналіз METT-TC проводиться лише після видачі WARNORD (Warning Order – бойовий наказ). Командири взводів отримують завдання декількома способами: або у формі Попереднього бойового розпорядження або Бойового наказу.

На основі інформації із отриманого завдання (висновків з нього), командир повинен: оцінити час необхідний для підготовки та виконання завдання; підготувати початковий графік планування та виконання завдання; провести початковий аналіз часу, який є для планування; визначити загальну кількість часу, який є на планування та підготовку; проаналізувати час, який є для підготовки свого підрозділу; підготувати початковий графік виконання основних заходів з розподілом часу за елементами.

Крок 2 – видача попереднього бойового розпорядження. Попереднє розпорядження – це повідомлення про дії, які необхідно буде виконати. Попереднє бойове розпорядження менш деталізоване ніж Бойовий наказ. Якнайшвидша віддача Попереднього бойового розпорядження дозволяє підлеглому особовому складу почати власне планування та підготовку (паралельне планування) до того часу, поки буде розроблено Бойовий наказ. Коли

командир отримує більше інформації, то видаються оновлені Попередні бойові розпорядження, які надають особовому складу всю відому командиру інформацію.

Попереднє бойове розпорядження відповідає 5 пунктам формату Бойового наказу та включає наступне: тип операції; місце проведення операції; первинний розрахунок часу; здійснення необхідної розвідки; здійснення необхідних переміщень; вказівки щодо планування та підготовки (включаючи розрахунок часу); вимоги щодо загальної інформації; вимоги командира щодо критичної інформації.

Зміст Попереднього бойового розпорядження:

1. Обстановка (зона особливої уваги; район ведення дій; війська противника; додані і виведені з під порядкування сили і засоби).

2. Завдання (хто; що; коли; де; чому).

3. Виконання (концепція бою (операції); завдання підпорядкованих підрозділів; вказівки щодо взаємодії).

4. Забезпечення (матеріально-технічне забезпечення; обслуговування особового складу; забезпечення системи охорони здоров'я).

5. Управління та зв'язок (управління, контроль, зв'язок).

Крок 3 – Розробка попереднього плану. В ситуації коли час обмежено, командир розробляє лише один варіант дій COA – (Course of action). Якщо час дозволяє, з метою порівняння, він може розробляти яку завгодно кількість варіантів дій. Командир починає крок 3 Порядку управління підрозділами після того, як він віддасть власне Попереднє бойове розпорядження і після того, як він отримає наступне попереднє бойове розпорядження від старшого командира.

Етапи 3-го кроку:

1. Аналіз (усвідомлення) завдання.

2. Загальна характеристика METT-TC:

- аналіз завдання (підрозділів одним та двома рівнями вище, задача свого підрозділу, обмеження та заборони, основні, допоміжні, найважливіші, переформульовані);

- оцінка противника (IPB – information preparation of the battlefield, інформаційна підготовка поля бою; тактичний аналіз; сильні сторони; можливості);

- оцінка місцевості і погодні умови (OAKOC – obstacles, avenues of approach, key terrain, observation, and cover and concealment, перешкоди, шляхи підходу, ключові ділянки місцевості, сектори спостереження та обстрілу, захисні та маскувальні властивості);

- аналіз військ та наявність підтримки;

- аналіз наявного часу;

- цивільні фактори;

3. Оцінка ризиків та розробка ключових моментів.

4. Розробка та вибір варіанту дій.

5. Розробка концепції операції.

6. Розподіл обов'язків.

7. Опис варіантів дій та підготовка їх схеми (макету). Командири невеликих підрозділів для опису концепції місії в основному використовують опис варіанту своїх дій та макет місцевості. Ці два елементи - основа для 3параграфу бойового наказу (OPORD).

8. Варіант дій визначає, як підрозділ буде виконувати місію.

9. Аналіз варіантів дій (воєнна гра).

10. Воєнна гра.

11. Порівняння і вибір варіанта дій.

Крок 4 – Початок руху (виконання завдань). Командири ініціюють виконання заходів, які необхідні для продовження підготовки до виконання завдання. Цей крок може бути проведений у будь-який час протягом усього TLP. Він може включати переміщення до району зосередження, до бойової позиції або іншого району операційної зони.

Підрозділи можуть здійснювати переміщення, залежно від ситуації, без командира підрозділу під командою сержантів. Командир підрозділу буде переміщуватись з рештою сил до початку виконання завдання. Це часто робиться для проведення наступного кроку TLP.

Структура бойового наказу

I. Обстановка

Район відповідальності (операції) – місцевість; погодні умови

Сили противника.

Останні дані розвідки – *власні війська; н*а 2 рівні вище; на рівень вище;

сусідні підрозділи

Додані або виділені підрозділи – Хто /Чому.

II. Завдання

Хто ?

Що ?

Де ?

Коли ?

Чому ?

III. Виконання

Намір (задум) командира.

Концепція операцій.

Схема переміщення і маневру – пояснення з початку до кінця.

Задачі для підлеглих підрозділів.

Координуючі інструкції – графік часу; критичні вимоги командира до інформації FFIR (Friendly Force Information Requirements); пріоритетні вимоги щодо розвідки; відомості про дружні сили і засоби заходи контролю за зменшенням ризику правила ведення бойових дій складова навколишнього середовища; захист військ

IV. Забезпечення

Логістика – технічне обслуговування; перевезення; польове обслуговування.

підтримка особового складу – вирішення питань EWP – electronic warfare plan

медичне забезпечення – надання медичної допомоги, евакуація поранених, медичні профілактичні заходи

V. Командування і сигнали

Командування – місце знаходження командирів.

Контроль – місце розташування КП (КСП).

Сигнали – радіочастоти, паролі, сигнали.

Крок 5 – Проведення розвідки (рекогносцирування). Командир повинен провести розвідку особисто та порівняти її з розвідувальною інформацією вищого штабу. Якщо можливо, командири повинні залучити для проведення розвідки (рекогносцирування) підлеглих командирів. Це дає можливість оглянути більше території і оцінити сили противника. Проведення розвідки також допомагає підлеглим командирам зрозуміти, як бачить операцію (бій) їхній командир.

Проведення розвідки командиром може включати переміщення до вихідного рубежу (LD – Line of Departure) або за його межі; розвідку району бойових дій; відхід від переднього краю ведення бойових дій назад до району зосередження взводу або висування на бойову позицію уздовж шляхів підходу противника. Якщо це можливо, командири повинні обрати тактично важливі пункти з найкращою можливістю огляду точки вирішальних дій.

Характер розвідки, її обсяг та тривалість залежить від тактичної обстановки і наявного часу. Результати та висновки з розвідки командир повинен включити у свій аналіз (розрахунок) часу. Він також повинен розглянути питання про те, як повідомити про зміни у плані своїм підлеглим і як ці зміни вплинуть на його план, дії підлеглих та інші підрозділи підтримки.

Крок 6 – Завершення планування. Під час цього кроку обраний (або уточнений) план дій командир перетворює у **бойовий наказ**.

Готуються оверлеї, уточнюється перелік цілей для ураження артилерією з закритих вогневих позицій, завершується розробка команд та сигналів для управління підрозділами, а також оновлюється попередній план на основі останніх даних розвідки.

Також командири готують матеріали для брифінгу, які можуть їм знадобитися, під час доведення бойового наказу підлеглим. Використання наведеної нижче структури бойового наказу допомагає пояснити усі аспекти операції (бою), врахувати місцевість, противника, підрозділи вищого рівня і сусідні підрозділи, завдання свого підрозділу, порядок виконання завдання, підтримку і децентралізацію управління в певні періоди операції (бою).

Цей формат також слугує контрольним списком, щоб гарантувати, що охоплено всі елементи операції. Він також дає підлеглим точне розуміння дій від самого початку і до кінця.

Крок 7 – Видання бойового наказу. Бойовий наказ точно і стисло пояснює намір командира і концепцію того, як він передбачає виконання підрозділом завдання. Бойовий наказ не повинен містити зайвої інформації.

Бойовий наказ доводиться до відома підлеглих швидко і таким чином, щоб підлеглі могли зосередитись і зрозуміти задум командира, а не просто дослівно копіювати те, що він сказав. Командир, в свою чергу, повинен підготувати і доповісти бойовий наказ впевнено і швидко, щоб вселити в підлеглих впевненість у своїх діях.

При виданні бойового розпорядження командир повинен впевнитися, що його підлеглі розуміють і притримуються його концепції, що може бути зроблено, коли і як саме. Вони повинні розуміти, як усі взводи повинні працювати разом, щоб виконати завдання. Вони також повинні розуміти, завдання взводу, хто підтримує, наміри старшого командира.

Кожен підлеглий повинен підтвердити, що він розуміє замисел командира і те, як завдання повинно бути виконано з урахуванням вирішального фактору. Це коротке підтвердження дає можливість визначити, чи є якісь недоліки або непорозуміння.

Крок 8 – Контроль та перевірка плану. Останній етап порядку дій командира з управління підрозділами є вирішальним. Після видання бойового наказу командир та підлеглі йому командири повинні забезпечити необхідні дії, а задачі повинні бути виконані заздалегідь, до завершення завдання. І офіцери, і сержанти повинні перевіряти все, що є важливим для завершення завдання. Це включає, але не обмежується: проведення чисельних інструктажів з приводу всіх аспектів бою; наявність заступника командира у кожному підрозділі для виконання обов'язків командира за умови його відсутності; заслуховування бойових наказів підлеглих командирів; перевірка плану дій; перевірка стану зброї і її готовності до використання; перевірка технічного обслуговування озброєння та військової техніки; виконання заходів безпеки у всіх видах діяльності.

Перевірка відпрацювань. Відпрацювання – це практичні заняття, які проводяться з метою підготовки підрозділів до майбутньої операції. Вони є дуже важливими, оскільки забезпечують підготовку, координацію, розуміння плану і наміру командира. Командири не повинні недооцінювати важливість відпрацювань. Відпрацювання повинні бути інтерактивними, підлеглі маневрують свої реальні бойові машини або використовують моделі машин або їх імітацію з озвучуванням дій підрозділу. Під час кожного відпрацювання увага надається тому, як підрозділ, який дозволяє підлеглим підрозділам відпрацьовувати дії, передбачає власну схему маневру [5].

Командири можуть проводити декілька видів відпрацювань, які включають: перевірочні інструктажі; загальновійськові відпрацювання (тактико-стройові заняття); відпрацювання з підтримки (вогневий супровід, забезпечення); відпрацювання взаємодії тактичних завдань бойових груп та пунктів управління.

На відпрацюваннях необхідно дотримуватись методики «повзти-йти-бігти», коли це можливо. Це готує особовий склад до умов, максимально наближених до бойових. Формами відпрацювань можуть бути [3]: повне (генеральне); у неповному складі (тільки ключові особи); макету місцевості; макету місцевості у цифровому форматі; схеми місцевості; карти місцевості; відпрацювання з комунікаційними мережами.

Зокрема, відпрацювання з комунікаційними мережами підрозділи здійснюють через глобальні або локальні комп'ютерні мережі. Командири і штаби практикують ці відпрацювання, обговорюючи найважливіші частини операції (бою) за допомогою мережі радіозв'язку в послідовності, яку встановлює командир. Підрозділ відпрацьовує тільки критично важливі частини операції (бою). Усім учасникам потрібні справні (реальні) інформаційні системи, виданий напередодні бойовий наказ і оверлеї. Командні пункти повинні спостерігати за розвитком бою під час відпрацювань з комунікаційними мережами.

Висновки. В статті, в загальних рисах, визначена процедура управління та прийняття рішення за стандартами НАТО – TLP. Автори наголошують, що TLP не є жорстким зводом

правил, які виконуються у певній послідовності. Деякі дії можуть виконуватися одночасно чи в порядку, який відрізняється від того, що вказаний у викладенні основного матеріалу.

По-друге, при виконанні бойових завдань в СВ ЗС країн НАТО застосовуються дві основні процедури командування та управління військами (підрозділами):

– процес прийняття військових рішень (military decision making process – MDMP), який застосовується на рівне від батальйону і вище;

– процедура управління військами (troop leading procedures – TLP), яка застосовується в підрозділах на рівні від роти та нижче) [8,9] і саме ця структура розкрита авторами в статті.

По-третє. Слід відмітити, що процедури управління військами (підрозділами) описані не тільки в статутах, керівництвах для механізованих підрозділів і рейнжерів, але і в «Операційному процесі» (ADP 5-0), «Керівництві для командира і штабного офіцеру» (ATTP 5-0.1) та інших настановах. Використання основ процедур TLP практично у всіх керівних документах воєнного відомства США, країн-членів НАТО підтверджує взаємозв'язок та залежність між методологією армійського проектування, військовим процесом прийняття рішення MDMP та процедурою управління TLP.

І останнє, необхідно внести зміни (коригування, доповнення) в робочі програми, погодити їх із Замовниками та в тематичні плани навчальних модулів. Зміни повинні торкнутися всієї тематики, що передбачає вивчення етапів підготовки бою (дій) та її основної складової – організації в ланці рота-взвод-відділення.

ЛІТЕРАТУРА:

1. Overview of troop leading procedures. Режим доступу: www.armystudyguide.com

2. Процес прийняття рішень під час бойових дій. Головний офіс: МКЧХ. К.: ICRCUA twitter.com/ICRC_ua, 2018 р.

3. Army troop leading procedures. Режим доступу: https://www.part-time-commander.com/troop-leading-procedures/

4. Поліщук Л.І., Климович О.К., Богуцький С.М., Пащетник О.Д. Процес прийняття рішення на ведення бойових дій в сухопутних військах збройних сил країн НАТО. Озброєння та військова техніка – 2018. – №4 (20). – с.3-8.

5. Поліщук Л.І., Климович О.К., Богуцький С.М. Алгоритм роботи органів управління в сухопутних військах збройних сил країн НАТО при прийнятті рішення на ведення бойових дій / Л.І. Поліщук, О.К. Климович, С.М. Богуцький // Зб. наук. праць – Одеса: Військова академия. – 2018. – № 2 (10). – с. 161-166.

6. Настанова з підготовки персоналу у Збройних силах України. ВКП 7-00(01).01. Головне управління доктрин та підготовки ГШ Збройних сил України. К.: 2020, 52 с.

7. Доктрина підготовки сил оборони держави (введена в дію наказом Генерального штабу Збройних Сил України від 21.01.2020 № 18). К.: 2020, 37 с.

8. Розвиток законодавства України у сфері оборони: проблеми адаптації до стандартів НАТО та шляхи їх вирішення : матеріали науково-практичної конференції. м. Київ, 23 квітня 2021 р. / упоряд.: П.П. Богуцький, В.Г. Пилипчук, С. О. Дорогих. – Київ, 2021. – 376 с.

REFERENCES:

1. Overview of troop leading procedures. Access mode: www.armystudyguide.com

2. The decision-making process during hostilities. Head office: ICRC. K .: ICRCUA twitter.com/ICRC_ua, 2018

3. Army troop leading procedures. Access mode: https://www.part-time-commander.com/troop-leading-procedures/

4. Polishchuk L, Klimovich O., Bogutsky S., Pashchetnik O. The decision-making process for combat operations in the ground forces of NATO forces. Weapons and military equipment - 2018. - №4 (20). - p.3-8.

5. Polishchuk L, Klimovich O., Bogutsky S. Algorithm of work of governing bodies in the land forces of the armed forces of NATO countries when deciding on combat operations / L.Polishchuk, O. Klimovich, C.Bogutsky // Coll. Science. works - Odessa: Military Academy. - 2018. - № 2 (10). - p. 161-166.

6. Guidelines for the training of personnel in the Armed Forces of Ukraine. VKP 7-00 (01) .01. Main Department of Doctrines and Training of the General Staff of the Armed Forces of Ukraine. K.: 2020, 52 p.

7. The doctrine of training of the state defense forces (introduced by the order of the General Staff of the Armed Forces of Ukraine of 21.01.2020 № 18). K.: 2020, 37 p.

8. Development of Ukrainian legislation in the field of defense: problems of adaptation to NATO standards and ways to solve them: materials of the scientific-practical conference. Kyiv, April 23, 2021 / edited by: P. Bogutsky, V. Pilipchuk, SO Dear. – K.: 2021, 376 p.

PhD Zaitsev D.V., PhD Prohorov O.A., D.Sci.Tech. Sieliykov O.V., Semeha S.M., Solodeeva L.V.

GENERAL PROVISIONS OF THE DEPARTMENT OF MANAGEMENT (TLP)

The article reveals the basics of unit management and substantiates the systematic planning and preparation for the tasks assigned by the commanders of mechanized units according to NATO standards.

The procedure for managing units, the beginning of management functions (activities) of the platoon commander after receiving a previous combat order, combat order or combat order from the senior commander until the end of the task. After receiving a new (updated) task, the process of managing units begins from the beginning, according to the identified and justified 8 steps of the procedure of managing units. At the same time, the general algorithm of actions of the platoon commander - planning, calculation of time, assessment of the situation, preparation of the unit, task execution, etc. remains stable and will be disclosed in the main part of the article.

It is emphasized that the order of management of units includes a sequence of actions that helps commanders to effectively use the available time to issue orders and perform assigned tasks. The TOP (troop leading procedures) procedure is not a rigid set of rules that are followed in a certain sequence. Some actions may be performed simultaneously or in a different order from that specified in the presentation of the main material. The unit management procedure is a procedure applied according to the situation, tactical situation, combat experience of the platoon commander and unit commanders, availability of time for decision-making, weather conditions, etc. Tasks related to certain actions (such as starting the task, maintaining a preliminary order, conducting reconnaissance (reconnaissance)) in the process of execution may be repeated several times.

Decision-making, as the final choice of action by the unit commander from the list of possible, is usually carried out at the nearest place to conduct hostilities - control point (command and observation post) after a clear, unambiguous awareness of the situation. The process of unit management begins when the platoon commander is notified of the future task by the relevant order of the senior commander and is carried out constantly from a stationary or mobile control point (CP) (command and control post – CCP).

The final stage - control and verification of the plan takes place during the task by the commander. Current information on the order of management of units is processed in a limited time. All steps must be performed, even in abbreviated form. Thus, the proposed steps of the unit management procedure are aimed at helping the commander to quickly develop and issue a combat order.

Keywords: the order of management of divisions; management of units according to the TLP procedure; preliminary combat order; steps of the unit management procedure; battle order.

УДК 681.32

к.т.н., ст. досл. **Лєнков Є.С.** (ЦНДІ ЗСУ)

DOI: https://doi.org/10.17721/2519-481X/2021/73-05

ПРОГНОЗУВАННЯ СКЛАДУ ТА РЕСУРСУ УГРУПУВАННЯ ОБ`ЄКТІВ ВІЙСЬКОВОЇ ТЕХНІКИ ТА АНАЛІЗ ЙОГО ВАРІАНТІВ

В роботі проведено прогнозування складу та ресурсу угрупування об`єктів військової техніки (ОВТ) та зроблено аналіз його варіантів. Можливими заходами по поповненню складу і ресурсу угруповання можуть бути поставки в угруповання нових ОВТ, а також ефективне технічне обслуговування і ремонт. Для того, щоб угрупування могло виконувати всі завдання у відповідності до свого призначення, воно повинно задовольняти встановленим вимогам за кількісним та якісним складом. Кількісний склад угрупування визначається кількістю ОВТ різних типів, наявних в даний момент часу і готових до негайного виконання завдань. При цьому кількість типів об'єктів і їх розподіл за типами повинно відповідати заданим вимогам. Для підтримки необхідної ефективності функціонування угрупування необхідно замість списаних поставити нові об'єкти відповідних типів, чи принципово нових типів, в тому числі закордонних.

Проаналізовано останні дослідження в даній предметній області, які наведено в великій кількості наукових робіт, що розв`язують проблему прогнозування складу та ресурсу угрупування об`єктів військової техніки. Аналіз його варіанту комплексі, в повній мірі фактично не існує. Це обумовлює необхідність розв`язання наукових задач прогнозування складу та ресурсу угрупування об`єктів військової техніки та аналіз його варіантів.

Математична модель процесу витрачання та поповнення ресурсу (ПВПР) угрупування розроблено методом імітаційного моделювання із застосуванням універсальної мови програмування процедурного типу. Це дозволяє, з одного боку, реалізувати в моделі всі істотні тонкощі моделюючого процесу і зробити програму компактною, зручною для практичного застосування.

Проведено прогнозування складу і ресурсу сучасних засобів ОВТ та їх угрупувань. Розглянуті режими нормативного планування термінів ремонтів та списання обєктів, що моделюються в моменти часу витрачення ресурсу. Поставки нових об'єктів моделюються в моменти часу, в які залишкова кількість працездатних об'єктів в угрупуванні знижується нижче допустимого значення. Для нових об'єктів, що надійшли в угрупування, ПВПР моделюється звичайним чином, точно так же, як і для всіх інших об'єктів. Розроблено генерування варіантів угрупування ОВТ та нормативне планування. Найменування збереженого варіанту автоматично формується за наступним правилом: ім'я угрупування- найменування типу об'єктів-кількість об'єктів в угрупуванні (в дужках) - порядковий номер варіанта. В подальшому це ім'я може бути змінено зручним для користувача чином. Для кожного зі збережених варіантів можна виконати повторне моделювання.

Ключові слова: прогнозування складу та ресурсу угрупування, об`єкти військової техніки, технічне обслуговування і ремонт, математична модель, поставка нових об'єктів, генерування варіантів угрупування.

Вступ та аналіз останніх досліджень. Складні об'єкти військової техніки (ОВТ) застосовуються за призначенням зазвичай в складі угруповань (військових частин, з'єднань, об'єднань). Прикладами складних ОВТ наприклад у протиповітряній обороні є радіолокаційні станції, зенітно-ракетні комплекси, станції радіоелектронної боротьби, системи зв’язку та управління. Можливими заходами по поповненню складу і ресурсу угруповання можуть бути поставки в угруповання нових озброєння і військова техніка (ОВТ), технічне обслуговування і ремонти різних видів [1]. Угрупування ОВТ створюються тимчасово, або на постійній основі для вирішення певних завдань на деякій території, чи окремих бойових дій. Для того, щоб воно могло виконувати всі завдання у відповідності зі своїм призначенням, воно повинно задовольняти встановленим для неї вимогам за її кількісним та якісним складом. Кількісний склад угрупування визначається кількістю ОВТ різних типів, наявних в даний момент часу і готових до негайного виконання завдань по їх призначенню [2]. При цьому кількість типів об'єктів і їх розподіл за типами повинно відповідати заданим вимогам.

Якісний склад визначається залишковим ресурсом ОВТ, наявних в угрупуванні. Чим більший в середньому залишковий ресурс об'єктів, тим якіснішим є її склад, тим більшою буде тривалість часу існування угрупування в стані, при якому всі поставлені завдання будуть виконуватися з необхідною ефективністю. В процесі експлуатації угрупування ресурс окремих об'єктів витрачається в цілому випадковим чином, внаслідок цього якісний його склад з часом погіршується, тобто скорочується «запас міцності». Після вичерпання ресурсу окремими об'єктами, їх експлуатація повинна бути припинена. Об'єкти, що вичерпали ресурс, повинні бути піддані ремонту для відновлення ресурсу, або списанню, тобто безповоротно вилучено з його складу.

Для підтримки необхідної ефективності функціонування угрупування необхідно замість списаних об'єктів поставити нові об'єкти відповідних типів, чи принципово нових типів, в тому числі закордонних.

Таким чином, для вищих органів (штабів), відповідальних за експлуатацію угрупування виникає важливе завдання своєчасного планування технічного обслуговування (ТО) і ремонту ОВТ і поставок в угрупування нових об'єктів [1,2]. Вочевидь, що вирішення такого завдання можливе лише на підставі застосування математичної моделі процесу витрачання та поповнення ресурсу (ПВПР) об'єктів, за допомогою якої можна і доцільно прогнозувати склад і ресурс угрупування.

В даній предметній області багато років працювали і працюють такі вчені Барзиловіч Є.Ю., Гніденко Б.В., Каштанов В.О., Креденцер Б.П., Ланєцький Б.М., Ушаков І.О., Шишанов М.О. та деякі інші.

Так в роботі [3] аналізуються особливості зенітної керованої ракети та ракетних двигунів твердого палива (РДТП), зенітної керованої ракети (ЗРК), як об'єктів експлуатації й продовження призначених показників, а також методи оцінки показників залишкового ресурсу. Запропоновано для оцінки показників залишкового ресурсу РДТП використовувати метод „доламування" і імовірнісну модель накопичення пошкоджень в елементах РДТП, ЗКР у часі. Розглянута імовірнісна модель у якій процеси накопичення пошкоджень описується марківськими випадковими процесами, приводяться основні розрахункові співвідношення.

У роботі [4] формулюються основні науково-методичні положення щодо оцінювання показників безвідмовності і залишкової довговічності при експлуатації складних технічних систем (СТС) за технічним станом. Розглядаються основні фактори, що визначають поняття граничного стану і залишкового ресурсу для СТС і їх складових частин, положення концепції оцінювання (прогнозування) залишкового ресурсу і терміну служби і методи їх оцінювання за результатами експлуатаційних спостережень і випробувань.

У роботі [5] формулюється задача визначення періоду проведення контролів граничного стану (КГС) за техніко-економічним критерієм, пропонується метод її вирішення. Наводяться основні розрахункові співвідношення для різних варіантів завдання регресійних залежностей показників безвідмовності від календарної тривалості експлуатації (сумарного напрацювання). Пропонуються рекомендації щодо обґрунтування періоду проведення КГС.

У роботі [6] наведено методичні рекомендації щодо розподілу агрегатів, блоків і систем керованих авіаційних засобів ураження (КАЗУ) на групи з урахуванням їх контролепридатності та впливу на безпеку застосування. У зв'язку з цим вважається доцільним представити КАЗУ у вигляді багаторівневої конструкції взаємодіючих елементів, що об'єднані в підсистеми різних рівнів. Використання процедури декомпозиції дозволить подати їх у вигляді деякої структури, що включає декілька рівнів, та провести розподіл систем, агрегатів, блоків тощо (далі – складових частин) на групи за деякими визначеними ознаками. Математичною основою формалізованого вирішення цієї задачі є агрегативно-декомпозиційний підхід, суть якого полягає в поданні структури складної системи сукупністю взаємозв'язаних елементів різного рівня.

Існує ще декілька робіт, найбільш цікавими з них, наприклад такі [7-11].

Аналіз цих та інших наукових робіт дозволяє зробити наступні висновки: доволі детально та повно вивчалась та розв`язувалась поставлена задача ще в часи колишнього СРСР,

оскільки вона була спрямована на підвищення боєготовності радянської ретро військової техніки. Наукових робіт, що розв`язують проблему прогнозування складу та ресурсу угрупування об`єктів військової техніки та аналіз його варіантів комплексно, в повній мірі сьогодні фактично не існує. Це обумовлює необхідність розв`язання наукової задачі прогнозування складу та ресурсу угрупування об`єктів військової техніки і аналізу його варіантів.

Основні результати досліджень. Математична модель ПВПР угрупування розробляється методом імітаційного моделювання. Це дозволяє, з одного боку, реалізувати в моделі всі істотні тонкощі моделюючого процесу і, з іншого боку, зробити програму компактною, зручною для практичного застосування. Автор є одним із розробників програми ISMPN [12-14], призначеної для моделювання процесів ТОіР складних об'єктів техніки. Виявилось зручним реалізувати імітаційну модель (ІМ) ПВПР угрупування шляхом введення в програму ISMPN додаткового режиму роботи. Введений режим був названий ***Угруповання ОВТ. Прогнозування складу і ресурсу***. Програмне забезпечення (ПЗ), реалізоване в рамках цього режиму, дозволяє вирішувати завдання двох типів:

1). виробляти дослідження моделі ПВПР для різних типів угрупувань з метою виявлення найбільш важливих властивостей моделі та подальшого використання цих знань на практиці;

2). вирішувати конкретні завдання планування експлуатації угрупувань ОВТ, що задаються користувачем.

Для викладу можливостей розробленого ПО моделі ПВПР угрупування, спочатку розглянемо всі можливі режими його роботи. Є два основні режими роботи:

- введення даних для нового угрупування (Reg=0);
- робота зі збереженими угрупуваннями (Reg=1).

Усі угрупування ОВТ (далі просто угрупування), з якими може працювати користувач, будемо розділяти на два типи - угрупування, які генеруються програмно (будемо називати їх віртуальними), і угрупування, що задаються користувачем (назвемо їх для користувача). Параметри генерування віртуальних угрупувань задаються користувачем, віртуальні угрупування існують тільки в пам'яті комп'ютера. Призначені для користувача угрупування відповідають конкретним угрупуванням, які існують у реальності, дані, що представляють ці угрупування (їх склад, ресурс кожного об'єкта, і т.і.), вводяться користувачем. Інформація про всіх угрупуваннях зберігається в базі даних (БД).

Власне моделювання ПВПР здійснюється тільки в режимі роботи зі збереженими угрупованнями. При цьому збережена угрупування може бути як віртуальної, так і для користувача. При роботі зі збереженими угрупованнями можливі два *режими моделювання*:

- генерування нового варіанту віртуальної угрупування (Reg_m=0);
- моделювання ПВПР (Reg_m=1).

Моделювання ПВПР можливо, як для згенерованого тільки що (ще не збереженого) варіанти угрупування, так і для створеної раніше і вже збереженої угрупування (віртуальної або користувальницької).

Безпосередньо моделювання ПВПР може проходити в одному з наступних режимів (назвемо їх режимами прогнозування):

- нормативне планування (Reg_p=0);
- нормативне планування + поставка нових об`єктів (Reg_p=1);
- планування користувача (Reg_p=2);
- планування користувача + поставка нових об`єктів (Reg_p=3).

У режимі нормативного планування терміни ремонтів і списання об'єктів, що моделюються (імітуються) в моменти часу витрачення ресурсу об'єктів. У режимі планування користувача відповідні терміни визначаються даними, що задаються користувачем (і збереженими в БД).

У режимах поставок нових об'єктів моменти часу надходження в угрупування нових об'єктів визначаються по заданому критерію необхідної кількості об'єктів даного типу в угрупуванні. Поставки нових об'єктів моделюються в моменти часу, в які залишкова кількість

працездатних об'єктів в угрупуванні знижується нижче допустимого значення. Для нових об'єктів, що надійшли в угрупування, ПВПР моделюється звичайним чином, точно так же, як і для всіх інших об'єктів.

По-перше, доцільно більш детально визначити вихідну інформацію для моделі ПВПР угрупування, яка була описана автором у [1,12,14]. Це необхідно тому, що склад вихідної інформації може відрізнятися в різних режимах роботи ПО моделі. Математична модель ПВПР в загальному вигляді представляється наступними співвідношеннями (наведемо їх тут ще раз):

$$N_{\Sigma i}(t) = N_i\left(t / \mathbf{P}^{\text{н}}_{\text{рес}\,i}, \boldsymbol{S}_i(t_0), \overline{\boldsymbol{\eta}}_i, \boldsymbol{\Pi}_{\text{р}i}, \boldsymbol{\Pi}_{\text{с}i}, \boldsymbol{\Pi}_{\text{н}i}\right);$$
$$R_{\Sigma i}(t) = R_{\Sigma i}\left(t / \mathbf{P}^{\text{н}}_{\text{рес}\,i}, \boldsymbol{S}_i(t_0), \overline{\boldsymbol{\eta}}_i, \boldsymbol{\Pi}_{\text{р}i}, \boldsymbol{\Pi}_{\text{с}i}, \boldsymbol{\Pi}_{\text{н}i}\right), \quad (1)$$

де $N_{\Sigma i}(t)$ та $R_{\Sigma i}(t)$ показники якості ПВПР, що представляють вихідну інформацію моделі (середня кількість об'єктів *i*-го типу, наявне в складі угрупування в момент часу *t*, та їх сумарний ресурс);

$\mathbf{P}^{\text{н}}_{\text{рес}\,i}, \boldsymbol{S}_i(t_0), \overline{\boldsymbol{\eta}}_i, \boldsymbol{\Pi}_{\text{р}i}, \boldsymbol{\Pi}_{\text{с}i}, \boldsymbol{\Pi}_{\text{н}i}$ – параметри моделі ПВПР.

Параметри $\mathbf{P}^{\text{н}}_{\text{рес}\,i}$, $\boldsymbol{S}_i(t_0)$ та $\overline{\boldsymbol{\eta}}_i$ є основними вихідними даними моделі, смисловий зміст їх наступне:

$\mathbf{P}^{\text{н}}_{\text{рес}\,i}$ – ресурсні характеристики об'єктів;

$\boldsymbol{S}_i(t_0)$ – стан ресурсу об'єктів в початковий момент часу t_0;

$\overline{\boldsymbol{\eta}}_i$ – середні значення інтенсивності витрачання ресурсу об'єктів.

Параметр $\mathbf{P}^{\text{н}}_{\text{рес}\,i}$ в розглянутої вище (у розділі 1) математичної моделі визначався таким чином:

$$\mathbf{P}^{\text{н}}_{\text{рес}\,i} = \left\{\left\langle R_i^{\text{нr}}, T_i^{\text{нr}}, N_i^{\text{нr}}\right\rangle, r = \overline{0, N_{\text{видр}}}\right\}, \quad (i = \overline{1, N_{\text{тип}}}) \quad 2)$$

де $R_i^{\text{нr}}$ – нормативний ресурс об`єкта *i*-го типу, заповнювати в результаті виконання *r*-го виду планового ремонту ПлР;

$T_i^{\text{нr}}$ – нормативний строк служби об`єкту *i*-го типу після проведення *r*-го виду ремонта;

$N_i^{\text{нr}}$ – кількість ПлР *r*-го виду до списання об`єкту;

$N_{\text{видр}}$ – кількість видів ПлР;

$N_{\text{тип}}$ – кількість типів об'єктів в угрупуванні. В описуваному тут ПО поки реалізована можливість моделювання тільки для одного типу ПР ($N_{\text{видр}} = 1$).

З урахуванням цього параметри $\mathbf{P}^{\text{н}}_{\text{рес}\,i}$ представляються наступним чином:

$$\mathbf{P}^{\text{н}}_{\text{рес}\,i} = \left\{\left\langle R_i^{\text{н0}}, T_i^{\text{н0}}, N_i^{\text{н0}}\right\rangle, \left\langle R_i^{\text{н1}}, T_i^{\text{н1}}\right\rangle\right\}, \quad (i = \overline{1, N_{\text{тип}}}) \quad (3)$$

де $\left\langle R_i^{\text{н0}}, T_i^{\text{н0}}, N_i^{\text{н0}}\right\rangle$ – нормативні параметри для нового об'єкта *i*-го типу; $\left\langle R_i^{\text{н1}}, T_i^{\text{н1}}\right\rangle$ – нормативні параметри заповнення ресурсу після проведення ПР, який за прийнятою практиці домовимося називати капітальним ремонтом (КР).

Крім параметрів (3) в якості характеристики КР задається також величина тривалості ремонту $\tau_{\text{кр}}$. Параметри $\mathbf{P}^{\text{н}}_{\text{рес}\,i}$ повинні бути задані в будь-якому випадку, незалежно від цілей і завдань моделювання. Параметр початкового стану об'єктів угрупування $\boldsymbol{S}_i(t_0)$ згідно (1.6) має таке уявлення:

$$\boldsymbol{S}_i(t_0) = \left\{\left\langle R_{ij}(t_0), T_{i_j}(t_0), n_{\text{р}ij}(t_0)\right\rangle; j = \overline{1, |\mathbf{O}_i|}\right\}, \quad (4)$$

де $R_{ij}(t_0)$ та $T_{ij}(t_0)$ – залишковий ресурс і залишковий термін служби *ij*-го об`єкту на момент часу t_0;

$n_{\text{р}ij}(t_0)$ – залишкова кількість ремонтів, яке повинно бути виконано до списання об'єкта;

$|\mathbf{O}_i|$ – кількість об`єктів *i*-го типу в досліджувальному угрупуванні.

Параметр $\boldsymbol{S}_i(t_0)$ в залежності від режиму роботи програми може здаватися двома способами:

- при роботі з віртуальним угрупуванням значення параметрів генерується випадковим чином в заданих діапазонах їх значень;
- при роботі з призначеної для користувача угрупованням ці параметри задаються користувачем шляхом безпосереднього введення їх значень в БД.

У розробленій версії ПО генеруються тільки параметри $R_{ij}(t_0)$ та $T_{ij}(t_0)$, для них задаються межі інтервалів варіювання:

$R1_i$ та $R2_i$ – межі інтервалу варіювання для параметра $R_{ij}(t_0)$;

$T1_i$ та $T2_i$ – межі інтервалу варіювання для параметра $T_{ij}(t_0)$.

Значення $R_{ij}(t_0)$ та $T_{ij}(t_0)$ при цьому генеруються як випадкові числа, рівномірно розподілені відповідно в інтервалах $[R1_i, R2_i]$ та $[T1_i, T2_i]$.

Параметр $n_{\text{р}ij}(t_0)$ не варіюється, для нього задається фіксоване значення $n_{\text{р}ij}(t_0) = N_i^{\text{н}0}$. Параметри $\overline{\boldsymbol{\eta}}_i = \{\overline{\eta}_{ij}\}$ (де $\overline{\eta}_{ij}$ – інтенсивності витрачання ресурсу *ij*-х об`єктів) равіюються тільки в режимі работи з віртуальним угрупуванням. Згідно (1.7) значення $\overline{\eta}_{ij}$ визначаються через ліміт витрачання ресурсу:

$$\overline{\eta}_{ij} = L_{Rij} / T ,$$

де L_{Rij} – ліміт витрати ресурсу, встановлений для *ij*-го об`єкту; *T* – період експлуатації, для якого встановлено ліміт $L_{Rij}$. З урахуванням цього варіюються не інтенсивності $\overline{\eta}_{ij}$, а ліміт витрачення ресурсу $L_{Rij}$. Для генерування його значень задаються нижня і верхня межі діапазону варіювання $L1_i$ та $L2_i$. Для кожного об`єкту значення L_{Rij} генерується як випадкова величина, рівномірно розподілена на інтервалі $[L1_i, L2_i]$. Параметри $\boldsymbol{\Pi}_{\text{р}i}, \boldsymbol{\Pi}_{\text{с}i}, \boldsymbol{\Pi}_{\text{н}i}$ – це плани заповнення ресурсу: план ремонту, план списання і план поставки нових об'єктів в угрупування. Відповідні плани можуть бути як вихідними даними (задаватися користувачем), так і результатами моделювання в залежності від режиму роботи моделі. Наприклад, в режимах **Нормативне планування** ці плани генеріруются в результаті моделювання незалежно від того, є угрупування віртуальної або користувальницької. У режимах **Планування користувача** плани задаються користувачем шляхом безпосереднього введення відповідних даних в БД.

У вихідних даних повинна бути введена також наступна інформація:

$N_i^{\text{тр}}$ $R_{\Sigma i}^{\text{тр}}$ – необхідні значення числа об'єктів *i*-го типу і їх сумарного ресурсу, які повинні підтримуватися протягом усього часу експлуатації угрупування;

D0 – дата, яка визначає початок інтервалу експлуатації угрупування (дата, відповідна моменту часу t_0);

N_I – кількість ітерацій моделювання при визначенні середніх значень результуючих показників $\overline{N}_{\Sigma i}(t)$ та $\overline{R}_{\Sigma i}(t)$;

Δ_η – інтервал варіювання середніх інтенсивностей витрачання ресурсу об'єктів $\overline{\eta}_{ij}$. Величина Δ_η задається у відсотках. Варіювання значень $\overline{\eta}_{ij}$ здійснюється від реалізації до реалізації процесу моделювання шляхом генерування їх значень як випадкових чисел, рівномірно розподілених в діапазоні

$$\left[\overline{\eta}_{ij}\cdot\left(1-\frac{\Delta_\eta}{2\cdot 100}\right),\overline{\eta}_{ij}\cdot\left(1+\frac{\Delta_\eta}{2\cdot 100}\right)\right].$$

Нижче розглядаються приклади, в яких докладно пояснюється технологія **введення даних і моделювання** в різних режимах застосування програми.

Для створення нового угрупування після запуску програми необхідно вибрати режим **Введення даних для нового угрупування** за допомогою списку вибору. Після вибору цього режиму вид екрану ПК буде таким, як це показано на рис. 1.

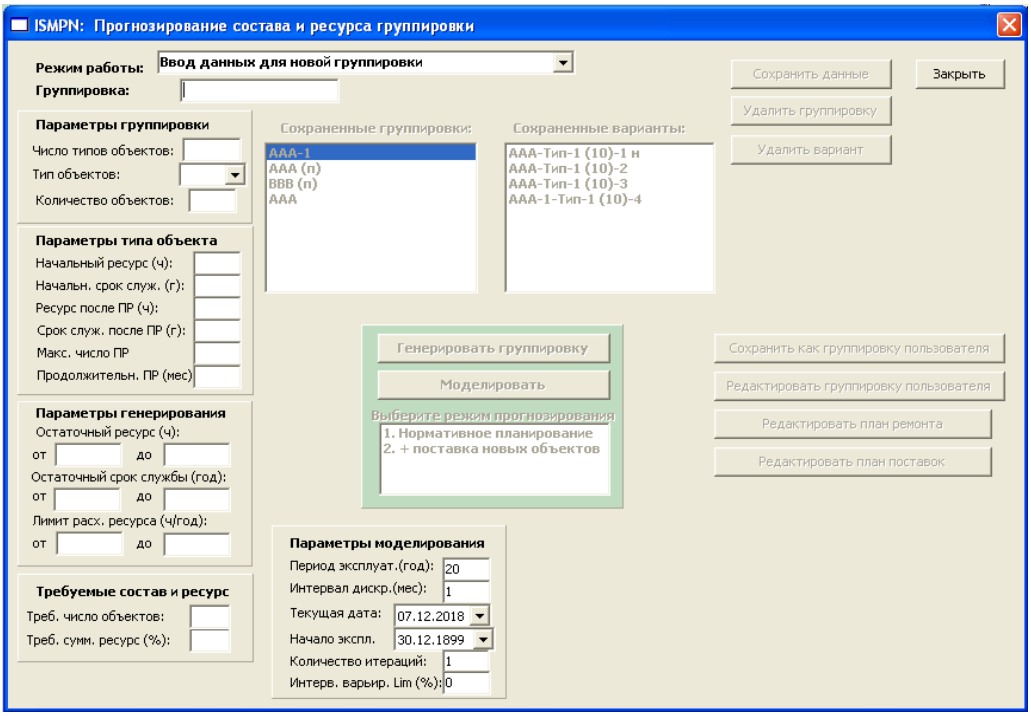


Рисунок 1 – Вихідний вид екрану ПК при введенні даних для нового угрупування

Для прикладу введемо наступні вихідні дані:

AAA - найменування угрупування;

$N_{\text{тип}}$ = 3 – кількість типів об'єктів.

Після введення $N_{\text{тип}}$ автоматично заповниться список типів об'єктів, яким будуть присвоєні умовні імена **Тип-0**, **Тип-1**, і т.д. На рис. 2 показаний фрагмент форми зі переліком вибору «**Тип об'єктів**» в розгорнутому стані.

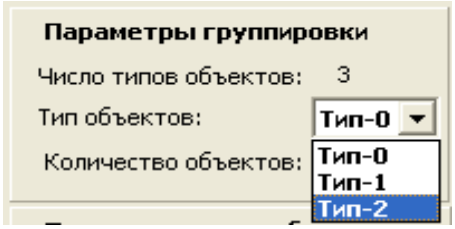


Рисунок 2 – Перелік вибору типу об`єктів

У розміщенні нижче елементах введення / редагування завжди відображається інформація, що відноситься до заданої в цьому списку типу об'єктів. Кількість об'єктів створюваної угрупування для різних типів об'єктів введемо наступне: $N_{\text{Тип-0}} = 3$, $N_{\text{Тип-1}} = 10$ та $N_{\text{Тип-2}} = 30$. Після цього для кожного типу об'єктів в панелі **Параметри типу об'єкта** введемо наступні дані (в розглянутому прикладі для всіх типів введемо однакові дані):

$R_i^{\text{н0}}$ = 1000 год – ресурс нового об`єкту;
$T_i^{\text{н0}}$ = 10 років; – строк служби нового об`єкту до 1-го ПлР чи до списання;
$R_i^{\text{н1}}$ = 8000 год – ресурс, з який заповнює після проведення ПлР;
$T_i^{\text{н1}}$ = 8 років – термін служби об'єкта, який заповнює після проведення ПР;
$N_i^{\text{н0}} = 2$ – кількість ПлР, яке повинно бути виконано на об'єкті до його списання;
$\tau_{\text{р}i} = 1\,\text{мес}$ – тривалість проведення ПлР.

Нижче, в панелі **Параметри генерування** введемо наступні дані:
$R1$ = 100 год та $R2$ = 10000 год – межі інтервалу варіювання початкового ресурсу об'єкта;
$T1 = T2$ = 10 років – межі інтервалу варіювання початкового терміну служби;
$L1$ = 1000 год/міс та $L2$ = 1500 год/міс – межі інтервалу варіювання ліміту витрати ресурсу.

В панелі **Необхідні склад і ресурс** введемо такі дані:
$N_{\text{Тип-0}}^{\text{тр}} = 2$, $N_{\text{Тип-1}}^{\text{тр}} = 8$ та $N_{\text{Тип-2}}^{\text{тр}} = 28$;
$R_{\text{тип-0}}^{\text{тр}} = R_{\text{тип-1}}^{\text{тр}} = R_{\text{тип-2}}^{\text{тр}} = 50\%$.

В панели **Параметры моделирования** вводятся данные:
$T_э$ = 20 років – період експлуатації угруповання (інтервал прогнозування);
Δt = 1 міс – інтервал дискретності зміни модельного часу;
D0 = 1.01.2018 – дата початку періоду експлуатації угрупування;
$N_I = 100\,(1)$ – кількість ітерацій моделювання;
$\Delta_\eta = 10\,(0)$ – інтервал варіювання середніх інтенсивностей витрачання ресурсу.

Після введення цієї інформації потрібно натиснути (клацанням миші) кнопку «Зберегти дані». Вся введена інформація буде збережена в БД. Програма автоматично перейде в режим **Робота зі збереженими угрупуваннями**. Найменування нового угрупування з'явитися в списку **Збережені угрупування**, як це показано на рис. 3. При цьому знаходиться праворуч список **Збережені варіанти** порожній, так як для щойно створеної угрупування її варіанти (реалізації) ще не генерувалися.

Далі у користувача є можливість наступних дій:

- виробляти дослідне моделювання із збереженою угрупуванням - для цього потрібно генерувати варіант (реалізацію) угрупування з заданими параметрами, зберегти створений варіант в БД і потім виконувати для нього прогнозні розрахунки (в цьому випадку створена угрупування має статус «віртуальна»);

- зберегти введене угруповання зі статусом «призначена для користувача» і продовжити введення необхідних вихідних даних, що визначають перебуваючи-ня об'єктів реальної угрупування.

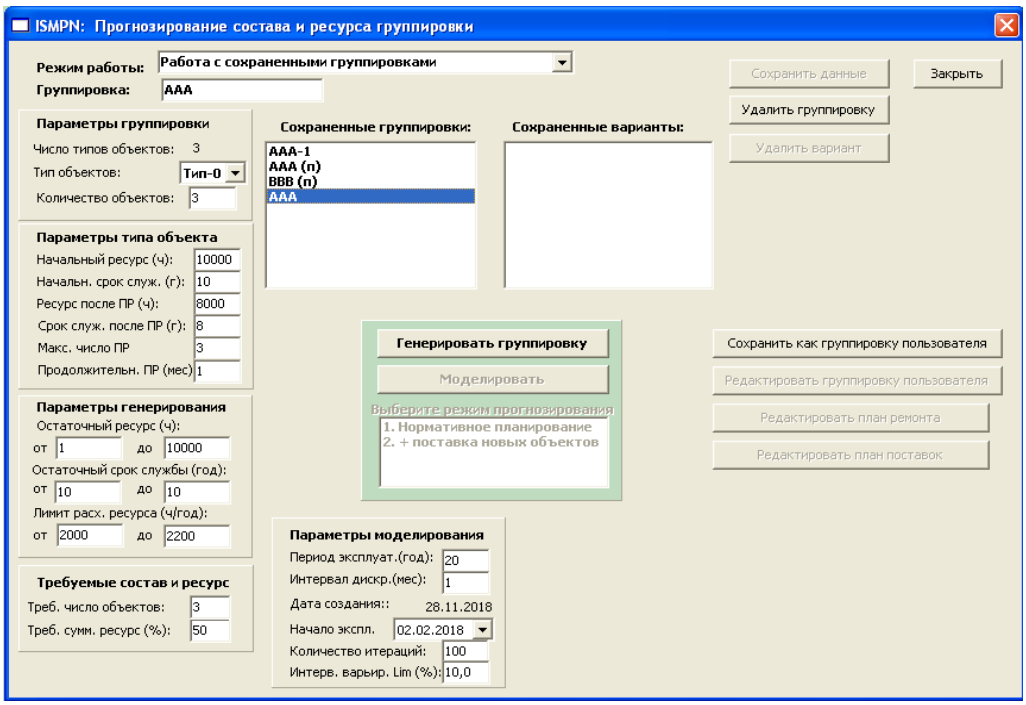


Рисунок 3 – Вигляд екрану ПК після збереження даних нового угрупування

Генерування варіантів угрупування. Для генерування варіанти угрупування необхідно вибрати потрібне угруповання в списку **Збережені угрупування** і потім натиснути кнопку «Генерувати угрупування» (рис.3) Якщо в даний момент кнопка не активована, необхідно в списку **Збережені угрупування** клацнути мишею на вибраному угрупуванню. Після цього активізується кнопка «Моделювати», а потім, після клацання на цій кнопці, активізується список доступних режимів прогнозування (рис.4). Для здійснення моделювання потрібно в цьому списку клацнути мишею на обраному режимі.

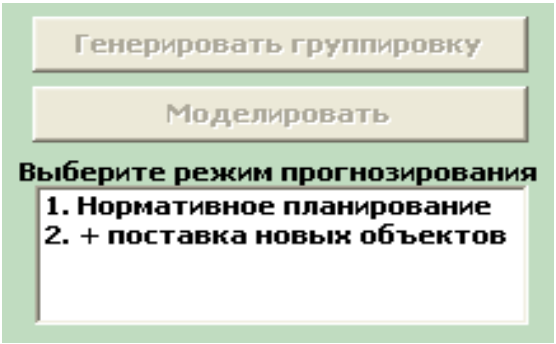
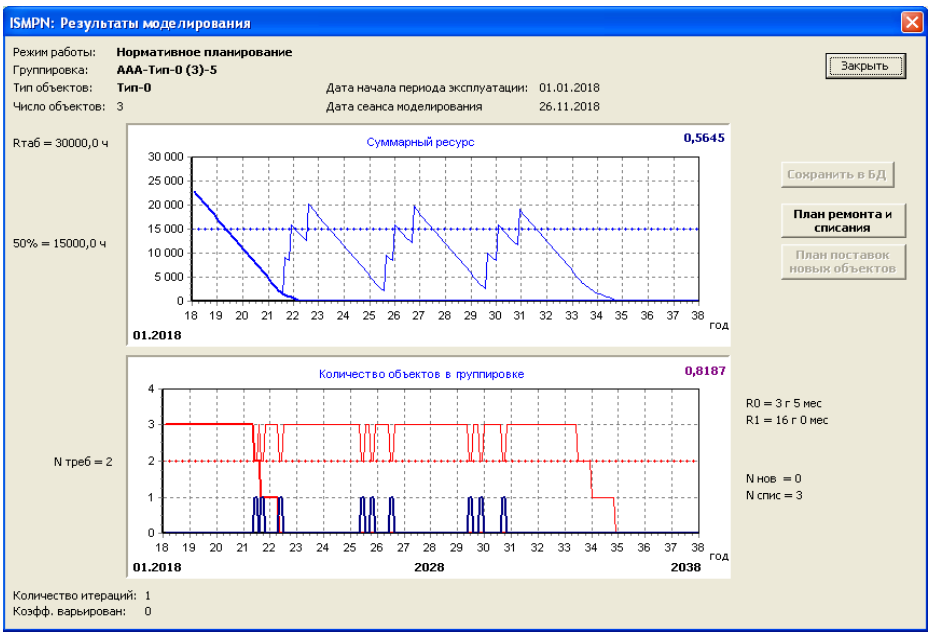
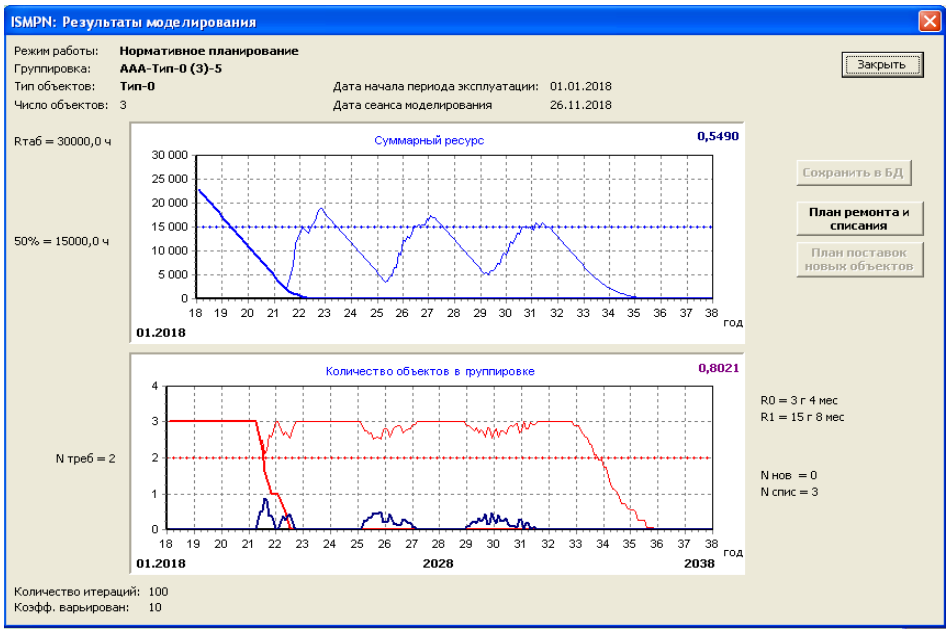


Рисунок 4 – Список вибору режимів прогнозування

На рис. 5 показана форма екрану ПК. одержувана після завершення процесу моделювання.



а) одна реалізація ($N_I = 1, KV_{\text{Lim}} = 0$)



б) 100 реалізацій ($N_I = 100, KV_{\text{Lim}} = 10\%$)

Рисунок 5 – Вигляд екрану ПК після завершення моделювання в режимі

Нормативне планування. На рисунку наведено два варіанти результатів моделювання: для 1 і для 100 реалізацій. Порівняння графіків функцій $\overline{N}_{\Sigma i}(t)$ та $\overline{R}_{\Sigma i}(t)$ для цих двох варіантів дозволяє оцінити приблизно вплив на вид графіків задаються значень N_I та Δ_η. Якщо на формі з результатами моделювання (рис. 5) клацнути ми-шию на кнопці «Показати план», відкриється форма з таблицею. У трьох крайніх справа шпальтах таблиці відображаються отримані в результаті моделювання нормативні планові дати відправлення в ремонт і списання об'єктів. Можна легко перевірити, що отримані планові дати точно відповідають графіками, показаним на рис. 6.

При бажанні зберегти згенерований варіант угрупування потрібно натиснути кнопку «Зберегти в БД». У цьому випадку після закриття форми у списку **Збережені варіанти** з'явиться рядок з найменуванням збереженого варіанту, як це показано на рис. 5.

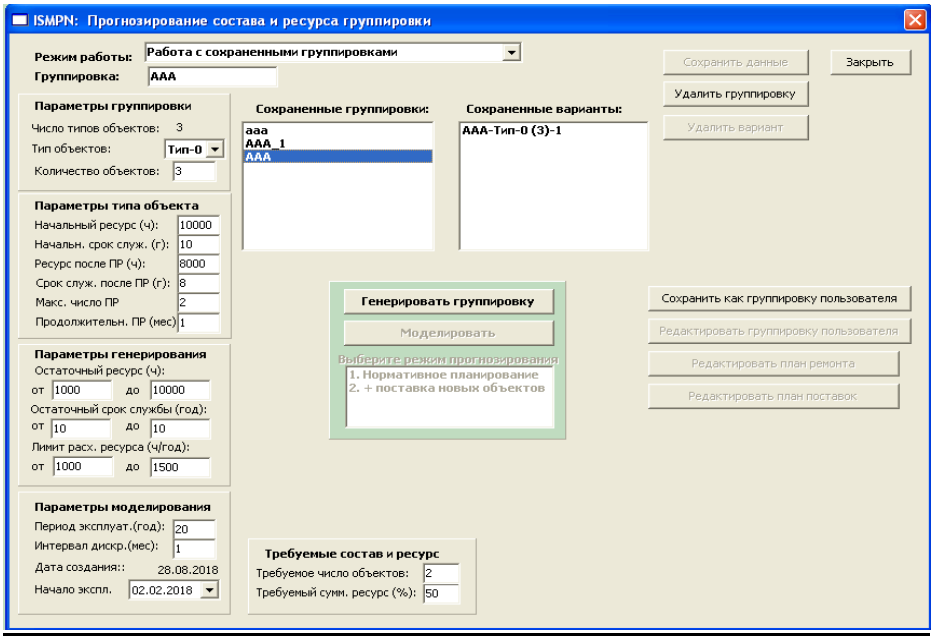


Рисунок 6 – Збережено варіант угрупування з'явився під ім'ям AAA-Тіп-0 (3) -1

Найменування збереженого варіанту автоматично формується за наступним правилом: ім'я угрупування- найменування типу об'єктів-кількість об'єктів в угрупуванні (в дужках) - порядковий номер варіанта. В подальшому це ім'я може бути змінено зручним для користувача чином. Для кожного зі збережених варіантів можна виконати повторне моделювання.

Для цього досить вибрати у списку збережених варіантів потрібний варіант, потім натиснути кнопку «Моделювати» і вибрати потрібний режим прогнозування. Результати моделювання відобразяться в такому ж вигляді, як це було вже показано на рис. 6.

Висновки

1. В роботі проведено прогнозування складу та ресурсу угрупування об`єктів військової техніки (ОВТ) та зроблено аналіз його варіантів.

2. Для того, щоб угрупування могло виконувати всі завдання у відповідності до свого призначення, воно повинно задовольняти встановленим вимогам за кількісним та якісним складом.

3. Кількісний склад угрупування визначається кількістю ОВТ різних типів, наявних в даний момент часу і готових до негайного виконання завдань.

4. Проаналізовано останні дослідження в даній предметній області, які наведено в великій кількості наукових робіт, що розв`язують проблему прогнозування складу та ресурсу угрупування об`єктів військової техніки, визначено, що єдиного комплексу досліджень не існує.

5. Математична модель процесу витрачання та поповнення ресурсу (ПВПР) угрупування розроблено методом імітаційного моделювання із застосуванням універсальної мови програмування процедурного типу.

6. Проведено прогнозування складу і ресурсу сучасних засобів ОВТ та їх угрупуванню. Поставки нових об'єктів моделюються в моменти часу, в які залишкова кількість працездатних об'єктів в угрупуванні знижується нижче допустимого значення.

7. Розроблено генерування варіантів угрупування ОВТ та зроблено нормативне планування.

ЛІТЕРАТУРА:

1. Lenkov E.S. The option for calculating the indicators of the needlessness of the unbelievable complex object of technique // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К., 2018. – № 59. – С.56 – 61.

2. Лєнков С.В., Толок І.В., Цицарєв В.М., Лєнков Є.С. Моделювання процесів витрачання та поповнення ресурсу угруповання технічних об'єктів // Журнал «Система озброєння і військова техніка» - Харків, – 2018. – №1(53). – С.155 – 162.

3. Ланецький Б.Н., Фролов А.Д., Борисенко К.В. Імовірнісна модель накопичення пошкоджень в елементах ракетного двигуна твердого палива зенітною керованою ракетою. Системи озброєння і військова техніка. – 2011. - №2(26). – С. 72 – 75.

4. Б.Н. Ланецький, Лукьянчук В.В., Артеменко А.А. Комплексное оценивание показателей безотказности и остаточной долговечности сложных технических систем, эксплуатируемых по техническому состоянию. Основные положения. Системи обробки інформації. – 2016. - №2(139). – С. 40 – 43.

5. Б.Н. Ланецкий, А.А. Артеменко. Обоснование выбора моментов проведения контроля предельного состояния РЭС ЗРК, эксплуатируемых по техническому состоянию Системи озброєння і військова техніка. — 2015. — № 2(42). – С. 119-121.

6. Гурба О., Шатров А., Шишанов М. Методологічні рекомендації щодо розподілу складових частин керованих авіаційних засобів ураження на групи зарівнями безпеки застосування та котролепригодності. Озброєння та військова техніка. – 2018. - №19. – К.: - С. 43-46.

7. Боряк К.Ф., Ленков С.В., Цыцарев В.Н. Моделирование и оптимизация процесса восполнения ресурса сложных объектов радиоэлектронной техники // Журнал «Інформатика та математичні методи в моделюванні». – Одеса, 2013. –Т.4., №2. - С.126 – 136.

8. Толок И.В. Определение системы технического обслуживания и ремонта автомобильной техники на предприятиях Министерства обороны Украины и ее критерии эффективности // Система управління, навігації та звязку. – К.: Центральний науково-дослідний інститут навігації і управління, 2008. – Вип.4(18). – С. 95 – 97.

9. Стрельников В.П. Новая технология исследования надежности машин и аппаратуры// Математические машины и системы, - К.: 2007. №3,4. С. 227 – 238.

10. Yu Zhou, Gang Kou, Hui Xiao, Yi Peng, FawazE.Alsaadi, "Sequential imperfect preventive maintenance model with failure intensity reduction with an application to urban buses", Reliability Engineering & System Safety, Volume 198, June 2020, 106871. https://doi.org/10.1016/j.ress.2020.106871.

11. Rui Zheng, BingkunChen, LiudongGu, "Condition-based maintenance with dynamic thresholds for a system using the proportional hazards model", Reliability Engineering & System GenadiyZhyrov et al., International Journal of Advanced Trends in Computer Science and Engineering, 9(4), July – August 2020, 5083 – 5088 5088 Safety, Volume 204, December 2020, 107123. https://doi.org/10.1016/j.ress.2020.107123.

12. Лєнков С.В., Толок І.В., Лєнков Є.С., Цицарєв В.М. Програмне забезпечення моделювання процесів витрачання і поповнення ресурсу угрупувань технічних об'єктів // Журнал «Наука і техніка Повітряних Сил ЗСУ. - Харків, – 2018. – Вип.3(32). – С. –120 -127. 16.

13. Лєнков С.В., Толок І.В., Лєнков Є.С., Банзак Г.В., Жиров Г.Б., Цицарєв В.М. Імітаційна статистична модель процесу технічного обслуговування і ремонту складної військової техніки. Частина 1. / Монографія на укр.м. – Одеса: Бондаренко М.О., 2019. – 132 с.

14. Жиров Г.Б., Лєнков Є.С., Толок І.В. Удосконалення алгоритм оптимізації процесу планового ремонту складних технічних об'єктів // Журнал «Сучасна спеціальна техніка», м.Київ, 2018. – №2(53). – С.23 – 28.

REFERENCES:

1. Lenkov E.S. (2018). The option for calculating the indicators of the needlessness of the unbelievable complex object of technique, Collection of Scientific Papers of the Military Institute, Kyiv, No. 59, pp. 56 – 61.

2. Lyenkov S.V., Tolok I.V., Cicaryev V.M. and Lyenkov Ye.S. (2018). Modelyuvannya procesiv vitrachannya ta popovnennya resursu ugrupovannya tehnichnih ob'yektiv, Sistemi ozbroyennya i vijskova tehnika, Harkiv, no. 1(53), pp. 155 – 162.

3. Laneckij B.N., Frolov A.D. and Borisenko K.V. (2011). Imovirnisna model nakopichennya poshkodzhen v elementah raketnogo dviguna tverdogo paliva zenitnoyu kerovanoyu raketoyu. Sistemi ozbroyennya i vijskova tehnika, no.2(26), pp.72 – 75.

4. Laneckij B.N., Lukyanchuk V.V. and Artemenko A.A. (2016). Kompleksnoe ocenivanie pokazatelej bezotkaznosti i ostatochnoj dolgovechnosti slozhnyh tehnicheskih sistem, ekspluatiruemyh po tehnicheskomu sostoyaniyu. Osnovnye polozheniya, Sistemi obrobki informaciyi, no. 2(139), pp. 40 – 43.

5. Laneckij B.N., Artemenko A.A. (2015). Obosnovanie vybora momentov provedeniya kontrolya predelnogo sostoyaniya RES ZRK, ekspluatiruemyh po tehnicheskomu sostoyaniyu, Sistemi ozbroyennya i vijskova tehnika, no. 2(42), pp. 119-121.

6. Gurba O., Shatrov A. and Shishanov M. (2018). Metodologichni rekomendaciyi shodo rozpodilu skladovih chastin kerovanih aviacijnih zasobiv urazhennya na grupi za rivnyami bezpeki zastosuvannya ta kotroleprigodnosti, Ozbroyennya ta vijskova tehnika, Kyiv, no. 19, pp. 43-46.

7. Boryak K.F., Lenkov S.V. and Cycarev V.N. (2013). Modelirovanie i optimizaciya processa vospolneniya resursa slozhnyh obektov radioelektronnoj tehniki, Informatika ta matematichni metodi v modelyuvanni, Odesa, Vol.4., no. 2, pp.126-136.

8. Tolok I.V. (2008). Opredelenie sistemy tehnicheskogo obsluzhivaniya i remonta avtomobilnoj tehniki na predpriyatiyah Ministerstva oborony Ukrainy i ee kriterii effektivnosti, Sistema upravlinnya, navigaciyi ta zvyazku, Kyiv, no. 4(18), pp. 95-97.

9. Strelnikov V.P. (2007). Novaya tehnologiya issledovaniya nadezhnosti mashin i apparatury, Matematicheskie mashiny i sistemy, Kyiv, no. 3,4, pp. 227-238.

10. Yu Zhou, Gang Kou, Hui Xiao, Yi Peng, FawazE.Alsaadi, “Sequential imperfect preventive maintenance model with failure intensity reduction with an application to urban buses”, Reliability Engineering & System Safety, Volume 198, June 2020, 106871. https://doi.org/10.1016/j.ress.2020.106871.

11. Rui Zheng, BingkunChen, LiudongGu, “Condition-based maintenance with dynamic thresholds for a system using the proportional hazards model”, Reliability Engineering & System GenadiyZhyrov et al., International Journal of Advanced Trends in Computer Science and Engineering, 9(4), July – August 2020, 5083 – 5088 5088 Safety, Volume 204, December 2020, 107123. https://doi.org/10.1016/j.ress.2020.107123.

12. Lyenkov S.V., Tolok I.V., Lyenkov Ye.S. and Cicaryev V.M. (2018). Programne zabezpechennya modelyuvannya procesiv vitrachannya i popovnennya resursu ugrupuvan tehnichnih ob’yektiv, Nauka i tehnika Povitryanih Sil ZSU, Harkiv, no.3(32), pp. 120 -127.

13. Lyenkov S.V., Tolok I.V., Lyenkov Ye.S., Banzak G.V., Zhirov G.B. and Cicaryev V.M. (2019). Imitacijna statistichna model procesu tehnichnogo obslugovuvannya i remontu skladnoyi vijskovoyi tehniki, Vol. 1, Odesa: Bondarenko M.O., 132 p.

14. Zhirov G.B., Lyenkov Ye.S. and Tolok I.V. Udoskonalennya algoritm optimizaciyi procesu planovogo remontu skladnih tehnichnih ob’yektiv, Suchasna specialna tehnika, Kiyiv, 2018, no. 2(53), pp. 23 – 28.

PhD Lenkov E.S.

FORECASTING THE COMPOSITION AND RESOURCE OF THE GROUP OF MILITARY EQUIPMENT OBJECTS AND ANALYSIS OF ITS OPTIONS

The paper forecasts the composition and resource of the grouping of military equipment (weapons) and analyzes its variants. Possible measures to replenish the composition and resources of the group may be the supply of new weapons to the group, as well as effective maintenance and repair. In order for the group to be able to perform all tasks in accordance with its purpose, it must meet the established requirements for quantitative and qualitative composition. The quantitative composition of the group is determined by the number of weapons of various types available at the moment and ready for immediate execution of tasks. The number of object types and their distribution by type must meet the specified requirements. To maintain the necessary efficiency of the group, it is necessary to replace new ones with new objects of appropriate types, or fundamentally new types, including foreign ones.

The last researches in the given subject area which are resulted in a large number of the scientific works solving a problem of forecasting of structure and a resource of grouping of objects of military equipment are analyzed. Analysis of its version of the complex in full does not actually exist. This necessitates the solution of scientific problems of forecasting the composition and resource of the grouping of military equipment and analysis of its options.

The mathematical model of the process of spending and replenishing the resource (PVPR) of the group was developed by the method of simulation modeling using a universal programming language of procedural type. This allows, on the one hand, to implement in the model all the essential subtleties of the modeling process and make the program compact, convenient for practical use.

Forecasting of the composition and resource of modern weapons and their groups has been carried out. The modes of normative planning of terms of repairs and write-off of objects modeled at the time of resource consumption are considered. Deliveries of new facilities are modeled at times when the residual number of operational facilities in the group falls below the allowable value. For new objects received in the group, PVPR is modeled in the usual way, just as for all other objects. Generation of options for armament grouping and normative planning have been developed. The name of the saved variant is automatically formed according to the following rule: name of grouping - name of type of objects - number of objects in grouping (in brackets) - ordinal number of variant. In the future, this name can be changed in a user-friendly way. You can re-simulate for each of the saved options.

Key words: forecasting of composition and resource of grouping, objects of military equipment, maintenance and repair, mathematical model, delivery of new objects, generation of variants of grouping.

УДК 621.396.967

к.військ.н., ст.досл. **Нікіфоров М.М.** (ВІКНУ)
к.військ.н., с.н.с. **Попков Б.О.** (ВІКНУ)
к.т.н., ст.досл. **Лоза В.М.** (ВІКНУ)
к.т.н., с.н.с. **Кульський О.Л.** (КНУ)
к.т.н. **Крихта В.В.** (КНУ)

DOI: https://doi.org/10.17721/2519-481X/2021/73-06

АНАЛІЗ ІСНУЮЧИХ СИСТЕМ ПАСИВНОЇ ДИСТАНЦІЙНОЇ РОЗВІДКИ НА ОСНОВІ СЕЙСМОАКУСТИЧНОГО МОНІТОРИНГУ

Робота пов'язана з проведенням аналізу існуючих систем пасивної розвідки щодо підвищення точності визначення координат об'єктів (цілей) противника та скорочення часу передачі даних. У теперішній час значно виріс обсяг завдань, які вирішує розвідка. Підвищилися вимоги щодо часу передачі даних і точності визначення координат об'єктів (цілей) противника. На перший план все гостріше висувається фактор часу, тобто крайнє скорочення циклу "виявлення – доповідь – відповідь". При цьому вимагається така точність визначення місцеположення противника, яка б дозволяла відразу наносити по ньому ураження. В більшості випадків, для дистанційної розвідки використовується декілька різнотипних систем, можливості яких доповнюють одна одну. Підтверджено що на даний час широке застосування знайшли системи, що побудовані на основі використання сейсмічних та акустичних датчиків отримання інформації. Проведений аналіз різнорідних систем розвідки дозволяє виділити сейсмоакустичні системи, якнайбільш ефективні для вирішення задач по виявленню та пеленгації позицій стріляючої артилерії та задачі визначення факту порушення кордону з подальшою ідентифікацією, за умови ведення військової розвідки. Обґрунтовується необхідність комплексного використання різноманітних систем дистанційної розвідки з різними фізичними властивостями дозволяє розширити їх область використання, а також зменшити вплив природних властивостей на якість результатів вимірювань.

Для вирішення поставлених завдань розвідки пропонується створити інтегровану пасивну систему моніторингу навколишнього простору зі сукупністю спільно функціонуючих сейсмо-акустичних та оптико-електронних датчиків, засобів зв'язку, обчислювальних і програмних засобів, засобів управління і індикації, призначених для отримання інформації про різного роду об'єктах, об'єднання інформації, що поступає, від датчиків і відображення результуючої інформації.

Ключові слова: пасивна розвідка, системи, сейсмоакустичний моніторинг, датчик.

Вступ. Під час активного розвитку систем дистанційної розвідки роль людини зводиться практично до мінімум. На заміну людини приходять сучасні, надійні засоби і системи охорони і ровідки небезпечних техногенних та військових об’єктів. Такі системи вимагають мінімум обслуговуючого персоналу та мінімум проведення робіт по обслугуванню та налаштуванню. Актуальність ролі систем дистанційної розвідки підвищується в період ведення державою бойових дій та активізації дій розвідувально-диверсійних підрозділів. В більшості випадків, для дистанційної розвідки використовується декілька різнотипних систем, можливості яких доповнюють одна одну.

Все це вимагає широкого впровадження у війська нових технічних засобів розвідки. Зростання обсягу завдань розвідки, з одного боку, і скорочення часу на їх виконання, з іншого, вимагають постійного удосконалення засобів та способів здійснення розвідки.

Завдання своєчасного виявлення та точної класифікації рухомих наземних об'єктів входить в число пріоритетних задач для сил розвідки, охорони важливих об’єктів та забезпеченні надійної безпеки об’єктів охорони та сухопутних кордонів.

Мета статті. Полягає в проведенні аналізу існуючих систем дистанційної розвідки та обґрунтуванні створення інтегрованої пасивної системи моніторингу навколишнього простору.

Основна частина. Розвідка є найважливішим видом забезпечення бойових дій військ, вона є сукупністю заходів усіх командирів і штабів із метою своєчасного отримання інформації про противника, місцевість, кліматичні і погодні умови в районі майбутніх бойових дій з метою найбільш ефективного застосування своїх сил і засобів щодо ураження противника. У теперішній час значно виріс обсяг завдань, які вирішує розвідка. Разом з тим терміни їх виконання суттєво скоротились. Підвищилися вимоги щодо часу передачі даних і точності визначення координат об'єктів (цілей) противника. Застосування противником нових далекобійних, високоточних, всепогодних засобів ураження, висока рухомість військ, мобільні й рішучі їх дії під час бою ставлять до розвідки підвищені вимоги, фактично розширюючи фазу активної дії розвідки до цілодобової. [1-3] Нині недостатньо тільки виявити противника. На перший план все гостріше висувається фактор часу, тобто крайнє скорочення циклу "**виявлення – доповідь – відповідь**". При цьому вимагається така точність визначення місцеположення противника, яка б дозволяла відразу наносити по ньому ураження. Одночасно і сам процес виявлення противника зазнав змін внаслідок застосування ним різноманітних засобів, як пасивних – приховування своїх дій, так і активних – проведення контррозвідувальних заходів.

Сейсмічні системи розвідки. Під сейсмічною розвідкою (СР) розуміється добування інформації шляхом виявлення і аналізу деформаційних та зсувних полів в земній поверхні, що виникають під впливом різних вибухів [1]. СР визначає: координати епіцентру вибуху, потужність і час вибуху, кількість вибухів в групі. Сейсмічний метод виявлення і ідентифікації ядерних вибухів отримав загальне визнання як один з основних, крім вибухів в космосі і в повітрі на великих висотах (понад декілька десятків кілометрів). Сейсмічний метод застосовний для виявлення ядерних вибухів як на малих, так і на великих відстанях, що досягають до 17 000 км [2].

Сейсмічна розвідка є складною високо інтегрованою та динамічною системою. У ній відбуваються процеси прийом і запис пружних коливань в точках спостереження, обробка і інтерпретація сейсмічних записів, найважливішими з яких є збудження сейсмічним джерелом первинних хвиль, поширення їх в геологічному середовищі з утворенням на неоднорідностях вторинних хвиль.

Історичні успіхи застосування сейсмодатчиків в розвідувально-сигналізаційних приладах (РСП), призначених для розвідки наземних рухомих об'єктів в першу чергу належать США. Висока ефективність застосування РСП привела до оснащення цими приладами збройних сил союзників США, а також до розробки їх аналогів у ряді інших країн. Типовими зразками таких автоматичних систем являються:

Система CLASSIC 2000 (фірма Thales, Франція). Система використовується в 42 країнах світу, включаючи 12 країн, що входять до складу НАТО. Сейсмічний датчик системи забезпечує виявлення людини в діапазоні від 1 до 80 метрів, а легкової машини – до 250 метрів;

Система REMBASS II (фірма L - 3 Communications - East, США). Система знаходиться на озброєнні сил спеціальних операцій, сухопутних військ і військово- повітряних сил США і Ізраїлю, успішно застосовувалася в Іраку і Афганістані. Комплексний датчик системи, що має сейсмічний і акустичний канали, забезпечує виявлення людини на дальності до 75 метрів, вантажного автомобіля - до 250 метрів, гусеничної машини - до 350 метрів;

Система Improved Air Delivered Sensor (IADS) (фірма Northrop Grumman Electronic Systems sector - ATE/Simulation, США), забезпечує виявлення як наземних, так і повітряних об'єктів. Наступний варіант системи IADS II додатково забезпечуватиме вимір координат і розпізнавання об'єктів;

Система SEMAG (фірма Hirtenberger AG, Австрія). Система включає сейсмічні і магнітометричні датчики і застосовується для виявлення танків і управління мінами. Ця система є прикладом широкого класу систем управління мінами і мінними полями [3].

Акустичні системи розвідки. Під акустичною розвідкою розуміється отримання інформації шляхом прийому і аналізу акустичних сигналів інфразвукового, звукового, ультразвукового діапазонів, що поширюються в повітряному середовищі від об'єктів розвідки

[4]. Акустична розвідка (АР) забезпечує отримання інформації, що міститься безпосередньо у виголошуваній або відтворній промові (акустична мовної розвідки), а також в параметрах акустичних сигналів, які є супутніми при роботі озброєння і військової техніки, механічних облаштувань оргтехніки і інших технічних систем (акустична сигнальна розвідка) [4].

Сухопутні війська зарубіжних країн широко використовують взаємодоповнюючі (комплексні) системи, що дозволяє ефективно вести розвідку і спостереження у будь-який час доби при будь-якій видимості і погоді.

Попри те, що деякі з існуючих РСП здатні виявляти літальні апарати, останнім часом підвищений інтерес проявляється до нових систем, спеціально сконструйованих для виявлення вертольотів і літаків на малих висотах. Такі системи вже з'явилися на озброєнні сухопутних військ США, Франції і Ізраїлю. До таких систем відносяться:

Американська система MANPAC - 100. Забезпечує виявлення, розпізнавання, визначення азимута і кута місця вертольотів, що летять низько, гвинтових літаків і дистанційно керованих безпілотних літальних апаратів (БЛА). Ця система у кінці 1990-х років проходила польові випробування і призначена для використання сухопутними військами в передових підрозділах протиповітряної оборони, озброєних переносними зенітними ракетними комплексами "Стингер" [3, 5].

Французька система HELISPOT (Balise Acoustique Classification Helicoptere). Система може застосовуватися як окрема акустична система або в групі для утворення "бар'єру" виявлення в широкому секторі. Вона формує пеленги на виявлені об'єкти і з вірогідністю забезпечує автоматичне розпізнавання десяти типів вертольотів, акустичні портрети яких закладені в облаштування системи. Інформація про тип і пеленг виявленого вертольоту передається вбудованим в систему ультракороткохвильовим (УКВ) передавачем на центральний процесор, що знаходиться на посту спостереження, який може одночасно приймати і обробляти дані від 16 систем. Система забезпечує виявлення легких вертольотів в нормальних погодних умовах на відстані 2 - 5 км, важких, - до 12 км (при сильному вітри - до 4 км), а також їх пеленгація з точністю від 2 до 20 град., залежною від відстані і умов [5].

Ізраїльська система HELISPOT. Вона включає акустичний прилад, що розміщується на землі або транспортному засобі. Система забезпечує виявлення, розпізнавання і пеленгацію вертольотів, що летять низько, та БЛА на дальності до 3 км з точністю до 3 град. Акустичний прилад включає мікрофон і класифікатор, що визначає тип цілі по спектру акустичного сигналу, що приймається. Інформація про виявлену ціль передається по УКВ радіоканалу або дротяній лінії зв'язку на пост збору розвідданих [5].

Ізраїльська система ROAD використовує акустичний прилад, що забезпечує виявлення середніх вертольотів на відстані 1 - 2 км, великих вертольотів - до 2,7 км, а також вертольотів що зависають на малих висотах - до 2,5-3 км [6].

Розглянуті системи використовують тільки акустичні хвилі, що поширюються в повітрі. В той же час експериментальні дослідження показують, що нарівні з акустичними хвилями можна ефективно використати і сейсмічні хвилі, що поширюються в землі. Комбінована обробка акустичних і сейсмічних хвиль може істотно підвищити ефективність розвідки. Акустичні хвилі, що поширюються в повітрі, приймаються акустичними мікрофонами, що перетворюють акустичний тиск в електричний сигнал. Аналогічно сейсмічні хвилі поширюються в поверхневому шарі землі і перетворяться сейсмічними датчиками в електричний сигнал, що відповідає коливанням ґрунту.

Поширення акустичних хвиль залежить від стану атмосфери, а поширення сейсмічних хвиль - від структури, складу і стану поверхневого шару землі.

Сейсмоакустичні системи розвідки. У сухопутних військах США на озброєнні знаходяться розвідувальне-сигналізаційні прибори (РСП) "Рембасс" (REmotely Monitored BAttlefield Sensor System - REMBASS) трьох поколінь [5]. Вони призначені для раннього виявлення, визначення місця розташування і ідентифікації наземних рухливих об'єктів і цілей, в першу чергу мобільних пускових установок оперативне-тактичних ракет, зенітних ракетних комплексів і бойових машин. Системи "Рембасс" усіх поколінь розгортаються в тактичній

глибині бойових порядків супротивника, а також у бойових порядках та тилу своїх військ. До їх складу входять РСП, радіоретранслятори, засоби прийому і обробки даних. Розвідувально-сигналізаційні прилади розгортаються на відстані 50-350 м один від одного на найбільш вірогідних напрямах руху мобільних об'єктів (дороги, переправи та ін.). Вони можуть встановлюватися як вручну, так і за допомогою авіації, і артилерії. Кожен РСП включає датчик, радіопередавач, електронний блок і акумуляторну батарею. Деякі прилади можуть бути забезпечені пристроями самоліквідації і фотоелементами для їх включення тільки в темний час доби.

Сейсмічні датчики уловлюють коливання ґрунту, рухи людини, що відбуваються в результаті його руху - до 75м. та транспортного засобу - до 350м. В якості чутливих елементів в них використовуються заглиблені у ґрунт геофони. Дальність дії цих приладів залежить від рівня і характеру фону навколишнього сейсмічного шуму і типу ґрунту.

На озброєнні ЗС Росії знаходиться комплекси розвідувальне-сигналізаційних засобів 1К18 "Реалія", який призначений для дистанційного виявлення пересування особового складу (до 70 м.) та техніки (до 500 м.) у тилу супротивника і на границях вірогідного зіткнення з ним та передачі відомостей про виявлені об'єкти по радіоканалу в масштабі часі, близькому до реального.

Малогабаритна розвідувально-сигналізаційної апаратура 1К124 " Табун" призначена для дистанційного виявлення пересування особового складу - до 50 м. та техніки - до 200 м.

Британська переносна система дистанційного спостереження Tobias має вагу без батареї живлення 6,35 кг і 80 сейсмічних датчиків (вага кожного 0,075 кг), що сполучаються дротами. Дальність виявлення людини, що рухається, до 300 метрів, а сама система перекриває простір радіусом 2,4 км [7].

Подальшим розвитком принципів об'єднання даних, що характеризують окремі об'єкти спостереження, є ідея "поєднання датчиків". Термін "поєднання датчиків" визначається також як "злиття розвідувальних даних" (intelligence fusion).

Поєднання датчиків припускає інтеграцію і аналіз даних від засобів виявлення і є процесом збору і узагальнення даних за визначенням місця розташування і ідентифікації, отриманих від різних датчиків (видовій інформації, РЛС, розпізнавання сигналів (Signal Intelligence SIGINT), виявлення руху), в цілях отримання єдиної комплексної картини навколишнього оточення. Поєднання датчиків, в процесі якого обробляються дані, що поступають від різних джерел, спрямоване на отримання точнішій, надійнішій і повнішій інформації в порівнянні з інформацією, що отримується від окремого джерела індивідуально. Під інтегрованою системою моніторингу (ІСМ) навколишнього простору розуміють сукупність спільно функціонуючих датчиків, засобів зв'язку, обчислювальних і програмних засобів, засобів управління і індикації, призначених для отримання інформації про різного роду об'єктах, об'єднання інформації, що поступає, від датчиків і відображення результуючої інформації. Найважливішу роль в ІСМ грають інформаційні датчики, тактико-технічні характеристики яких визначають можливості високоефективного функціонування [8].

Інша ситуація може складатися з отриманням відомостей про стан об'єктів або процесів на великій території при обмеженій дальності дії інформаційних датчиків. В цьому випадку доводиться об'єднувати інформацію, що поступає від просторово рознесених датчиків, сукупна зона огляду яких забезпечує перекриття усієї площі території, що контролюється. Найбільш складним є поєднання датчиків в системах геопросторової розвідки (Geospatial Intelligence Systems - GIS), що представляють важливий інструмент ведення бойових дій. Прикладом такої системи є мережева розвідувальна система Imilite ізраїльській компанії Rafael Advancend Defence Systems [9]. Система призначена для використання декількох видових датчиків, отримання і обробки даних в уніфікованому виді для поширення користувачам і клієнтам.

Поєднання датчиків сприяє збільшенню чіткості зображень. Зокрема, коли використовується тільки один тип датчика, то при його функціонуванні в умовах поганої

погоди або дії несприятливих чинників, обумовлених веденням бойових дій, отримання чіткого зображення може виявитися неможливим [10].

Проведений аналіз різнорідних систем розвідки дозволяє виділити сейсмоакустичні системи, як найбільш ефективні для вирішення задач по виявленню та пеленгації позицій стріляючої артилерії та задачі визначення факту порушення кордону з подальшою ідентифікацією, за умови ведення військової розвідки. Дане твердження базується на тому, що сейсмоакустичні системи володіють наступними перевагами, вони забезпечують стійке автоматичне функціонування: в складних метео умовах (дощ, сніг, туман); в умовах поганої оптичної видимості (ніч); в напрямках на джерела яскравого світла (сонце); в умовах сильної задимленості і запиленості; в умовах порізаного рельєфу місцевості (пагорби, гірські перевали, ущелини, русла річок та інше). Сейсмоакустичні системи мають повну скритністю, так як не формують зондуючих сигналів, це виключає їх завчасне виявлення. Найважливішим якістю цих систем є збереження працездатності в умовах сучасного радіоелектронного придушення. Такі системи мають малі габарити, низьке енергоспоживання і краще у порівнянні з іншими системи (радіолокаційними, оптико-електронними та ін.) відповідають критеріям «ефективність - вартість» [11].

Використання трьох різнорідних інформаційних потоків значно зменшує похибку при визначенні координат цілі. Зокрема, використання ресурсів такої системи дає суттєву основу для розробки нових способів застосування як озброєння, так і підрозділів. Таким чином, для вирішення поставлених завдань розвідки пропонується створити інтегровану пасивну систему моніторингу навколишнього простору зі сукупністю спільно функціонуючих сейсмо-акустичних та оптико-електронних датчиків, засобів зв'язку, обчислювальних і програмних засобів, засобів управління і індикації, призначених для отримання інформації про різного роду об'єктах, об'єднання інформації, що поступає, від датчиків і відображення результуючої інформації.

Розвиток сучасних технологій, засобів обробки інформації дозволяють зробити ще один крок у вдосконаленні практики застосування систем озброєння, зокрема виробити нові концептуальні підходи, щодо створення єдиної інформаційної розвідувальної системи.

Висновки

1. У даній статті проведено аналіз існуючих різнорідних систем пасивної розвідки та визначені оптимальні, найбільш ефективні системи, для вирішення задач ведення військової розвідки.
2. Розглянуто сейсмоакустичні системи, як найбільш ефективні для вирішення задач по виявленню та пеленгації позицій стріляючої артилерії та задачі визначення факту порушення кордону охорони з подальшою ідентифікацією.
3. Запропоновано створити інтегровану пасивну розвідувально-інформаційну систему моніторингу, що володіє широкими можливостями для вирішення різноманітних завдань військового призначення.

ЛІТЕРАТУРА:

1. Волчихин В.И., Дудкин В.А., Панков А.А. Об использовании комбинирования акустических и сейсмических принципов обнаружения наземних обэктов. «Надежность и качество», 2011 - cyberleninka.ru https://cyberleninka.ru/.../ob-ispolzovanii-kombinirovaniya
2. Д. В. Зайцев, А. П. Наконечний, С. О. Пахарєв, І. О. Луценко Військова розвідка: навчальний посібник. Київський університет, 2016. – 335 с
3. Ерохин Е.И., Чабанов В.А. Современные средства воздушной разведки и наблюдения США. Научно-техн. информация. Сер. Авиационные системы. – 2014. – №6. – С.18–35.
4. Красильников В.А, Крылов В.В. Введение в физическую акустику: учебное пособие Под ред. В.А. Красильникова. - М: Наука. Главная редакция физико-математической литературы, 1984. – 400 с
5. Мосалев В. Системы дистанционного наблюдения за полем боя на базе разведывательно-сигнализационных приборов / Зарубежное военное обозрение. – 2000. – № 2. – С. 21–27.
6. Averbuch A., Zheludev V., Rabin N., Schclar A. Wavelet based acoustic detection of moving vehicles. School of Computer Science Tel Aviv University, Tel Aviv 69978, Israel March 11, 2007.

7. Верба В.С. Интеграция данных в многодатчиковых бортовых информационно- управляющих системах. В.С. Верба, В.И. Меркулов, Е.В. Попов, В.С. Чернов. Информационно- управляющие системы. 2014. – № 2. – С.32-43.

8. Нікіфоров М.М., Пампуха І.В., Щербіна С.В., Шевцов А.Г., Лоза В.М. Особливості використання автоматизованого сейсмоакустичного комплексу за допомогою комбінованого способу виявлення об'єктів. Геофізичний журнал. Інституту геофізики ім. С. І. Субботіна НАН України. 2018 - №6, т. 40 с.150-158.

9. The Military and Civil Aviation Passive Radar Market: 2013 – 2023/ http://www.researchandmarkets.com/reports/2598562/the_military_and_civil_aviation_passive_radarpos-0.

10.Лепіх Я.І., Гордієнко Ю.О., Дзядевич С.В., Ленков С.В., Дружинін А.О., Євтух А.А., Мельник В.Г., Романов В.О. (2010) Створення мікроелектроних датчиків нового покоління для інтелектуальних систем. Монографія. Одеса. Астропрінт, 2010 - 296 С.

11.Щербина С.В., Фещенко А.І., Ільєнко В.А., Лукіянчук А.А., Кривицький ГВ., Пампуха І.В., Боровська О.Г., Охрамович М.М., Нікіфоров М.М., Лоза В.М., Савков П.А. Автоматизована комплексна система для детекції координат військових та техногенних об'єктів. 2018. Patent, no. u201709127.

REFERENCES:

1. Volchihin, V.I., Dudkin, V.A., Pankov, A.A., (2011) *Ob ispol'zovanii kombinirovaniya akusticheskih i sejsmicheskih principov obnaruzheniya nazemnih obehktov*. [About the use of combination of acoustic and seismic principles of detection of ground objects]. Nadezhnost' i kachestvo. https://cyberleninka.ru/.../ob-ispolzovanii-kombinirovaniya (Accessed 3 November 2021).

2. Zajcev D. V., Nakonechnyj A. P., Pakharjev S. O., Lucenko I. O. (2016) Vijsjkova rozvidka : navchaljnyj posibnyk. [Military intelligence] Kyjivsjkyj universytet, 335 P.

3. Erohin, E.I., Cнabanov, V.A., (2014) *Sovremennye sredstva vozdushnoj razvedki i nablyudeniya USA*. [Modern means of aerial reconnaissance and surveillance of the USA.]. Nauchno-tekhn. informaciya. Ser. Aviacionnye sistemy. Minsk. no 6, pp. 18-35.

4. Krasilnikov V.A, Krylov V.V. (1984) *Vvedenie v fizicheskuyu akustiku* [Introduction to physical acoustics] uchebnoe posobie. Glavnaya redaktsiya fiziko-matematicheskoy literatury, 400 P.

5. Mosalev, V., (2000) *Sistemy distancionnogo nablyudeniya za polem boya na baze razvedyvatel'no-signalizacionnyh priborov*. [Remote monitoring systems for the battlefield based on reconnaissance and signaling devices]. Zarubezhnoe voennoe obozrenie. no 2, pp. 21 - 27.

6. Averbuch, A., Zheludev V., Rabin N., Schclar A., (2007) Wavelet based acoustic detection of moving vehicles. School of Computer Science Tel Aviv University, Israel. https://www.cs.tau.ac.il/~amir1/PS/Acoustics2.pdf. (Accessed 3 November 2021)

7. Verba V.S., Merkulov V.I., Popov Ye.V., Chernov V.S. (2014*) Integratsiya dannykh v mnogodatchikovykh bortovykh informatsionno-upravlyayushchikh sistemakh*. [Data integration in multi-sensor on-board information and control systems] Informatsionno-upravlyayushchie sistemy. n. 2. pp. 32-43.

8. Nikiforov M.M., Pampukha I.V., Shherbina S.V., Shevcov A.Gh., Loza V.M. (2018) *Osoblyvosti vykorystannja avtomatyzovanogho sejsmoakustychnogho kompleksu za dopomoghoju kombinovanogho sposobu vyjavlennja ob'jektiv*. [Features of using an automated seismic acoustic complex using a combined method of object detection.] Gheofizychnyj zhurnal. Instytutu gheofizyky im. S. I. Subbotina NAN Ukrajiny. no 6, t. 40 pp.150-158.

9. The Military and Civil Aviation Passive Radar Market: (2013) – 2023/ http://www.researchandmarkets.com/reports/2598562/the_military_and_civil_aviation_passive_radar#pos-0/ (Accessed 3 November 2021).

10.Lepikh Ja.I., Ghordijenko Ju.O., Dzjadevych S.V., Lenkov S.V., Druzhynin A.O., Jevtukh A.A., Meljnyk V.Gh., Romanov V.O. (2010) Stvorennja mikroelektronykh datchykiv novogho pokolinnja dlja intelektualjnykh system. [Development of a new generation of microelectronic sensors for intelligent systems.] Monoghrafija. Odesa.Astroprint, 296 P.

11.Sherbina, S. V., Feshchenko, A. I., Il'єnko, V. A., Lukiyanchuk, A. A., Krivic'kij, G. V., Pampuha, I. V., Borovs'ka, O. G., Ohramovich, M. M., Nikiforov, M. M., Loza, V. M., Savkov, P. A. (2018). Avtomatizovana kompleksna sistema dlya detekciї koordinat vijs'kovih ta tekhnogennih ob'єktiv. [Automated complex system for detecting the coordinates of military and technogenic objects]. Patent, no. u201709127.

PhD Nikiforov M.M., PhD Popkov B.O., PhD Loza V.M.,
PhD Kulsky O.L., PhD Krykhta V.V.

ANALYSIS OF EXISTING PASSIVE REMOTE INTELLIGENCE SYSTEMS BASED ON SEISMOACOUSTIC MONITORING

The work is related to the analysis of existing passive intelligence systems to improve the accuracy of determining the coordinates of objects (targets) of the enemy and reduce the time of data transmission. At present, the volume of intelligence tasks has grown significantly. The requirements for data transmission time and accuracy of determining the coordinates of enemy objects (targets) have increased. The time factor, ie the extreme reduction of the "detection - report - response" cycle, is becoming more and more acute. This requires such accuracy in determining the location of the enemy, which would immediately defeat him. In most cases, several types of systems are used for remote reconnaissance, the capabilities of which complement each other. It is confirmed that currently built systems based on the use of seismic and acoustic sensors to obtain information. The analysis of heterogeneous reconnaissance systems allows to identify seismic acoustic systems that are most effective for solving problems of detection and direction finding of firing artillery positions and the task of determining the fact of border violation with subsequent identification, subject to military reconnaissance. The necessity of complex use of various systems of remote reconnaissance with various physical properties is substantiated allows to expand their field of use, and also to reduce influence of natural properties on quality of results of measurements.

To solve the tasks of intelligence, it is proposed to create an integrated passive system for monitoring the surrounding space with a set of jointly functioning seismic-acoustic and optoelectronic sensors, communications, computing and software, controls and indications designed to obtain information about various types of information. projects, combining incoming information from sensors and displaying the resulting information.

Key words: passive reconnaissance, systems, seismic acoustic monitoring, sensor.

УДК 621.391.3

Dulia O.O. (Igor Sikorsky Kyiv Polytechnic Institute)
PhD **Minochkin D.A.** (Igor Sikorsky Kyiv Polytechnic Institute)

DOI: https://doi.org/10.17721/2519-481X/2021/73-07

METHODS OF THE PUBLIC-KEY BASED AUTHENTICATION IN THE INTERNET OF THINGS

The Internet of Things (IoT) is a modern paradigm where everyday objects are interconnected and communicate with each other over the Internet. IoT facilitates the direct integration of physical objects with the cyber world through intelligent sensors, RFID tags, smartphones and wearable devices. IoT networks offer a variety of application areas, covering environmental monitoring, healthcare, smart cities, military aviation, and intelligent transportation systems. The number of devices open to the public network is gradually increasing; devices have a direct interaction with the physical world to collect data. Currently, one of the most debatable problems in the development of post-NGN communication networks is the problem of identifying the Internet of Things devices. Modern anonymization methods and the supposed large number of Internet of Things devices connected to the public communications network make modern communication systems vulnerable to intruders. The vulnerability of security consists in the impossibility of authentication of the Internet of Things devices, which opens the possibility for attackers to manufacture counterfactual physical and virtual products.

This situation requires secure solutions to prevent private information leakage and malicious activation through peer-to-peer authentication and secure data transfer between IoT nodes and servers. However, the existing structure and IP-based IoT primitives are not fully developed with resource-constrained IoT devices (such as power consumption, computational resource, communication ranges, RAM, FLASH, etc.). As a result, lighter solutions are needed to ensure security on IoT devices with limited resources.

Objective is to create a public-key based authentication method for IoT system that will be more optimized and secure than methods which already used for the Internet of Things. During the work process most of the existing methods of the public-key based authentication have been analyzed. Based on this analysis was proposed an authentication method that combines existing methods with improved cryptography algorithm.

Keywords: IoT, Interent of Things, authentication, cryptography, public-key, internet.

Introduction. The Internet of Things (IoT) is a modern paradigm where everyday objects are interconnected and communicate with each other over the Internet. IoT facilitates the direct integration of physical objects with the cyber world through intelligent sensors, RFID tags, smartphones and wearable devices [1]. IoT networks offer a variety of application areas, covering environmental monitoring, healthcare, smart cities, military aviation, and intelligent transportation systems. The number of devices open to the public network is gradually increasing; devices have a direct interaction with the physical world to collect data.

Currently, one of the most debatable problems in the development of post-NGN communication networks is the problem of identifying the Internet of Things devices. These problems are stipulated by the impossibility of detection and control of IP devices by modern methods used to find devices in the public communications network (PCN). Modern anonymization methods and the supposed large number of Internet of Things devices connected to the PCN make modern communication systems vulnerable to intruders. The vulnerability of security lies in the impossibility of authentication of the Internet of Things devices, which opens the possibility for attackers to manufacture counterfactual physical and virtual products.

This situation requires secure solutions to prevent private information leakage and malicious activation through peer-to-peer authentication and secure data transfer between IoT nodes and servers. However, the existing structure and IP-based IoT primitives are not fully developed with

resource-constrained IoT devices (such as power consumption, computational resource, communication ranges, RAM, FLASH, etc.) [2]. As a result, lighter solutions are needed to ensure security on IoT devices with limited resources.

Formation of the problem. There are several types of public-key based authentication methods that can be used for IoT devices but we should relay to the fact that IoT devices are really resources limited. The methods of authentication with large mathematical operations can cause the IoT device or sensor to malfunction. And it's a really big problem since the sensor needs to do a high resource loading operation before each data sending to the server and while it will be doing this the main data processing will be blocked which leads to losing data.

By analyzing existing public-key based authentication methods we need to find the best solution that can be applied to IoT devices depending on the limitations. This method should have a high security level and be lightweight.

Analysis of previous studies. One of the first examples of symmetric cryptography is presented in [3]. A symmetric-key system is used to provide confidentiality of messages in transmission, storing, and processing. The symmetric-key algorithm performs the operations of encryption/decryption based on a single key that is shared by two or more parties. Unlike [3 - 4] argues that there is a difficulty in symmetric cryptography; unsecure delivery of the key from the encoder to the decoder(s) can introduce a security risk. Anyone who gains access to the symmetric key can access/modify/send the message without the recipient's knowledge that the message has been modified.

Authors in [4] argue that the symmetric key algorithms are quite efficient, but the key distribution is difficult to IoT end devices. The key distribution requires a secure connection between the key distribution server and the IoT nodes. Public-Key Cryptography (PKC) and asymmetric cryptography are two effective ways of providing confidentiality and authentication.

The author of [5] has also found that this method of cryptography is difficult for IoT end devices. However, researchers have concluded that the RSA is a relatively slow algorithm for encryption however it is commonly used to pass encrypted shared keys for symmetric key cryptography. Since RSA encryption is an expensive operation, in IoT it is rather used in combination with symmetric cryptography.

As we know from [6] in the IoT environment, the general public-key problem is the requirement of an authenticated exchange of public keys. The PKI consists of components to securely distribute public keys and is widely used in the traditional Internet. The most important aspect of the PKI is a trusted third party who signs the identifier of an entity with its private key.

But PKI also has cons, as reported by [7] and [8], when PKI comes to very resource-constrained devices in the IoT, for most current deployments there is either no security at all or security that is based on shared keys or pins/passwords. It means that the risk of hacker attacks and eavesdropping is huge. As we are getting more and more dependent on the IoT, this risk is not acceptable.

Security in IoT implementations must be a critical component either during the device design and manufacturing phase or during the initialization phase or a product update. Previous studies indicate that there is no method of public-key-based authentication which will fit best in all situation, it depends on the performance of the devices. All of these methods, presented in the review, have pros as well as cons. The purpose of the study is to find a way to combine symmetric and asymmetric cryptography in order to achieve the best results, so that we can compensate for different method's shortcomings. Theoretically, this combined method will have good security enough in most cases and will fit most Internet of Things end devices.

Main part. Symmetric encryption (Fig. 1) is used to ensure the confidentiality of the message during its transmission, storage, and processing [3]. The symmetric key algorithm performs encryption/decryption operations based on a single key used by two or more parties. The difficulty in symmetric cryptography is the secure delivery of the key from the encoder to the decoder, which can create a security risk. Anyone who accesses the symmetric key can access/modify/send the message without the recipient knowing that the message has been modified. To address these issues, public-key encryption has been developed.

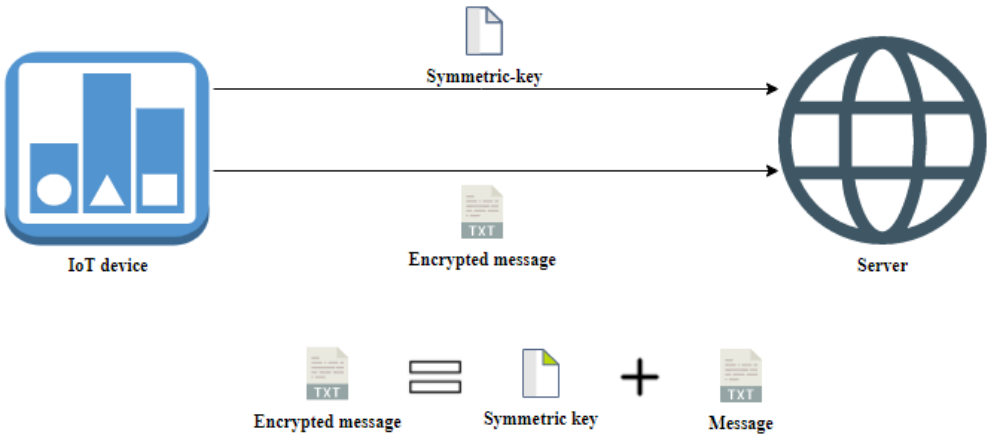


Figure 1 - Authentication method with symmetric cryptography

In symmetric-key encryption, the secret key S, the text message T and the encrypted text E of have the same length. For example, in AES 128 (Advanced Encryption Standard), the length of S, T, E is 128 bits (16 bytes), and encryption and decryption operations consist of XORing, permutations, bit offset, and linear mixing functions, which are performed in a known order. In general, the original plain text is divided into several blocks of fixed length:

$$E_i = Encrypt\ (S, T_i) \tag{1}$$

The weakness of symmetric cryptography is that the same blocks of plain text lead to the same cipher blocks. This is especially important for packages with a known format and a repeating pattern in the payload. To introduce randomness into cipher blocks and make decryption attacks difficult, you can use a Cipher Block Chaining (CBC), where before encoding each block of plain text is an exclusive operation (XORed) with the previous cipher block [9].

Asymmetric encryption or Public-Key cryptography (Fig. 2) always uses two different keys - private and public [10]. However, they are always generated as a linked pair. The private key always remains with the sender, while the public key is transmitted over an insecure channel to the receiving party [4]. The public key can be used to encrypt messages that can only be decrypted with the associated private key. The private key can generate an electronic signature that allows the recipient to uniquely identify the sender using the associated public key.

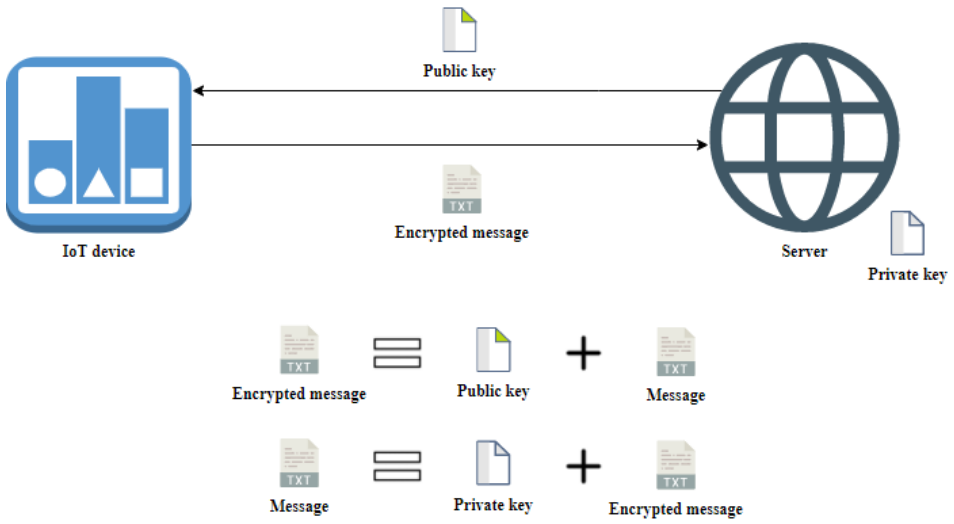


Figure 2 - Authentication method with asymmetric cryptography

Symmetric key algorithms are quite efficient, but key transfer is quite complex for IoT end devices. Key distribution requires a secure connection between the key distribution server and the IoT nodes. Public-key cryptography (PKC) is an effective way to ensure confidentiality and authentication [4]. Unlike symmetric encryption, asymmetric encryption is based on the idea of using one-way mathematical functions. They should be as simple as possible to calculate, but it is very difficult for them to do the reverse calculation. Since the constant increase in computing power improves the ability of computers to compute complex reversing functions, keys must be of appropriate length for proper security. Currently, 2048-bit keys such as RSA 2048 are classified as secure. Since encryption and decryption rates decrease as key lengths increase, asymmetric methods are only practical for processing small amounts of data.

As we see from [5] it also has been found that this method of cryptography is difficult for IoT end devices. It's because of a relatively slow speed of The RSA algorithm for encryption and that's the reason why it is commonly used to pass encrypted shared keys for symmetric key cryptography. Since RSA encryption is an expensive operation, in IoT it is rather used in combination with symmetric cryptography.

The problem with using public-key cryptography is the certainty/proof that a certain public key is genuine. It is correct and belongs to the declared person or legal entity, and has not been changed or replaced by an attacker or a third party. The usual approach to solving the problem is to use a PKI in which one or more third parties, known as a Certification Authority (CA), certify ownership of the key pairs.

A Public-Key Infrastructure (PKI) (Fig. 3) is a set of roles, policies, and procedures required to create, manage, distribute, use, store, and revoke digital certificates, and manage public-key encryption [11]. In the IoT environment, a common public key problem is the requirement for authenticated public key exchange. PKI consists of components for reliable public key distribution. The most important thing in PKI is a trusted third party that signs the entity ID with its private key.

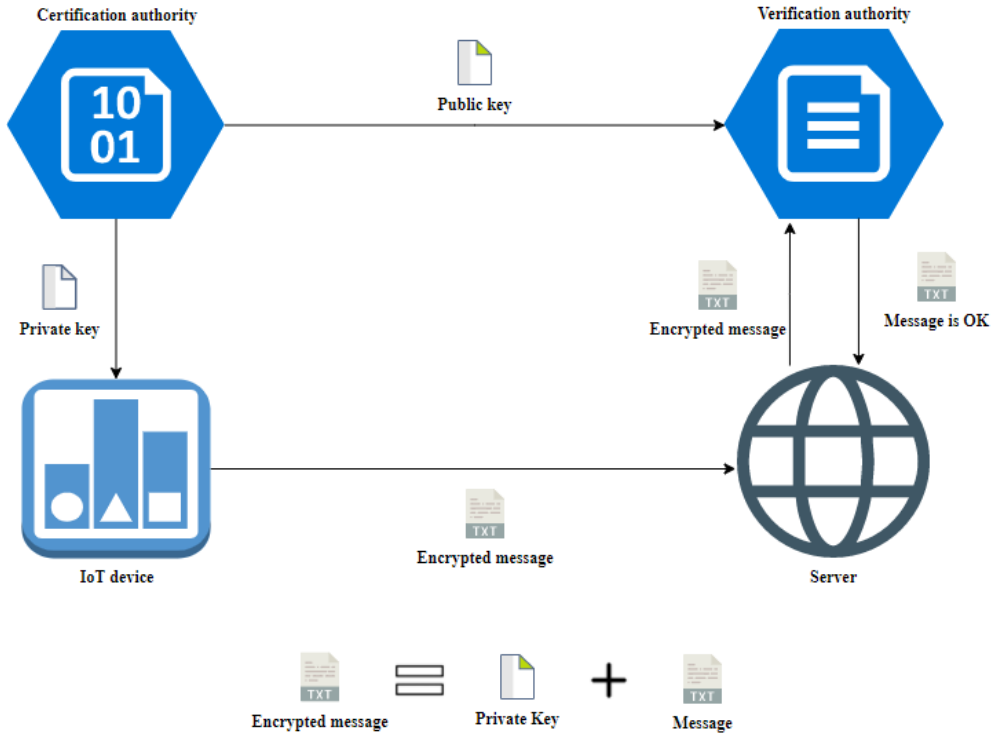


Figure 3 - Authentication method with public-key infrastructure

As we know from [6] in the IoT environment, the general public-key problem is the requirement of an authenticated exchange of public keys. The PKI consists of components to securely distribute

public keys and is today widely used in the traditional Internet. The most important part of the PKI is a trusted third party who signs the identifier of an entity with its private key.

But PKI also has cons, as reported by [8] and [12], when PKI comes to very resource-constrained devices in the IoT, for most current deployments there is either no security at all or security that is based on shared keys or pins/passwords. It means that the risk of hacker attacks and eavesdropping is huge. As we are getting more and more dependent on the IoT, this risk is not acceptable.

Proposed solution. We already know that symmetric cryptography has very good performance, which is exactly what we need to use it with resource-limited devices and sensors of the Internet of Things, but there is a drawback in the form of an insecure transmission of a single symmetric key. On the other hand, we have asymmetric cryptography, which has very good protection against hacking, but has algorithms that are difficult to calculate, which limits its use with devices of the Internet of Things. We propose a solution to combine these methods for maximum performance and security.

In the proposed solution, asymmetric cryptography is used only once when communicating between IoT devices in order to encode a symmetric key. For asymmetric cryptography, the Elliptical curve cryptography (ECC) algorithm was chosen, which provides the smallest key size, which provides good performance for IoT devices. Symmetric cryptography will be used for the main communication between devices and the server, using asymmetric cryptography to encrypt the symmetric key, we get rid of the most important disadvantage of symmetric cryptography, namely, the secure transfer of the key from the device to the server. The general scheme of work of my solution is shown in the Fig 4.

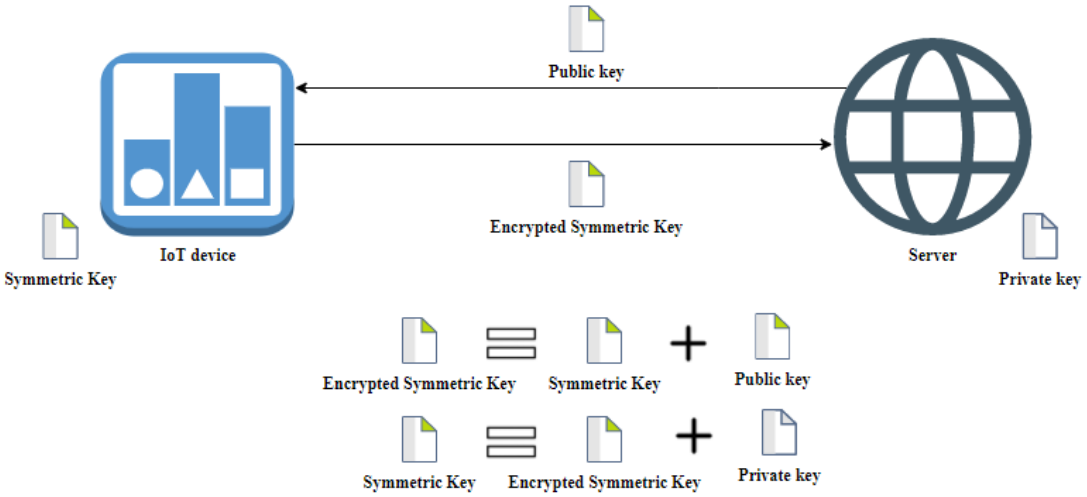


Figura 4 - Proposed solution, work algorithm

Conclusions. The proposed solution has good performance and is suitable for use in resource-limited devices and sensors of the Internet of Things, which is achieved by using asymmetric cryptography only for encrypting the symmetric key, as well as using the EEC algorithm, also the solution has required level of security, since the main drawback of symmetric encryption has been fixed. This solution can be used both for home devices and sensors as well as for industrial devices of the Internet of Things.

REFERENCES:

1. Zhao, Guanglei & Wang, Jingcheng & Luo, Jian & Long, Xiao & Si, Xianping. (2011). Applicability of Elliptic Curve Cryptography on Internet of Things. Energy Procedia. 11. 128-133. 10.1016/j.egypro.2011.10.220.

2. Singh, Deepti, et al. "A Secure IoT-Based Mutual Authentication for Healthcare Applications in Wireless Sensor Networks Using ECC." IJHISI vol.16, no.2 2021: pp.21-48. http://doi.org/10.4018/IJHISI.20210401.oa2

3. Rao U.H., Nayak U. (2014) Cryptography. In: The InfoSec Handbook. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4302-6383-8_8

4. Baldimtsi, F., Kiayias, A. and Samari, K. (2021), Watermarking public-key cryptographic functionalities and implementations: The case of encryption and signatures. IET Inf. Secur, 15: 205-222. https://doi.org/10.1049/ise2.12013

5. Z. Li, H. Zhao, X. Su and C. Wan, "Asymmetric Cryptography Based Unidirectional Authentication Method for RFID," 2018 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Zhengzhou, China, 2018, pp. 374-3743, doi: 10.1109/CyberC.2018.00073.

6. Marino, Francesco & Moiso, Corrado & Petracca, Matteo. (2019). PKIoT: A public key infrastructure for the Internet of Things. Transactions on Emerging Telecommunications Technologies. 30. 10.1002/ett.3681.

7. Vulić, I., Prodanović, R., Vukčević, G., Sretenović, S. Trust Establishing Model in IoT using PKI and Timestamp. In: Konjović, Z., Zdravković, M., Trajanović, M. (Eds.) ICIST 2018 Proceedings Vol.2, pp.333-338, 2018

8. Won, Jongho & Singla, Ankush & Bertino, Elisa & Bollella, Greg. (2018). Decentralized Public Key Infrastructure for Internet-of-Things. 907-913. 10.1109/MILCOM.2018.8599710.

9. Baldimtsi, F., Kiayias, A., Samari, K.: Watermarking public-key cryptographic functionalities and implementations. ISC 2017, 173– 191 (November 2017)

10. El. Gamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. CRYPTO 1985., 10– 18 (1985)

11. Gope P. Hwang T. (2016). A Realistic Lightweight Anonymous Authentication Protocol for Securing Real-Time Application Data Access in Wireless Sensor Networks.IEEE Transactions on Industrial Electronics, 63(11), 7124–7132. 10.1109/TIE.2016.2585081

12. Watro R. Kong D. Cuti S. F. Gardiner C. Lynn C. Kruus P. (2004, October). TinyPK: securing sensor networks with public key technology. In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (pp. 59-64). ACM.10.1145/1029102.1029113

Дуля О.О., к.т.н., с.н.с. Міночкін Д.А.

МЕТОДИ АВТЕНТИФІКАЦІЇ НА ОСНОВІ ВІДКРИТОГО КЛЮЧА ДЛЯ СИСТЕМИ ІНТЕРНЕТУ РЕЧЕЙ

Інтернет речей (IoT) – це нова парадигма, де повсякденні об'єкти взаємопов'язані та спілкуються один з одним через Інтернет. IoT полегшує пряму інтеграцію фізичних об'єктів із кібер-світом за допомогою інтелектуальних датчиків, RFID-міток, смартфонів та носимих пристроїв. Мережі IoT пропонують різноманітні сфери застосування, охоплюючи моніторинг навколишнього середовища, охорону здоров'я, розумні міста, військову авіацію та інтелектуальні транспортні системи. Кількість пристроїв, відкритих для загальнодоступної мережі, поступово збільшується; пристрої мають безпосередню взаємодію з фізичним світом для збору даних. Наразі однією з найбільш дискусійних проблем розвитку мереж зв'язку пост-NGN є проблема ідентифікації пристроїв Інтернету речей. Сучасні методи анонімізації та передбачувана велика кількість пристроїв Інтернету речей, підключених до загальнодоступної комунікаційної мережі, роблять сучасні комунікаційні системи вразливими для зловмисників. Уразливість безпеки полягає в неможливості аутентифікації пристроїв Інтернету речей, що відкриває можливість зловмисникам виготовляти контрафактні фізичні та віртуальні продукти.

Ця ситуація вимагає безпечних рішень для запобігання втрати приватної інформації та зловмисної активації за допомогою одноранговоі аутентифікації та безпечної передачі даних між вузлами Інтернету речей і серверами. Однак існуюча структура та примітиви IoT на основі IP не повністю розроблені з урахованням можливостей пристроїв IoT з обмеженими ресурсами (такими як енергоспоживання, обчислювальний ресурс, діапазон зв'язку, RAM, FLASH тощо). Як

наслідок, потрібні більш легкі рішення для забезпечення безпеки пристроїв IoT з обмеженими ресурсами.

Мета полягає в тому, щоб створити метод аутентифікації на основі відкритого ключа для системи IoT, який буде більш оптимізованим і безпечним, ніж методи, які вже використовуються для Інтернету речей. У процесі роботи було проаналізовано більшість існуючих методів аутентифікації на основі відкритих ключів. На основі цього аналізу був запропонований метод аутентифікації, який поєднує існуючі методи з покращеним алгоритмом криптографії.

Ключові слова: IoT, Interent of Things, аутентифікація, криптографія, відкритий ключ, Інтернет.

УДК 004.415

д.т.н., проф. **Гунченко Ю.О.** (ОНУ)
д.т.н., проф. **Лєнков С.В.** (ВІКНУ)
к.пед.н., доц. **Толок І.В.** (ВІКНУ)
к.т.н. **Степаненко Є.О.** (ЗСУ)

DOI: https://doi.org/10.17721/2519-481X/2021/73-08

ОСНОВНІ ПРИНЦИПИ СИНТЕЗУ НАВЧАЛЬНО-ІНФОРМАЦІЙНИХ СИСТЕМ ДЛЯ ОРГАНІЗАЦІЇ БЕЗПЕРЕРВНОЇ ОСВІТИ

Постановуючим критерієм ефективності любого проектування є побудова її архітектури, що залежить від засобів і методів реалізації цієї системи. Удосконалення системи організації безперервної освіти у військовій навчальній системі сьогодні є величезна кількість програм, які певною мірою підвищують ефективність навчання за допомогою організації адаптивного діалогу з користувачем (як з учнем, студентом, курсантом, ад`юнктом, слухачем, так і з викладачем).

В цій статті проаналізовані основні принципи синтезу навчально-інформаційних систем для організації безперервної освіти. Розглянуті основні чинники, які впливають на якість навчально-інформаційних систем (НІС), а саме: мета функціонування; умови функціонування; топологія об'єкта дослідження, взаємозв'язок між завданнями, що розв'язуються; формальний опис процесів навчання персоналу; моделі функціонування; критерії ухвалення рішення про можливість використання отриманих результатів для вибору варіанта системи; узагальнені параметри (характеристики) НІС і обмеження; стратегії (моделі) навчання фахівців в умовах невизначеності вихідних даних і періодичності розв'язання завдань. Синтезована функція яка повинна бути гладкою й монотонною; у критичних випадках повинна виражати принцип мінімакса; у типових умовах повинна дотримуватися принципу інтегральної оптимальності; у проміжних випадках повинна приводити до парето-оптимальних розв'язів, що дають різні міри часткового задоволення критеріїв. Показано, що можливості традиційних методик навчання обмежені і не можуть забезпечити належної інтенсифікації підготовки майбутніх військових фахівців. Вихід полягає у принциповому повороті від екстенсивних до інтенсивних методик навчання з використанням перспективних НІС інтенсивної підготовки. Головною перевагою таких систем підготовки фахівців є можливість за допомогою імітаційних НІМ, що включає розвиток та наслідки вирішення баз знань, оцінити ефективність приймальних рішень фахівцями при різноманітних варіантах їх дій.

Констановано, що створення НІС інтенсивної підготовки та організація їх функціонування у вигляді двохфазової моделі інтенсивного навчання забезпечує професійну підготовку фахівців до необхідного (максимально можливого) рівня навченості при визначених фінансових і часових витратах.

Ключові слова: навчально-інформаційні системи, побудова архітектури, завдання синтезу, вибір схем компромісів.

Вступ та аналіз останніх досліджень. Початковим етапом *проектування будь-якої складної сис*теми є побудова її архітектури, що залежить від засобів і методів реалізації цієї системи. Зараз є величезна кількість програм, які певною мірою підвищують ефективність навчання за допомогою організації адаптивного діалогу з користувачем (як з учнем, студентом, курсантом, ад`юнктом, слухачем, так і з викладачем). Перші (НІС) будувалися відповідно до твердого сценарію подання навчальної інформації й діалогу з користувачем. До таких систем належать, наприклад, програмовані навчальні системи, а також електронні підручники, які й зараз не втрачають своєї актуальності й привабливості. Проте на сучасному етапі, коли обсяги інформації стрімко зростають, виникає необхідність створення таких засобів підтримки електронних підручників, які б дали змогу користувачеві не тільки переглядати інформацію, що цікавить його, шляхом навігацій по гіперструктурах, а й задавати різні більш складні питання [1-4]. Це приводить до розширення типології питань користувача, завдяки чому користувач заощаджує час на пошук тієї або іншої інформації. Ускладнення номенклатури й змісту, потреба вдосконалення засобів опису навчального матеріалу, тобто,

крім структури й змісту, необхідно також ураховувати семантичні зв'язки між описуваними поняттями. Використання такого підходу дозволяє розробити інтелектуальні довідкові системи або експертні системи (ЕС), які необхідні не тільки в складі НІС, а й у будь-якій комп'ютерній системі. ЕС є різновидом комп'ютерних систем для ефективної підготовки фахівців гуманітарного чи технічного профілю. Специфічною особливістю ЕС є наявність бази знань, де зберігаються розв'язання множини завдань, у тому числі при виконанні лабораторних та практичних робіт, які входять у програму навчання. База знань безупинно поповнюється й модифікується відповідно до досвіду застосування й вимог споживачів.

Розроблювачі НІС пропонують різні варіанти архітектур систем даного класу. Спільним у всіх цих архітектурах є те, що НІС складається з кількох підсистем, у результаті взаємодії яких користувачеві повинен забезпечуватися оптимальний режим навчання з обраної предметної області. Всі підсистеми в складі НІС тісно взаємодіють між собою, тобто НІС з повною впевненістю можна вважати колективом інтелектуальних систем, що підтримують різні аспекти процесу навчання [1,5].

Один з варіантів архітектур НІС описано в роботі [6]. Кожна з підсистем у складі НІС будується за тими самими принципами, що й будь-яка окрема експертна система, тобто має свою базу знань (БЗ) і механізми її перероблення. При цьому БЗ кожної з підсистем входить до складу загальної БЗ НІС і зберігається в одній і тій самій пам'яті, що значно полегшує процес взаємодії підсистем [6]. При цьому БЗ НІС здобуває складну структуру й великий обсяг, а механізми її оброблення мають різну типологію, тобто є змішаними. Для розроблення системи з такою складною структурою необхідні потужні базові інструментальні засоби, розроблення яких є одним із завдань даної роботи.

Постановка завдання синтезу автоматизованих навчально-інформаційних **систем для організації безперервної освіти.** Важливим завданням проектування НІС є завдання оптимального синтезу, спрямованого на вибір такого варіанта побудови НІС, який найкраще пристосований для виконання заданих функцій. Як правило, функції системи визначаються виходячи з переліку завдань, покладених на НІС. Реалізація основних функцій НІС здійснюється з урахуванням певних обмежень, поданих у вигляді припустимого часу й вартості навчання, а також обмежень на час підготовки, повноту та якість відтворення навчально-інформаційних моделей (НІМ) на робочих місцях тих, хто навчається [7-9]. Відповідно, вибір раціонального варіанта побудови НІС повинен здійснюватися на основі узагальненого критерію ефективності, що характеризує фінансово-часові витрати, які потрібні для досягнення необхідного рівня підготовки фахівців (персоналу) по виконанню поставлених завдань. При цьому, як параметри (характеристики) НІС, використовуються узагальнені параметри, що характеризують повноту та якість імітуючих НІМ, об'єктивного контролю й інші. Виходячи з цих відомостей, необхідно визначити структуру раціонального варіанта побудови НІС (склад робочих місць і зв'язку між ними) та стратегію керування процесом навчання, які повинні задовольняти заданим обмеженням на характеристики (узагальнені параметри) і бути оптимальними за заданим критерієм ефективності.

У роботі [7] авторами були розглянуті основні заходи та результати дослідження і розвиту. Проведено аналіз навчально-інформаційних систем нового покоління для безперервної підготовки військових фахівців. Розглянута класифікація навчально-інформаційної системи нового покоління, а саме системи: консультаційна, діагностична, керуюча, супроводжуюча. Проаналізовані стимулятори процесу пізнання: інтелектуальне середовище, гіперсередовище, мікросвіти, спеціальні окуляри тощо.

Якість НІС значною мірою залежить від розробки математичного, програмного, технічного й дидактичного забезпечення НІС [8,11]. Для розв'язання даних завдань повинні бути визначені:

1). мета функціонування НІС у процесі підготовки фахівців і завдання, що розв'язуються за допомогою цієї системи;

2). умови функціонування НІС у процесі підготовки персоналу;

3). топологія об'єкта дослідження, взаємозв'язок між завданнями, що розв'язуються НІС;

4). безліч навчальних завдань і НІМ, зіставлення позначених рівнів з їхніми структурами, що реалізують НІС;

5). формальний опис процесів навчання персоналу;

6). моделі функціонування НІС;

7). критерії ухвалення рішення про можливість використання отриманих результатів для вибору варіанта системи;

8). узагальнені параметри (характеристики) НІС і обмеження, що накладаються на процес організації функціонування НІС;

9). стратегії (моделі) навчання фахівців в умовах невизначеності вихідних даних і періодичності розв'язання завдань, необхідні узагальнені параметри системи для контролю поводження учнів з урахуванням динаміки функціонування НІС, стану, вірогідності й оперативності прийнятих рішень.

Дослідження повинні базуватися на вивченні інформаційно-функціональної структури системи підготовки фахівців, їхні результати повинні забезпечити таку декомпозицію цієї структури, яка дозволить сформулювати вимоги до раціонального (із системної точки зору) організації структури й функціонування НІС у процесі підготовки фахівців.

Найважливішими етапами системного синтезу є завдання структурного й параметричного синтезу НІС на заданій множині навчальних завдань системи підготовки фахівців.

У підсумку синтезу НІС повинні бути отримані наступні результати:

1) можливі варіанти структури НІС і діапазони зміни її параметрів, де забезпечується виконання всіх критеріальних, функціональних і вартісних обмежень;

2) значення керованих параметрів НІС, для яких за обраними показниками досягаються їхні екстремальні значення;

3) ранжировані моделі за ступенем їхнього впливу на обрані показники;

4) припустимі варіанти, які видаються особі, що приймає рішення.

Практичний напрямок дослідження – забезпечення необхідного рівня підготовки фахівців за рахунок оптимального проектування й використання НІС. Реалізація цього напрямку вимагає обґрунтування системи показників ефективності НІС.

Основні результати досліджень. У загальному випадку мірою ефективності дій курсантів, студентів є ймовірність своєчасного й безпомилкового розв'язання поставлених завдань (P), що включають виконання n типів операцій

$$P = \frac{1}{n}\sum_{i=1}^{n} p_i , \qquad (1)$$

де p_i – ймовірність своєчасного й безпомилкового виконання i-го типу операцій;

n – кількість типів виконуваних операцій.

Рівень підготовки персоналу за N етапів тренування може оцінюватися за наступною формулою:

$$P = \frac{1}{N}\sum_{j=1}^{N} P_j , \qquad (2)$$

де P_j – досягнутий рівень навченості персоналу в процесі проведення j-го етапу тренування (або за виконання завдань j-го типу).

Основною метою функціонування НІС є підготовка фахівців до необхідного («відмінного») рівня навченості (P_i) при мінімальних витратах часу й засобів (коштів) (C). При цьому узагальнений показник C повинен складатися з показників, що враховують витрати на розробку (C_1), серійне виготовлення (C_2) і впровадження (C_3) кожного x-го ($x \in X$) варіанта НІС, тимчасові (C_4), а також експлуатаційні витрати (C_5), необхідні для підготовки персоналу

до необхідного рівня (**$P_н$**). Крім того, узагальнений показник повинен враховувати трудовитрати для створення й ведення баз даних і баз знань про навчально-інформаційні моделі предметної діяльності фахівців (C_6), організації об'єктивного контролю й керування процесом тренування (C_7). У загальному випадку в узагальнений показник *C* можуть включатися витрати (C_8), необхідні для підвищення стійкості функціонування засобів обчислювальної техніки, програмного забезпечення, адаптерів сполучення й системи передачі даних кожного *x*-го варіанта НІС (розподіленої мережі НІС). При цьому значення ***К*-го (*К*=** 1, ..., *S*) показника витрат не повинне перевищувати максимально припустимого значення $C_к$. Виходячи з того, що часткові показники витрат задаються в різних одиницях виміру й носять суперечливий характер для розв'язання завдання вибору раціонального варіанта побудови НІС, скористаємося концепцією нелінійної схеми компромісів.

Математична модель завдання виглядає наступним чином:

$$\begin{cases} P \geq P_H; \\ C(x) \to min; \\ Y_x \in Y_{доп}, \end{cases} \tag{3}$$

де P – рівень навченості персоналу з виконання поставлених завдань;

P_H – необхідний рівень підготовки;

$C(x)$ – узагальнений показник витрат, необхідних для створення *x*-го варіанта НІС;

Y_x – узагальнені параметри (характеристики) *x* варіанта НІС;

$Y_{доп}$ – допустимі значення узагальнених параметрів НІС.

Зробимо скалярну згортку за нелінійною схемою компромісів і проаналізуємо його можливе застосування для розв'язання поставленого завдання. Нехай задано безліч можливих розв'язків $X \subset E^{\nu}$, що складається з векторів $x = \{x_i\}_{i=1}^{\nu}$ ν-мірного евклідового простору, компоненти яких можуть набувати тільки дискретні значення: $x_i = x_i^{(j)},\ j \in [1, J_i],\ J_i \geq 2,\ i \in [1, \nu]$. Розв'язання приймається за умов, які описуються вектором *ф*, заданим на безлічі можливих факторів *Ф.* Ситуація, що складається в результаті прийняття багатокритеріального розв'язку *X* у заданих умовах *Ф,* характеризується декартовим добутком *S=X*Ф*. Якість розв'язання оцінюється за сукупністю суперечливих часткових критеріїв, що утворять *s*-мірний вектор $C(x) = \{c_k(x)\}_{k=1}^{s}$, визначений на безлічі *X*. Вектор часткових критеріїв обмежений допустимою областю $c_k(x) \in c_{доп\,к}$, в якій $y \in y_{доп}$.

Ставиться завдання: визначити такий розв'язок $x^* \in X$, який при заданих умовах і обмеженнях мінімізує узагальнений показник витрат $C(x)$. Визначення багатокритеріального розв'язку за своєю природою компромісне. Вибравши схему компромісів, можна перейти від загального векторного вираження до скалярної згортки часткових критеріїв, що є основою для побудови конструктивного апарата розв'язання багатокритеріальних завдань. Якщо використовується спосіб скалярної згортки, то математично модель розв'язання завдання векторної оптимізації подається у вигляді:

$$x^* = \arg\min_{x \in X} C(x), \tag{4}$$

де *C(x)* – скалярна функція, що має зміст скалярної згортки вектора часткових критеріїв, вид якої залежить від обраної схеми компромісів.

Основна складність переходу від векторного критерію якості до скалярної згортки полягає в тому, що згортка повинна являти собою конгломерат часткових критеріїв, важливість кожного з яких у загальній оцінці змінюється залежно від випадку. У різних

ситуаціях ранг «найбільш важливого» можуть здобувати різні часткові критерії. Іншими словами, скалярна згортка часткових критеріїв повинна бути вираженням схеми компромісів, що адаптується до випадку. Поняття випадку, що виражається двійкою $S = \langle \phi, x \rangle$ з декартовим добутком *ФхХ,* фундаментальне для теорії векторної оптимізації, тому що воно, будучи об'єктивним, є єдиною підставою для спроб формалізації вибору схеми компромісів.

На підставі аналізу завдання вибору схеми компромісів замінюється еквівалентним завданням синтезу деякої єдиної скалярної згортки часткових критеріїв, що в різних випадках виражало б різні принципи оптимальності. Синтезована функція *C(x) [10,12]:*

1) повинна бути гладкою й монотонною;

2) у критичних випадках повинна виражати принцип мінімакса;

3) у типових умовах повинна дотримуватися принципу інтегральної оптимальності;

4) у проміжних випадках повинна приводити до парето-оптимальних розв'язків, що дають різні міри часткового задоволення критеріїв.

Іншими словами, така універсальна згортка повинна бути вираженням схеми компромісів, що адаптується до ситуації. Можна сказати, що адаптація та здатність до адаптації – головна змістовна суть дослідження багатокритеріальних систем, для чого необхідно, щоб у вираження для скалярної згортки в явному вигляді входили характеристики критичності ситуації. Такою функцією вважається уніфікована скалярна згортка за нелінійною схемою компромісів

$$C(x) = \sum_{k=1}^{s} c_{k_{доп}} \left[c_{k_{доп}} - c_k(x) \right]^{-1}, \tag{5}$$

яка виражає принцип «подалі від обмежень». При цьому нелінійна схема компромісів задовольняє умову парето-оптимальності.

Перевага концепції нелінійної схеми компромісів полягає в можливості прийняття багатокритеріального розв'язку формально, без особистої участі людини. Апарат нелінійної схеми компромісів, розроблений як формалізований інструмент для дослідження складних ергатичних систем із суперечливими критеріями, дає змогу пов'язувати багатокритеріальні завдання широкого класу.

У загальному випадку значення параметрів НІС обчислюються за наступними формулами. Параметр, що характеризує ступінь подоби алгоритму діяльності, який відпрацьовується на НІС, реальному

$$У_o = \sum_{j=1}^{m} b_j \sum_{i=1}^{m_j} R_{ij} K_{ij}\ , \tag{6}$$

де b_j – коефіцієнт значимості *j*-го фахівця при виконанні завдання;

R_{ij} – коефіцієнт значимості *i*-ї операції в алгоритмі діяльності *j*-го фахівця, причому

$$\sum_{j=1}^{m} b_j = \sum_{i=1}^{m_j} R_{ij} K_{ij} = 1, \tag{7}$$

де K_{ij} – коефіцієнт, що характеризує ступінь відповідності дій *j*-го фахівця при виконанні *i*-ї операції реальним;

m – кількість фахівців, які навчаються з використанням НІС;

m_j – кількість операцій в алгоритмі діяльності *j*-го фахівця.

Параметр повноти і якості відтворених навчально-інформаційних моделей обчислюється за формулою

$$y_1 = \sum_{i=1}^{n} \alpha_i k_i \frac{m_i}{m_i^o}, \tag{8}$$

де α_i – коефіцієнт, що характеризує значимість відтвореного *i*-го типу навчально-інформаційної моделі (у більшості випадків це очікувана частота появи *i*-ї навчально-інформаційної моделі),

k_i – коефіцієнт, що характеризує ступінь відповідності відтвореної навчально-інформаційної моделі *i*-го типу реальній обстановці;

m_i – кількість реалізацій навчально-інформаційних моделей *i*-го типу досліджуваної НІС за етап підготовки персоналу (фахівця);

m_i^o – необхідне число реалізацій навчально-інформаційної моделі *i*-го типу, яка необхідна для підготовки персоналу (фахівця) до необхідного рівня;

n – кількість типів навчально-інформаційної моделі. Для розрахунку показника (8) складається перелік типів навчально-інформаційних моделей, що підлягають відтворенню. Цей перелік повинен ураховувати повний діапазон усіх можливих інформаційних моделей, прогнозованих під час діяльності персоналу й необхідних для його підготовки до потрібного рівня.

Параметр повноти та якості об'єктивного контролю дій фахівців і керування процесом навчання обчислюється за формулою

$$y_2 = \sum_{i=1}^{r} q_i \, l_i \, \frac{f_i}{f_i^o}, \tag{9}$$

де r – кількість типів функцій контролю й керування;

q_i – коефіцієнт, що характеризує ступінь відповідності дидактичних функцій *i*-го типу необхідним;

l_i – коефіцієнт, що характеризує вагу функції *i*-го типу (в основному це очікувана частота використання *i*-ї функції), $\sum_{i=1}^{n} l_i = 1$;

f_i – кількість реалізованих функцій *i*-го типу за певний час;

f_i^o – кількість реалізацій функцій *i*-го типу, яка потрібна для підготовки персоналу до необхідного рівня.

Параметр, що характеризує повноту циклу підготовки фахівців за допомогою НІС:

$$y_3 = 1 - \sum_{i=1}^{n} b_i \, \frac{\Delta t_д}{t_{підг}}, \tag{10}$$

де $\Delta t_д$ – додатковий час підготовки в реальних умовах;

$t_{підг}$ – загальний час підготовки персоналу для забезпечення необхідної якості діяльності;

b_i – коефіцієнт значимості *i*-го завдання в загальній системі підготовки $\left(\sum_{i=1}^{n} b_i = 1\right)$;

n – число навчальних завдань, що становлять повний цикл підготовки.

Таким чином, вибір раціонального варіанта побудови НІС повинен здійснюватися на основі використання системи показників, що враховують динаміку підготовки персоналу (фахівців), а також витрати, необхідні для досягнення необхідного (максимально можливого) рівня їхньої навченості з виконання поставлених завдань.

Концептуальні засади побудови НІС інтенсивної підготовки. Практика показує, що можливості традиційних методик навчання обмежені і не можуть забезпечити належної інтенсифікації підготовки майбутніх фахівців. Вихід полягає в рішучому повороті від екстенсивних до інтенсивних методик навчання з використанням перспективних НІС інтенсивної підготовки.

Головною перевагою таких систем підготовки фахівців є можливість за допомогою імітаційних НІМ, що включає розвиток та наслідки вирішення БЗ, оцінити ефективність

приймальних рішень фахівцями при різноманітних варіантах їх дій. Однак, як показують результати досліджень, відставання в цій області обумовлюється не тільки недостатньою кількістю обчислювальної техніки, але й насамперед відсутністю концептуальних засад побудови НІС інтенсивної підготовки.

В загальному вигляді постановка задачі побудови НІС формулюється наступним чином. Необхідно визначити найбільш раціональний варіант побудови НІС, застосування якого забезпечить підготовку фахівців до максимально можливого рівня навченості у встановлений термін. Вирішення цієї задачі можливо на основі використання сучасних інтенсивних технологій навчання. При цьому інтенсивна технологія визначається "як система факторів, що інтенсифікують процес навчання: ідеальних, спрямованих на підвищення ступеня активності тих, кого навчають, і матеріальних (технічних), що забезпечують заданий (максимальний) рівень навчання в найкоротший термін" [7]. При цьому найбільш суттєвим для процесу інтенсифікації навчання є активізація діяльності фахівців [1,8]. У зазначених умовах прискорені режими навчання можуть стати джерелом як позитивних, так і негативних емоцій. Виникаючі в результаті дефіциту часу емоційні реакції до визначеного граничного значення впливають на підготовку фахівців як організуючий фактор. При цьому мотивація сприяє підвищенню швидкості засвоєння навчального матеріалу і скороченню часових та фінансових витрат на навчання. Однак, після досягнення визначеного порогу з прискореного навчання, емоційна напруженість стає дезорганізуючим фактором у цьому процесі.

В основу запропонованого методичного підходу до інтенсифікації навчання покладене те, що "внутрішня переконаність" фахівців в обмеженості часу, що залишився на вивчення необхідного матеріалу чи виконання навчального завдання, викликає в них стан напруженості. Якщо ж напруженість не перевищує граничне значення (гранично припустиму напруженість) – вплив стає організуючим. У моделі функціонування НІС напруженість визначена як внутрішній стан j-го фахівця безпосередньо перед виконанням і-ої елементарної задачі.

Концепція напруженості реалізується в НІС шляхом зменшення циклу відображення навчальної інформації (змісту навчальної задачі) на моніторах ПЕОМ, поки напруженість не досягне заданого рівня, при якому ще дефіцит часу діє як організуючий фактор. Організуючий вплив емоційної напруженості (S-напруженості) визначається тим, що в процесі підготовки фахівці працюють зосередніше, точніше, й імовірність правильного і своєчасного виконання елементарних завдань навчання підвищується.

Функція напруженості являє собою відношення часу, необхідного на виконання навчального завдання до фактично наявного часу в розпорядженні фахівців в кожному циклі функціонування АНС

$$h_{ij} = \frac{\sum_{i-1}^{I} \bar{t}_{iT\,\text{р}}}{T_j}, \qquad (11)$$

де – середній час, необхідний фахівцям для виконання і-ої елементарної задачі;

I – кількість задач, що залишилися для виконання;

T – повний час, що є в розпорядженні j-ої особи, яку навчають, для виконання I задач навчання, що залишилися в кожному циклі функціонування СІП.

Середні значення часу виконання елементарних навчальних завдань обчислюються на основі статистичних даних, отриманих у ході занять. Обчислення значення напруженості в процесі підготовки фахівців обмежені в НІС і знаходяться в межах від 1.0 до 4.0.

Якщо в ході підготовки фахівець вичерпав час то вважається, що величина напруженості цієї особи при виконанні операцій, що залишилися, дорівнює пороговому значенню. Значення порогу S-напруженості знаходиться в межах 1.8 - 2.9. Вибір конкретного значення порогу стресу залежить від індивідуальних особливостей тих, кого навчають. Як показує практика для

"середньостатистичної" особи 2.3, для "більш спокійного" 1.8 - 2.2, для "менш спокійного" 2.4 - 2.9. У зв'язку з цим в залежності від індивідуальних особливостей тих, кого навчають, на кожному занятті виникає необхідність у формуванні навчальних завдань з різною швидкістю. Таким чином, для реалізації технології інтенсивного навчання повинна забезпечуватися адаптивна зміна швидкості видачі навчальних завдань з ПЕОМ викладача на ПЕОМ тих, кого навчають. При цьому структура НІС умовно підрозділяється на комп'ютерні класи, до яких належать ПЕОМ викладача і ПЕОМ тих, кого навчають, і підсистему дистанційного навчання, що забезпечує реалізацію гнучкої віртуальної структури НІС для найбільш ефективного проведення усіх видів комп'ютерних занять.

Підготовка курсів (модулів) інтенсивного навчання здійснюється за єдиним оптимальним планом інтенсивного навчання, що припускає комбіноване рішення наступних двох основних задач [7,8]:

прискорена підготовка фахівців до необхідного рівня з виконання навчальних завдань при мінімальних витратах часу (перша фаза інтенсивного навчання).

підготовка фахівців для виконання завдань до максимально можливого рівня фахової навченості при заданих часових (вартісних) обмеженнях у ході проведення планових навчальних занять (друга фаза інтенсивної підготовки).

Вирішення першої задачі здійснюється у випадку, коли фахівці за результатами тестування не досягли необхідного рівня підготовки. Для рішення даної задачі здійснюється віртуальне підключення ПЕОМ тих, кого навчають, до ПЕОМ викладача з метою організації проведення першої фази інтенсивного навчання. При цьому в прискореному режимі забезпечується формування такої кількості різнотипних навчальних завдань на засобах відображення ПЕОМ, при відпрацюванні яких скорочуються часові (фінансові) витрати, необхідні для підготовки фахівця до необхідного рівня.

Для тих, які успішно пройшли тестування, здійснюється вирішення завдання зі створення такої віртуальної структури НІС, при якій одночасно на засобах відображення ПЕОМ тих, кого навчають, формується необхідна кількість навчальних завдань, що забезпечує подальше максимальне підвищення рівня підготовки фахівців з навчальних тем. Розв’язання даних задач може здійснюватися, наприклад, на основі використання спеціальних методів оптимального планування й управління процесом підготовки фахівців [6], які будуть розглянуті у наступних розділах. У загальному вигляді систему інтенсивної підготовки можна представити (рис. 1) у виді двох основних частин: об'єкта управління (тих, кого навчають) і керуючого пристрою (ПЕОМ викладача).

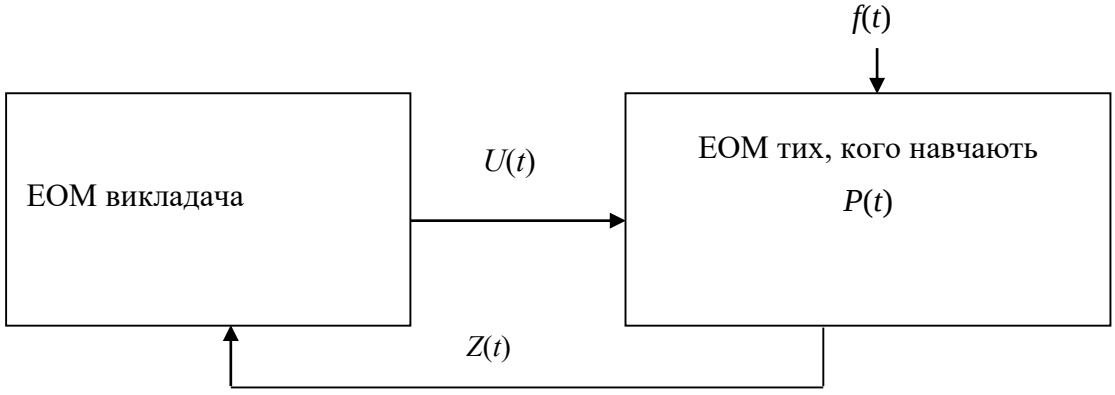


Рисунок 1 – Загальний вигляд системи інтенсивної підготовки

Математичний опис системи інтенсивного навчання може бути представлений в наступному вигляді:

$$\varphi_i[z_i(t),\ \dot{z}_i(t),...,z_i^{(n_K)};\quad u_1(t),\dot{u}_1(t),...,u_1^{(k_1)}(t);u_2(t),\dot{u}_2(t),...,u_2^{(k_2)}(t);$$

$$u_m(t),\dot{u}_m(t),...,u_m^{(k_k)}(t);\ f_1(t),\dot{f}_1(t),...,f_1^{(k_1)}(t);\ f_2(t),\dot{f}_2(t),...,f_2^{(k_2)}(t); \qquad (12)$$

$$f_m(t),\dot{f}_m(t),...,f_m^{(k_k)}(t)],\ i=1,2,...,K,$$

де K – кількість фахівців, що навчаються;

$z_i(t),\ \dot{z}_i(t),...,z_i^{(n_K)}$ – вихідні параметри (відповіді) тих, кого навчають;

$u_m(t),\dot{u}_m(t),...,u_m^{(k_k)}(t)$ – управляючі впливи інтенсивної підготовки у вигляді адаптивної зміни швидкості відтворення навчальних завдань;

$f_m(t),\ \dot{f}_m(t),...,\ f_m^{(k_k)}(t)$ – зовнішні впливи.

При K=1 об'єкт є одномірним. Якщо K=1, то K диференціальних рівнянь (8) при відсутності зовнішнього впливу та з урахуванням перемінних стану тих, кого навчають, можна представити в нормальній формі Коші:

$$\dot{p}_i(t)=\psi(p_1(t),\ p_2(t),\ ...,\ p_n(t);\ u_1(t),\ u_2(t),\ ...,\ u_k(t))\ ,\ \text{i=1, 2, …, } n. \qquad (13)$$

Вихідні результати (відповіді) тих, кого навчають, виражаються співвідношеннями виду:

$$\dot{z}_i(t)=\Theta(p_1(t),\ p_2(t),\ ...,\ p_n(t);\ u_1(t),\ u_2(t),\ ...,\ u_k(t))\ ,\ \text{i=1, 2, К.} \qquad (14)$$

У загальному випадку можна представити рівняння стану тих, кого навчають, у такому вигляді:

$$\dot{P}(t)=\psi[P(t),\ U(t),\ t];\ Z(t)=\theta[P(t),\ U(t),\ t]. \qquad (15)$$

Допускаємо, що у деякий момент часу $t_0 = 0$, який приймається як початок відліку часу, перемінні стану y1, y2, …, yn мають значення $y1(t_0)$, $y2(t_0)$, …, $yn(t_0)$ чи, іншими словами вектор стану дорівнює $P(t_0)$. Припустимо, що момент t_0 відповідає початку управління процесом інтенсивного навчання, тобто починаючи з цього моменту на об'єкт навчання подається управління U(t). Сукупність обмежень формує область можливих значень впливів, які управляють. Позначимо цю область символом Курси інтенсивної підготовки, що реально подаються на вхід об'єкта управління, мають належати області припустимих управлінь:

$$U(t)\in\Omega(U). \qquad (16)$$

Вцілому формування курсів інтенсивної підготовки полягає в плануванні необхідного набору навчальних завдань з метою інтенсифікації процесу відпрацьовування різнотипних елементарних задач навчання на кожному і-ому (i=1, …, N) етапі інтенсивної підготовки.

Модель функціонування НІС припускає реалізацію наступних двох фаз інтенсифікації процесу навчання:

1 фаза: прискорена підготовка фахівців до необхідного рівня навчання Рн(t) при мінімальних часових та вартісних витратах С і h_{ij} . У цьому випадку потрібно знайти таке управління U(t) , при якому ті, які навчаються, перейдуть зі стану P(t0=0) у необхідний стан Рн(t) при мінімальних С і $h_{ij}\to V_{j0}$, тобто

$$\left\lfloor \min_{U(t)\in\Omega(U)} \right\rfloor C. \qquad (17)$$

2 фаза: після досягнення необхідного рівня підготовки забезпечується підтримка отриманих навичок (знань, умінь) та їх подальше вдосконалювання при $h_{ij} \to V_{j0}$ і $C=C_{доп}$. У цьому випадку задається початковий стан фахівців $P(t_0)$, область припустимих управлінь $\Omega(U)$ і критерій оптимальності:

$$[\max_{U(t)\in\Omega(U)}]P(t). \qquad (18)$$

Основною метою функціонування НІС є підготовка фахівців до необхідного (максимально можливого – "відмінного") рівня (Рн) при мінімальних витратах часу і засобів (С).

При цьому узагальнений показник С повинен враховувати витрати на розробку (С1), серійне виготовлення (С2) і впровадження (С3) кожного r – го (r=1, …, R) варіанта СІП, часові (С4), а також експлуатаційні витрати (С5), необхідні для підготовки фахівців необхідного рівня (Рн). Крім того, узагальнений показник С має враховувати витрати для створення і ведення баз даних (баз знань) про навчальні завдання (С6), організацію об'єктивного контролю і управління процесом навчання (С7). Також в узагальнений показник С можуть включатися витрати (С8), необхідні для підвищення стійкості функціонування засобів обчислювальної техніки, програмного забезпечення і мережного обладнання кожного r-го варіанту НІС. При цьому значення к-го (к = 1, …, s) показника витрат не повинне перевищувати максимально припустимого значення .

Виходячи з того, що показники витрат задаються в різних одиницях виміру і носять різний фізичний зміст, для рішення задачі вибору раціонального варіанту побудови та організації функціонування НІС на першій фазі навчання скористаємося концепцією нелінійної схеми компромісів [9].

При цьому для вибору r-го (раціонального) варіанта побудови НІС, що забезпечить прискорену підготовку фахівців, доцільно використовувати наступний узагальнений показник (Cr):

$$C_r = \sum_{k=1}^{s} \left(\frac{F_k C_{k_{доп}}}{C_{к_{доп}} - C_{kr}}\right) \to \min, \qquad (19)$$

при $P_r \geq P_н$, $C_{кг} \leq C_{k_{доп}}$, $\sum_{k=1}^{s} F_k = 1$ $(r = 1, \ldots, R;\ \ k = 1, \ldots, s)$,

де P_r – середній рівень підготовки фахівців, що досягається при використанні *r*-го варіанта НІС на першій фазі навчання;

$P_н$ – необхідний рівень підготовки фахівців;

F_k - коефіцієнт важливості k-го показника.

Крім того r-ий (раціональний) варіант побудови АНС, при його використанні на другій фазі навчання, повинен задовольняти наступному критерію ефективності:

$$P_r \to \max, \qquad (20)$$

при $C_{кг} \leq C_{k_{доп}}$, $\sum_{k=1}^{s} F_k = 1$ $(r = 1, \ldots, R;\ \ k = 1, \ldots, s)$.

Таким чином, створення НІС інтенсивної підготовки та організація їх функціонування у вигляді двохфазової моделі інтенсивного навчання забезпечує професійну підготовку фахівців до необхідного (максимально можливого) рівня навченості при визначених фінансових і часових витратах.

Висновки

1. В роботі проаналізовані основні принципи синтезу сучасних навчально-інформаційних систем для організації безперервної освіти у військовій сфері.

2. Розглянуті основні чинники, які впливають на якість навчально-інформаційних систем, а саме: мета функціонування; умови функціонування; топологія об'єкта дослідження, взаємозв'язок між завданнями, що розв'язуються; формальний опис процесів навчання персоналу; моделі функціонування; критерії ухвалення рішення про можливість використання отриманих результатів для вибору варіанта системи. Узагальнені параметри (характеристики) НІС і обмеження; стратегії (моделі) навчання фахівців в умовах невизначеності вихідних даних і періодичності розв'язання завдань.

3. На підставі аналізу завдання вибору схеми компромісів замінюється еквівалентним завданням синтезу деякої єдиної скалярної згортки часткових критеріїв, що в різних випадках виражає різні принципи оптимальності. Синтезована функція *C(x) яка:* повинна бути гладкою й монотонною; у критичних випадках повинна виражати принцип мінімакса; у типових умовах повинна дотримуватися принципу інтегральної оптимальності; у проміжних випадках повинна приводити до парето-оптимальних розв'язків, що дають різні міри часткового задоволення критеріїв.

4. Концептуальні засади побудови НІС інтенсивної підготовки. Показує, що можливості традиційних методик навчання обмежені і не можуть забезпечити належної інтенсифікації підготовки майбутніх військових фахівців. Вихід полягає у принциповому повороті від екстенсивних до інтенсивних методик навчання з використанням перспективних НІС інтенсивної підготовки.

5. Головною перевагою таких систем підготовки фахівців є можливість за допомогою імітаційних НІМ, що включає розвиток та наслідки вирішення НЗ, оцінити ефективність приймальних рішень фахівцями при різноманітних варіантах їх дій.

6. Констановано, що створення НІС інтенсивної підготовки та організація їх функціонування у вигляді двохфазової моделі інтенсивного навчання забезпечує професійну підготовку фахівців до необхідного (максимально можливого) рівня навченості при визначених фінансових і часових витратах.

ЛІТЕРАТУРА:

1. Герасимов Б.М. Тарасов В.А., Токарев И.В. Человека-машинные системы принятия решений с элементами искусственного интеллекта . – К.: Наукова думка, 1993. – 184 с.

2. V. Lysenko, Y. Gunchenko, S. Shvorov, S. Lenkov, S. Kuznichenko, E. Lenkov. Methodological Bases of Construction of Intensive Training Flight Simulators of Aircrews // Proceedings 5th International Conference “Methods and Systems of Navigation and Motion Control”. ISBN: 978-153865870-3 – Kyiv, 2018. – P. 198 – 203. (IEEE Catalog Number: CFP1852Y-PRT).

3. Лєнков С.В., Гунченко Ю.О., Гришин С.П., Плосконос І.М. Автоматизація вирішення розрахункових задач у складних системах управління // Вісник Хмельницького національного університету. Економічні науки. – Хмельницький, 2012. – № 3.Т1. – С.31 – 35.

4. Толок І.В. Розвиток психолого-педагогічної компетентності майбутніх магістрів військового управління в системі післядипломної освіти: дис.канд.пед.наук: 13.00.04 / Толок І.В. Київ, 2013. 231 с.

5. Shvorov, S.A., Pasichnyk, N.A., Kuznichenko, S.D., Tolok I., Lienkov, S.V., Komarova, L.A. Using UAV during Planned Harvesting by Unmanned Combines // IEEE 5th International Conference Actual Problems of Unmanned Aerial Vehicles Developments, APUAVD 2019 ISBN: 978-172812592-3. – Proceedings 8943842, P. 252-257.

6. Голенков В.В., Гулякина Н.А. Елисеева О.Е. Инструментальные средства проектирования интеллектуальных обучающих систем: Методическое пособие по курсу «Интеллектуальные обучающие и тренажерные системы» для студентов специальности «искусственный интеллект». Мн.: БГУИР, 1999. – 102 с.

7. Гунченко Ю.О. Концептуальні засади побудови систем інтенсивної підготовки фахівців спецпідрозділів // Журнал «Сучасна спеціальна техніка». – К., 2012. – №1(28). – С. 97 – 103.

8. Гунченко Ю.О., Лєнков С.В. Модель функціонування адаптивної тренажерної системи для підготовки фахівців спецпідрозділів // Інформатика та математичні методи в моделювання. – Одеса, 2011. - №3. – С. 260 – 265.

9. Гунченко Ю.О., Лєнков С.В., Шворов С.А., Гончарук А.А. Планування процеса тренувань фахівців спецпідрозділів з урахуванням їх функціонального стану та обмежень на часові (вартісні) витрати // Журнал «Інформаційна безпека». - Луганськ, 2012. - №2(8). – С. 37 – 42.

10. Толок І.В., Браун В.О., Мірошніченко О.В., Пампуха І.В., Солодєєва Л.В. Аналіз навчально-інформаційних систем нового покоління для безперервної підготовки військових фахівців // Збірник наукових праць Військового інституту Київського університету імені Тараса Шевченка. – Київ, - 2021. - №71. – С. – .

11. Патент на користу модель № 67752, Україна, МПК G06F 12/08. Пристрій підвищення завадостійкості систем з програмним управлінням [текст] / Гунченко Ю.О., Мартинюк С.М., Лєнков С.В., Омельченко О.С., Купрацевич А.В.; власник Одеський національний університет ім. І.І. Мечникова. - № u201107423, заявл. 14.06.2011, опубл. 12.03.12. Бюл. №5.

12. Яйлаханов С.В. Организация учебной деятельности студентов (курсантов) в информационной образовательной среде: дис.канд.пед.наук: 13.00.08 / Яйлаханов С.В. – Ставрополь, 2006. – 158 с.

REFERENCES:

1. Gerasimov B.M. Tarasov V.A. and Tokarev I.V. (1993). Cheloveka-mashinnye sistemy prinyatiya reshenij s elementami iskusstvennogo intellekta, Kiyiv, Naukova dumka, 184 p.

2. V. Lysenko, Y. Gunchenko, S. Shvorov, S. Lenkov, S. Kuznichenko, E. Lenkov. Methodological Bases of Construction of Intensive Training Flight Simulators of Aircrews // Proceedings 5th International Conference “Methods and Systems of Navigation and Motion Control”. ISBN: 978-153865870-3 – Kyiv, 2018. – P. 198 – 203. (IEEE Catalog Number: CFP1852Y-PRT).

3. Lyenkov S.V., Gunchenko Yu.O., Grishin S.P. and Ploskonos I.M. (2012). Avtomatizaciya virishennya rozrahunkovih zadach u skladnih sistemah upravlinnya, Visnik Hmelnickogo nacionalnogo universitetu. Ekonomichni nauki, Hmelnickij, no. 3, Vol. 1, pp. S.31 – 35.

4. Tolok I.V. (2013). Rozvitok psihologo-pedagogichnoyi kompetentnosti majbutnih magistriv vijskovogo upravlinnya v sistemi pislyadiplomnoyi osviti: dis.kand.ped.nauk: 13.00.04, Kiyiv, 231 p.

5. Shvorov, S.A., Pasichnyk, N.A., Kuznichenko, S.D., Tolok I., Lienkov, S.V., Komarova, L.A. Using UAV during Planned Harvesting by Unmanned Combines // IEEE 5th International Conference Actual Problems of Unmanned Aerial Vehicles Developments, APUAVD 2019 ISBN: 978-172812592-3. – Proceedings 8943842, P. 252-257.

6. Golenkov V.V., Gulyakina N.A. and Eliseeva O.E. (1999). Instrumentalnye sredstva proektirovaniya intellektualnyh obuchayushih sistem: Metodicheskoe posobie po kursu «Intellektualnye obuchayushie i trenazhernye sistemy» dlya studentov specialnosti «iskusstvennyj intellekt». Mn.:BGUIR, 102 p.

7. Gunchenko Yu.O. (2012). Konceptualni zasadi pobudovi sistem intensivnoyi pidgotovki fahivciv specpidrozdiliv. Suchasna specialna tehnika, Kiyiv, no. 1(28), pp. 97-103.

8. Gunchenko Yu.O., Lyenkov S.V. (2011). Model funkcionuvannya adaptivnoyi trenazhernoyi sistemi dlya pidgotovki fahivciv specpidrozdiliv, Informatika ta matematichni metodi v modelyuvannya, Odesa, no. 3, pp. 260 – 265.

9. Gunchenko Yu.O., Lyenkov S.V., Shvorov S.A. and Goncharuk A.A. (2012). Planuvannya procesa trenuvan fahivciv specpidrozdiliv z urahuvannyam yih funkcionalnogo stanu ta obmezhen na chasovi (vartisni) vitrati, Informacijna bezpeka, Lugansk, no. 2(8), pp. 37-42.

10. Tolok I.V., Braun V.O., Miroshnichenko O.V., Pampuha I.V. and Solodyeyeva L.V. (2021). Analiz navchalno-informacijnih sistem novogo pokolinnya dlya bezperervnoyi pidgotovki vijskovih fahivciv, Zbirnik naukovih prac Vijskovogo institutu Kiyivskogo universitetu imeni Tarasa Shevchenka, Kiyiv, no. 71, pp. 68-77.

11. Patent na koristu model № 67752, Ukrayina, MPK G06F 12/08. Pristrij pidvishennya zavadostijkosti sistem z programnim upravlinnyam [tekst] / Gunchenko Yu.O., Martinyuk S.M., Lyenkov S.V., Omelchenko O.S., Kupracevich A.V.; vlasnik Odeskij nacionalnij universitet im. I.I. Mechnikova. - № u201107423, zayavl. 14.06.2011, opubl. 12.03.12. Byul. No. 5.

12. Yajlahanov S.V. (2006). Organizaciya uchebnoj deyatelnosti studentov (kursantov) v informacionnoj obrazovatelnoj srede: dis.kand.ped.nauk: 13.00.08, Stavropol, 158 p.

D.Sci. Tech., prof. Gunchenko Yu.O., D.Sci. Tech., prof. Lienkov S.V.,
PhD Tolok I.V., PhD Stepanenko Ye.O.

BASIC PRINCIPLES OF SYNTHESIS OF EDUCATIONAL INFORMATION SYSTEMS FOR THE ORGANIZATION OF CONTINUING EDUCATION

The decisive criterion for the effectiveness of any design is the construction of its architecture, which depends on the means and methods of implementing this system. Improving the system of continuing education in the military education system today is a huge number of programs that to some extent increase the effectiveness of training through adaptive dialogue with the user (as a student, cadet, associate professor, student and teacher).

This article analyzes the basic principles of synthesis of educational and information systems for the organization of continuing education. The main factors that affect the quality of educational information systems (NIS) are considered, namely: the purpose of operation; operating conditions; topology of the object of research, the relationship between the tasks to be solved; formal description of staff training processes; functioning models; criteria for deciding on the possibility of using the results to select a system option; generalized parameters (characteristics) of NIS and restrictions; strategies (models) of training specialists in the conditions of uncertainty of initial data and periodicity of solving tasks. Synthesized function which should be smooth and monotonous; in critical cases must express the principle of minimax; in typical conditions must adhere to the principle of integral optimality; in intermediate cases should lead to pareto-optimal solutions that give different measures of partial satisfaction of the criteria. It is shown that the possibilities of traditional training methods are limited and cannot provide proper intensification of training of future military specialists. The way out is a fundamental turn from extensive to intensive teaching methods using promising NIS intensive training. The main advantage of such training systems is the ability to use simulation BAT, which includes the development and consequences of solving knowledge bases, to assess the effectiveness of decision-making by specialists in a variety of options.

It is stated that the creation of NIS intensive training and the organization of their functioning in the form of a two-phase model of intensive training provides professional training to the required (maximum possible) level of training at a certain financial and time costs.

Key words: educational and information systems, architecture construction, synthesis tasks, choice of compromise schemes.

УДК 004.891

к.т.н. **Джулій А.В.** (УЕП, м.Хмельницький)
к.т.н., доц. **Чорненький В.І.** (УЕП, м.Хмельницький)

DOI: https://doi.org/10.17721/2519-481X/2021/73-09

МЕТОД ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ПРОТОКОЛУ РОЗПОДІЛЕННЯ КЛЮЧІВ БЕЗПЕЧНОЇ IP-ТЕЛЕФОНІЇ НА ОСНОВІ АЛГОРИТМУ ДІФФІ – ХЕЛМАНА

У роботі запропоновано метод підвищення ефективності протоколу розподілення ключів безпечної Ip-телефонії на основі алгоритму Діффі – Хелмана, відрізняється від існуючого методу виявлення нелегітимного абонента, впровадженням автоматизованої програмно-апаратної перевірки аутентифікаційного рядка. При використанні в даному випадку декілька каналів зв'язку, відповідна перевірка надасть можливість виявити нелегітимного абонента.

Вирішує наступні задачі: надає можливість виявити активного нелегітимного кореспондента, який використовує програмне забезпечення синтезу голосу; визначити активного нелегітимного кореспондента IP - протоколів в каналах зв'язку Інтернет-телефонії при відсутності попередньо розподіленої секретної ключової інформації між кореспондентами, довіреного центру. Результати проведеного дослідження надають можливість вказати, що найбільш відомі IP-протоколи розподілу загальної секретної інформації необхідно вдосконалювати в двох напрямках: підвищення інформаційної безпеки IP - телефонії та покращення основних показників IP-протоколів Інтернет мереж. Найбільш небезпечною атакою є атака типу «зустріч по середині» на IP -протоколи розподілу загальної секретної інформації. Завдання формування загальної секретної інформації в умовах проведення атаки типу «зустріч по середині» вторгнення нелегітимного кореспондента на сучасному етапу є актуальною. Одним з методів забезпечення підвищення безпеки IP протоколу формування загальної секретної інформації є відслідкування і заборона виконання атаки типу «зустріч по середині» за рахунок використання в Інтернет мережах IP - телефонії декількох паралельних незалежних каналів сеансів зв'язку. Знаючи вразливості та рівень захищеності об'єкта, для якого необхідно провести захист, активний нелегітимний кореспондент може виконувати комбінацію атак, яка може привести до отримання несанкціонованого доступу до даних об'єкта.

Запропоновано метод виявлення активного нелегітимного абонента IP - протоколів розподілу загальної секретної інформації, заснованих на алгоритмі обміну ключів Діффі-Хелмана, особливість методу полягає у використанні декількох відкритих каналів зв'язку. Забезпечує зниження вірогідності проведення активним нелегітимним абонентом успішної атаки «зустріч по середині», а також присутність механізму визначення активного зловмисника в каналі зв'язку, при відсутності наперед розподіленої загальної секретної інформації. Метод накладає обмеження на використовувані канали зв'язку, в тому плані, що канали зв'язку повинні бути незалежні.

Ключові слова: нелегітимний кореспондент, інформаційна взаємодія, інтернет-телефонія, криптографічний захист, канали зв'язку, розподілення ключів.

Вступ. Поширення IP-телефонії через Internet мережі поставило під загрозу прибутки операторів телефонних мереж. Проте, оператори AT&T, British Telecomunications, Deutsche Telecom, починають надавати послуги Internet-телефонії. Аналогічні послуги передачі голосу через Internet мережі надають компанії WorldPort, Lucent, ITXC та інші. Найперспективнішими ринками передачі голосу через IP-мережі для IP-телефонії вважаються Австралія, США та Японія.

Поширенню IP-телефонії в Україні перешкоджає декілька факторів: недостатньо надійна інфраструктура Internet мереж каналів зв‘язку; організації, які забезпечують телефонні мережі послугами зв‘язку, не зацікавлені в розвитку IP-телефонії. Лише кілька провайдерів надають послуги IP-телефонії - Infocom, IP Telecom, Sovam Teleport.

Перевагою Internet-телефонії є низька вартість міжміських і міжнародних переговорів, дозволяє зменшити витрати на послуги передачі факсів і мультимедіа зв'язку, за рахунок шифрування і стиснення голосового потоку.

Розвиток нових IP-протоколів Internet мереж, а також передача потоку пакетних даних у вигляді голосових пакетів у відкритому виді через публічні мережі призвели до необхідності стандартизації IP-протоколів Імереж, а також криптографічного захисту даних для забезпечення безпечної Internet-телефонії. IP-протоколи Internet мереж розділені, в відповідності до вирішуваних задач, на три групи: протоколи забезпечення захищеності і сигналізації, криптографічний захист пакетного потоку даних (медіа трафіку) і програмний розподіл ключів сучасними криптографічними алгоритмами генерації загальних ключів для медіа трафіка.

Стандартизація протоколів, а також масове використання персональних комп'ютерів операторами IP-телефонії в якості терміналів, призвели до розробки спеціалізованого програмного забезпечення для IP-телефонії, дало поштовх розширювати можливості IP-телефонії і використовувати криптографічні алгоритми та алгоритми розподілу ключів для забезпечення надійності в Інтернет-телефонії.

Постановка задачі. Для розподілу секретної інформації між кореспондентами IP – телефонії на даному етапі використовуються алгоритми асиметричного шифрування. До переваг використання алгоритмів асиметричного шифрування можна віднести розподіл секретної інформації між кореспондентами IP – телефонії. Недоліком є те що вони досить повільні, мають відносно велику довжину ключа, є не придатними для шифрування великих об’ємів інформації. Область їх застосування - розподіл секретної інформації між кореспондентами IP – телефонії, формування цифрового підпису.

Запропонований У.Діффі і М.Хеллманом принципово новий підхід організації секретного зв'язку, шифрування з відкритим ключем, без попереднього обміну ключами. Для шифрування і дешифрування потоку даних використовуються різні ключі, при цьому доступ до одного ключа не надає практичної гарантії обчислити інший. Криптосистема запропонована У. Діффі і М. Хелманом забезпечує обмін секретною інформацією по Інтернет мережам по відкритим лініям зв'язку для абонентів, які використовують не захищені канали зв’язку.

Наявність двох і більше каналів у одного абонента на сьогодні досить поширене явище. Інформація яка необхідна для організації захищеного каналу сесії може бути отримана абонентами наступним чином: по телефону, при особистій зустрічі, по електронній пошті, та іншими доступними засобами зв’язку.

При побудові повної мережі з використанням існуючих автономних систем не можливо вказати точний маршрут, по якому інформаційні пакети будуть передаватися між абонентами сесії, які підключені до автономних систем. Маршрутизація IP - пакетів в Інтернет мережі будь-якого оператора зв'язку залежить від завантаження каналів зв'язку, аварій що виникають на обладнанні використовуваного в мережі, а також від діючих додаткових наданих угод між операторами IP - телефонії, що визначають цінову політику і параметри наданих послуг.

Основна частина. Для забезпечення підвищення надійності та безпеки Інтернет мереж IP -телефонії пропонується для вирішення поставленої задачі застосовувати метод виявлення нелегітимного абонента IP - протоколів розподілу загальної секретної інформації, заснованих на алгоритмі обміну ключами Діффі-Хелмана, алгоритм дозволяє розподіл загальної секретної інформації з використанням одночасно декількох каналів зв'язку (рис. 1) і при цьому виявляти активного нелегітимного абонента.

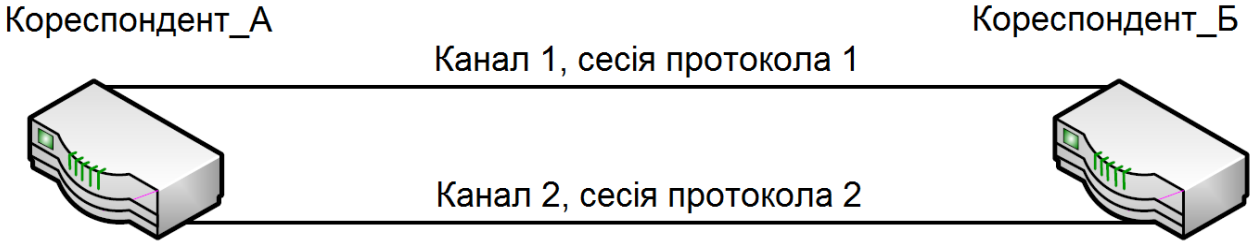


Рисунок 1 - Використання каналів зв'язку для обміну ключами

Для успішної реалізації роботи IP - протоколу ZRTP за декілька каналами зв'язку необхідно виконати інтеграцію багатоканального IP - протоколу з протоколами Інтернет мережі SIP/RTP для вирішення програмно-апаратних та технічних задач, мати можливість визначення IP-адрес додаткових каналів, а також TCP/UDP портів для успішного виконання другого сценарію IP – протоколу Інтернет мережі, а також передачу відповідних параметрів в протокол IP – телефонії, клас IP – протоколу Інтернет мережі а також функцію IP – протоколу мережі. Таким чином, реалізація перевірки роботи алгоритму обміну ключами Діффі-Хелмана по декільком каналах зв'язку в залежності від отриманих результатів під час перевірки: продовжити виконання відповідних подальших дій; виконати інтеграцію з протоколами Інтернет мережі SIP / RTP.

Для реалізації двоканального підходу для підвищення безпеки потоку даних по каналам зв'язку IP – телефонії з використанням асиметричного алгоритму обміну ключами Діффі-Хелмана будемо передавати відповідно до протоколу однакові повідомлення. Абонент *A* відправляє по каналам зв'язку однакові повідомлення. Абонент *B* отримує повідомлення, відповідно до алгоритму, проводить обчислення, перевіряє, чи отримані повідомлення співпадають. У випадку, якщо отримані повідомлення не співпадають - в одному з каналів виявлена присутність активного нелегітимного абонента, що виконує активну атаку типу «зустріч посередині». Абонент *B* відповідає абоненту *A* про наявність в одному з каналів активного нелегітимного абонента, відправляючи по каналах зв'язку повідомлення, використовуючи алгоритм Діффі-Хелмана. Абонент *A* отримує відповідне повідомлення і перевіряє їх на співпадання. У випадку, якщо отримані повідомлення співпадають – це означає відсутність активного нелегітимного абонента в каналах зв'язку, або, що також вірогідно, що активний нелегітимний абонент один і той же присутній в обох каналах зв'язку. Взаємодія абонентів Інтернет мережі IP – телефонії при використанні модифікованого протоколу ZRTP представлена на рис. 2.

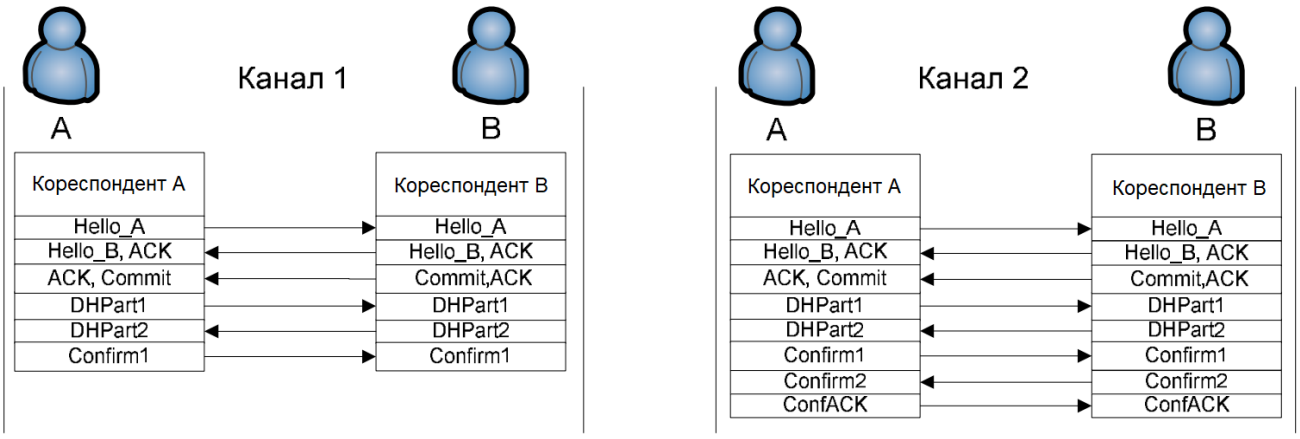


Рисунок 2- Взаємодія абонентів Інтернет мережі IP – телефонії при використанні модифікованого протоколу ZRTP

Розглянемо ймовірність захоплення обладнання оператора $P_{НСДЦ_{ЗАХОБЛ\_2}}$, яка визначає що нелегітимний абонент може виконувати активну атаку типу «зустріч по середині» в одному з двох каналів зв'язку Інтернет мережі IP -телефонії. Дана ймовірність відповідає неуспішній можливості виконання атаки типу «зустріч по середині», так як дана активна атака виявляється використанням модифікованого протоколу ZRTP. Виконується розрахунок ймовірностей подій (виявлення атаки, успішної атаки «зустріч по середині», успішного розподілу секретної інформації): $P_{BA\_ЗС}$ $P_{УA\_ЗС}$ $P_{У\_СК}$. Активна атака називається успішної, якщо нелегітимний абонент реалізував активну атаку типу «зустріч по середині», при цьому попередньо виконавши обмін секретною інформацією з обома абонентами по двом каналах зв'язку Інтернет мережі IP -телефонії. Під час проведення успішної атаки нелегітимний абонент не

виявляє себе. Це є можливим тільки в тому разі, коли нелегітимний абонент (один і то й же) може контролювати всі канали зв'язку, які використовують учасники сесії IP -телефонії і при цьому нелегітимний абонент в стані виконувати синхронну модифікацію потоку даних між учасниками сесії IP -телефонії в кожному з каналів зв'язку. Імовірність виконання успішної активної атаки $P_{УА\_ЗС2}$ для IP - протоколу який використовує два канали відповідає ймовірності здійснення події, що нелегітимний абонент може одночасно прослуховувати і в той же час виконувати модифікацію повідомлень в двоканальному зв'язку одночасно $P_{УА\_НА2} = \left(P_{НСДЦ_{ЗАХОБЛ\_2}}\right)^2$.

Виявлення нелегітимного абонента дозволяє користувачам визначити, що може бути вироблений компрометуючий ключ, що дозволяє дешифрувати і прослуховувати передану інформацію, а також виконувати модифікацію повідомлень. Ймовірність виявлення нелегітимного абонента залежить від числа використовуваних каналів зв'язку, а також від здатності алгоритму розподілу ключів визначити існування зловмисника в конкретному або конкретних каналах зв'язку з сукупності використовуваних. Ймовірність виявлення нелегітимного абонента $P_{В\_ЗАХОБЛ2}$ при використанні двоканального методу відповідає ймовірності знаходження нелегітимного абонента в одному каналі зв'язку при відсутності нелегітимного абонента в іншому каналі зв'язку IP - телефонії. Імовірність наявності нелегітимного абонента в першому каналі при відсутності нелегітимного абонента в іншому каналі зв'язку визначиться наступним чином: $P_{НА1К\_NO\_2К} = (1 - P_{НСВА}) P_{НСВА}$.

Імовірність наявності нелегітимного абонента в другому каналі зв'язку IP – телефонії при відсутності нелегітимного абонента в першому каналі зв'язку визначиться наступним чином:

$$P_{НА2К\_NO\_1К} = (1 - P_{НСВА}) P_{НСВА} = P_{НСВА} - P_{НСВА}{}^2.$$

$$P_{ВА2} = P_{НА1К\_NO\_2К} + P_{НА2К\_NO\_1К} = 2(1 - P_{НСВА}) P_{НСВА}.$$

Під успішної подією генерації загального секретного ключа розуміється, що нелегітимного абонента не виявлено ні в одному каналі зв'язку і абонентами генерації загального секретного ключа для шифрування потоку даних, які передаються по каналам зв'язку. Це можливо тільки в разі відсутності нелегітимного абонента в каналах зв'язку, або при використанні можливості алгоритму розподілу загальної секретної інформації визначати точне місцезнаходження нелегітимного абонента в конкретному (конкретних) каналах зв'язку. Імовірність успішної генерації секретного ключа $P_{УК2}$ для двоканального IP - протоколу відповідає імовірності відсутності нелегітимного абонента одночасно в обох каналах зв'язку. Імовірність відсутності нелегітимного абонента в одному каналі зв'язку $P_{NO\_НА}$:

$$P_{NO\_НА} = 1 - P_{НСВА} \quad \text{тоді:} \quad P_{УК2} = P_{NO\_НА}{}^2 = (1 - P_{НСВА})^2.$$

Розглянемо варіант виявлення нелегітимного абонента з використанням трьох каналів зв'язку IP – телефонії. Допустимо, що по трьох каналах зв'язку IP – телефонії передається однакова інформація обміну ключами Діффі-Хелмана. Приклад взаємодії абонентів при використанні модернізованого IP - протоколу ZRTP наведено на рис. 3. Ініціатор сеансу зв'язку відправляє по трьох каналах зв'язку IP – телефонії три однакових повідомлення. Інший абонент отримує повідомлення, проводить, при цьому необхідні обчислення, а також перевіряє, чи отримані повідомлення співпадають по трьох використовуваних каналах зв'язку. У випадку, неспівпадання повідомлень, активний нелегітимний абонент присутній в каналах зв'язку IP – телефонії, та виконує атаку типу «зустріч посередині» або активний нелегітимний абонент контролює одночасно всі три канали зв'язку IP – телефонії.

Абонент відповідає, відправляючи по відповідним трьом каналах зв'язку у відповідь інформацію отриману на основі IP - протоколу Діффі-Хелмана. Абонент сеансу отримує

повідомлення і перевіряє на співпадання отримані повідомлення В даній ситуації розглянемо декілька варіантів роботи IP - протоколу при використанні методу виявлення нелегітимного абонента: якщо порівнюванні повідомлення однакові – це означає, або відсутній активний нелегітимний абонент у всіх каналах зв'язку IP – телефонії, або існує активний нелегітимний абонент IP – телефонії у всіх трьох каналах зв'язку; якщо одне тільки повідомлення відрізняється від інших, в даній ситуації або присутній активний нелегітимний абонент в відповідному каналі зв'язку, або присутні два активних нелегітимних абоненти в двох інших каналах зв'язку IP – телефонії; у випадку якщо всі повідомлення різні, означає присутність двох окремо працюючих активних нелегітимних абонентів, які в даному випадку не мають між собою каналу зв'язку.

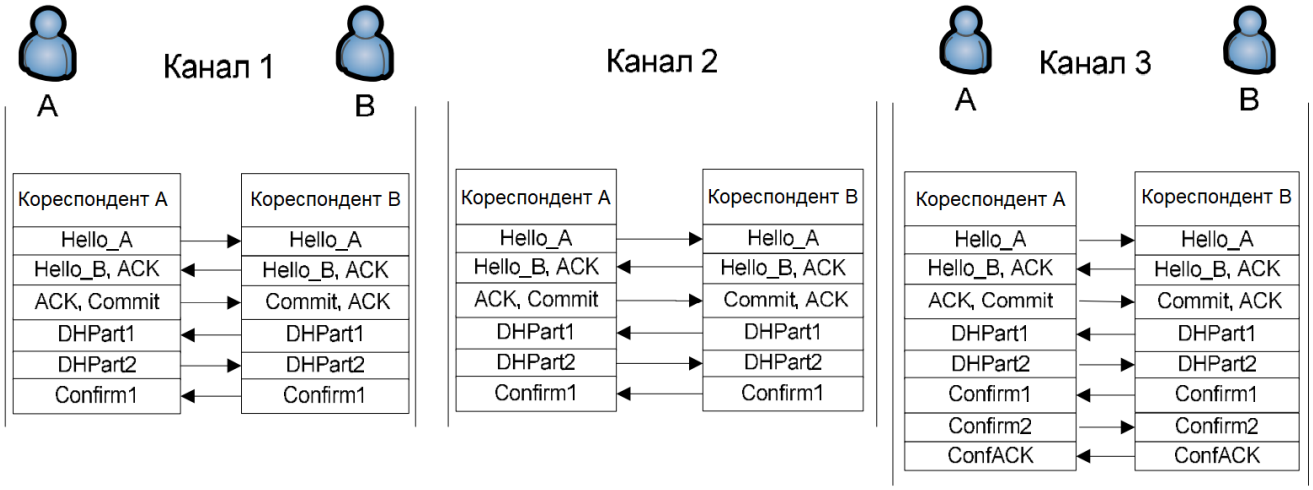


Рисунок 3 - Взаємодія кореспондентів при роботі одночасно по трьох каналах зв'язку

Таким чином, IP -протокол дозволяє: при наявності одного нелегітимного абонента в одному з трьох каналів зв'язку IP – телефонії визначити канал з нелегітимним абонентом; при наявності нелегітимного абонента одночасно в двох каналах зв'язку IP – телефонії виявити наявність нелегітимного абонента, при цьому без визначення каналів зв'язку IP – телефонії, що містять нелегітимного абонента. Однак, IP - протокол не дозволяє при знаходженні нелегітимного абонента одночасно в трьох каналах зв'язку IP – телефонії визначити наявність нелегітимного абонента. Таким чином, відповідно, можна виділити два режими роботи методу підвищення безпеки IP - телефонії: ВНА: режим роботи з виявленням нелегітимного абонента (З-ВНА); ВКНА: режим роботи з виключенням нелегітимного абонента (З-ВКНА).

При роботі в режимі ВНА в разі виявлення неспівпадання хоча б одного з трьох повідомлень – IP - протокол завершується з помилкою, повідомляючи користувача про присутність нелегітимного абонента в каналі зв'язку IP - телефонії. У разі роботи в режимі ВКНА при виявленні неспівпадання одного з трьох переданих повідомлень - формується повідомлення про наявність нелегітимного абонента в конкретному каналі зв'язку, IP - телефонії при цьому протокол продовжує роботу і при цьому контролює повідомлення в тих каналах зв'язку IP - телефонії, де не виявлено нелегітимного абонента. Таким чином забезпечується виключення нелегітимного абонента. Імовірність виключення нелегітимного абонента $P_{ПрВНА}$ для трьох канального IP - протоколу відповідає події присутності нелегітимного абонента в одному з каналів зв'язку IP - телефонії при його відсутності, в даному сеансі зв'язку, в двох інших каналах $P_{ПрВНА} = 3 \cdot P_{НСВ\_ЗАХОБЛ} \cdot \left(1 - P_{НСВ\_ЗАХОБЛ}\right)^2$.

Однак, при наявності активного нелегітимного абонента одночасно в двох каналах зв'язку із трьох використовуваних каналів, а також, при цьому синхронної модифікації повідомлень в двох каналах зв'язку IP - телефонії нелегітимним абонентом, використовуваний механізм виключення може викликати некоректне визначення каналу з нелегітимним

абонентом, що призведе, в даному випадку до помилкового вибору двох каналів зв'язку IP - телефонії, в яких присутній нелегітимний абонент, як надійних. Це дозволить нелегітимному абоненту успішно виконати обмін загальною секретною інформацією з абонентами сесії, здійснивши, при цьому успішну атаку типу «зустріч по середині». Імовірність помилкового виключення, в даному випадку відповідає ймовірності події, що нелегітимний абонент перебуває одночасно в двох каналах зв'язку IP - телефонії

$$P_{ПомВНА} = 3 \cdot P_{НСВ\_ЗАХОБЛ}{}^2 \cdot \left(1 - P_{НСВ\_ЗАХОБЛ}\right).$$

Ця ймовірність буде також складовою частиною ймовірності успішної атаки типу «зустріч посередині».

Виконаємо розрахунок ймовірностей для протоколу трьох канального обміну в режимі ВНА $P_{УА}$, $P_{ВА}$, $P_{УК}$.

Імовірність успішної атаки $P_{УАНА\_ВНА}$ Для тре канального протоколу в режимі ВНА відповідає ймовірності події, що нелегітимний абонент може прослуховувати і виконувати модифікацію повідомлень в трьох каналах зв'язку одночасно $P_{УАНА\_ВНА} = \left(P_{НСВ\_ЗАХОБЛ}\right)^3$.

Ймовірність виявлення нелегітимного абонента $P_{ВАНА\_ВНА}$ для трьох канального IP - протоколу Інтернет мережі в режимі ВНА відповідає ймовірності знаходження нелегітимного абонента в одному або двох каналах зв'язку при відсутності нелегітимного абонента в іншому каналі зв'язку. Імовірність присутності нелегітимного абонента в одному з каналів зв'язку IP – телефонії при відсутності нелегітимного абонента в двох інших каналах зв'язку:

$$P_{НА1К\_NO\_НА23К} = 3 \cdot \left(1 - P_{НСВ\_ЗАХОБЛ}\right)^2 \cdot P_{НСВ\_ЗАХОБЛ}$$

Імовірність наявності нелегітимного абонента в двох з трьох каналів зв'язку при відсутності нелегітимного абонента в одному з каналів зв'язку:

$$P_{НА23К\_NO\_НА1К} = 3 \cdot \left(1 - P_{НСВА}\right) \cdot P_{НСВА}{}^2$$

$$P_{ВАНА\_ВНА} = P_{НА1К\_NO\_НА23К} + P_{НА23К\_NO\_НА1К} =$$

$$= 3 \cdot \left(1 - P_{НСВА}\right)^2 \cdot P_{НСВА} + 3 \cdot \left(1 - P_{НСВА}\right) \cdot P_{НСВА}{}^2 \quad .$$

Імовірність успішної генерації загальної секретної інформації $P_{УКНА\_ВНА}$ для трьох канального IP - протоколу в режимі ВНА відповідає вірогідності відсутності нелегітимного абонента в трьох каналах зв'язку $P_{УКНА\_ВНА} = \left(1 - P_{НСВ\_ЗАХОБЛ}\right)^3$.

Виконаємо розрахунок ймовірностей $P_{УА}$, $P_{ВА}$, $P_{УК}$ для протоколу трьох канального обміну в режимі ВКНА.

Імовірність успішної атаки $P_{УАНА\_ВКНА}$ для трьох канального протоколу відповідає ймовірності події, що нелегітимний абонент може прослуховувати і виконувати модифікацію повідомлень в двох або трьох каналах зв'язку одночасно.

$$P_{УАНА\_ВКНА} = P_{НСВ\_ЗАХОБЛ}{}^3 + 3 \cdot \left(1 - P_{НСВ\_ЗАХОБЛ}\right) \cdot P_{НСВЗАХОБЛ}{}^2.$$

Ймовірність виявлення нелегітимного абонента $P_{ВАНА\_ВКНА}$ для трьох канального протоколу в режимі ВКНА відповідає ймовірності знаходження нелегітимного абонента в одному каналі зв'язку при відсутності нелегітимного абонента в двох інших каналах зв'язку і буде мати вигляд $P_{ВАНА\_ВКНА} = 3 \cdot \left(1 - P_{НСВ\_ЗАХОБЛ}\right)^2 \cdot P_{НСВ\_ЗАХОБЛ}$.

Імовірність успішної генерації загальної секретної інформації $P_{УКНА\_ВКНА}$ для трьох канального IP - протоколу в режимі ВКНА відповідає вірогідності відсутності нелегітимного абонента в двох або трьох каналах зв'язку

$$P_{УКНА\_ВКНА} = \left(1 - P_{НСВ\_ЗАХОБЛ}\right)^3 + 3 \cdot \left(1 - P_{НСВ\_ЗАХОБЛ}\right)^2 \cdot P_{НСВ\_ЗАХОБЛ} .$$

Для простого IP – протоколу обміну ключами Діффі-Хелмана, що працює по одному каналу зв'язку, наступні ймовірності матимуть вигляд $P_{У\_ЗАХОБЛ} = P_{НСВ\_ЗАХОБЛ}$, $P_{В\_ЗАХОБЛ1} = 0$, $P_{УК1} = 1 - P_{НСВ\_ЗАХОБЛ}$.

Модифікація IP - протоколу при роботі одночасно по декількох незалежних каналах зв'язку істотно зменшує ймовірність проведення успішної атаки «зустріч по середині». Ефективність захисту зростає зі збільшенням числа незалежних каналів зв'язку IP - телефонії. Модифікація в режимі виявлення нелегітимного абонента з використанням трьох каналів зв'язку, в даному випадку має найбільшу ймовірність виявлення нелегітимного абонента, а також, при цьому найменшу ймовірність успішної атаки нелегітимного абонента. Модифікація в режимі виключення нелегітимного абонента із застосуванням декількох (трьох) каналів має найбільшу ймовірність успішної генерації загальної секретної інформації між учасниками зв'язку. Для реалізації вибирається одна з модифікацій в залежності від цілей і доступних ресурсів, виражених в числі доступних каналів зв'язку.

Результати проведених досліджень показують, що при підключенні абонентів одночасно до декількох операторів зв'язку IP – телефонії незалежні двійки маршрутів присутні завжди. Імовірність успішного формування загальної секретної інформації при використанні багатоканальної схеми з виявленням нелегітимного абонента при цьому зменшується незначно. У схемі з виключенням нелегітимного абонента ймовірність збільшується, але при використанні каналів зв'язку IP – телефонії великої протяжності можливо співпадання вузлів проходження маршрутів потоку даних, що, в даному випадку, може призвести до зниження ефективність роботи модифікованого IP - протоколу.

Висновки. Запропоновано метод підвищення захищеності IP – телефонії та безпеки програмного розподілу загальної секретної інформації, що відрізняється від існуючого методу виявлення нелегітимного абонента, впровадженням автоматизованої програмно-апаратної перевірки аутентифікаційного рядка. При використанні в даному випадку декілька каналів зв'язку, відповідна перевірка надасть можливість виявити нелегітимного абонента.

IP - протокол з програмною перевіркою аутентифікаційного рядка IP- телефонії не надає можливості визначити, на який саме канал зв'язку нелегітимний абонент буде виконувати активну атак. Також виявлення нелегітимного абонента в каналі зв'язку можливе тільки після успішного повного завершення роботи протоколу, нелегітимний абонент не може бути виявленим протягом роботи протоколу. Таким чином виникає необхідність розгляду додаткових варіантів модифікації IP - протоколу IP – телефонії ZRTP, із врахуванням наведених недоліків.

ЛІТЕРАТУРА:

1. Джулій, В.М. Модель нелегітимного абонента забезпечення безпеки IP-телефонії / О.С. Андрощук, В.М. Джулій, Ю.П. Кльоц, І.В. Муляр // Вимірювальна та обчислювальна техніка в технологічних процесах. – Хмельницький, 2020. – №2. – С. 38–45.

2. Бабаш, А.В. Криптографические методы защиты информации: учебник для студетнов вузов / А. В. Бабаш, Є. К. Баранова. - М. : КНОРУС, 2016. - 190 с.

3. Борисов, М.А. Основы для программно-аппаратной защиты информации: учеб. пособие для вузов / М. А. Борисов, И. В. Заводцев, И. В. Чижов. - 4-е изд., переработаное и доп. - М. : ЛЕНАНД, 2016. - 416 с.

4. Васильева, И. И. Криптографические методы защиты информации: практикум и учебник для академ. бакалавриата / И. И. Васильева. - Санкт-Петерб. гос. эконом. университет. - М. : Юрайт, 2017. - 349 с.

5. Нестеров, С.А. Основы информационной безопасности: учебник / С. А. Нестеров. - СПб. : Лань, 2017. – 423 с.

6. Олифер, В.Г. Безопасность компьютерных сетей / В. Г. Олифер, Н. А. Олифер. - М. : Горячая линия-Телеком, 2017. - 644 с.

7. Основы программно-аппаратной защиты информации. / М. А. Борисов, И. В. Заводцев, И. В. Чижов. – М.: УРСС: Либроком, 2013. – 370 с.

8. Касперский, Е. В. «Компьютерное зловредство» / Е. В. Касперский. – Санкт-петербург: Питер, 2009. – 208 с.

9. Партыка, Т. Л. Информационная безопасность учебное пособие / Т. Л. Партыка, И. И. Попов. – М.: ФОРУМ, 2011. – 432 с.

10. Сердюк, В. А. Организация и технологии защиты информации / В. А. Сердюк. – М.: Издательский дом Государственного университета – Высшей школы экономики, 2011. – 571 с.

11. Шаньгин, В. Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. - М. : ДМК Пресс, 2017. - 702 с.

REFERENCES:

1. Dzhulii, V.M. Model nelehitymnoho abonenta zabezpechennia bezpeky IP-telefonii / O.S. Androshchuk, V.M. Dzhulii, Yu.P. Klots, I.V. Muliar // Vymiriuvalna ta obchysliuvalna tekhnika v tekhnolohichnykh protsesakh. – Khmelnytskyi, 2020. – №2. – Pp. 38–45.

2. Babash, A.V. and Baranova, Ye. K. (2016), “Kryptohrafycheskye metodы zashchytы ynformatsyy : uchebnyk dlia studetnov vuzov” / M. : KNORUS, 190 p.

3. Borysov, M.A., Zavodtsev, Y.V. and Chyzhov Y.V.(2016), “Osnovы dlia prohrammno-apparatnoi zashchytы ynformatsyy : ucheb. posobye dlia vuzov” / M. : LENAND, 416 p.

4. Vasyleva, Y.Y. (2017),_”Kryptohrafycheskye metodы zashchytы ynformatsyy : praktykum y uchebnyk dlia akadem. Bakalavryata” / M. : Yurait, 349 p.

5. Nesterov, S.A. (2017), “Osnovы ynformatsyonnoi bezopasnosty : uchebnyk” / SPb. : Lan, 423 p.

6. Olyfer, V.H. and Olyfer, N. A. (2017), “Bezopasnost kompiuternыkh setei” / M. : Horiachaia lynyia-Telekom, 644 p.

7.. Borisov, M. A., Zavodcev, I. V. and CHizhov, I. V. (2013), ”Osnovy programmno-apparatnoj zashchity informacii” / M.: URSS: Librokom,. 370 p.

8. Kasperskij, E. V. (2009), ”Komp'yuternoe zlovredstvo”, Sankt-peterburg: Piter,. 208 p.

9. Partyka, T. L. and Popov, I. I. (2011), ”Informacionnaya bezopasnost' uchebnoe posobie” / M.: FORUM, 432 p.

10. Serdyuk, V. A. (2011), ”Organizaciya i tekhnologii zashchity informacii ” / M.: Izdatel'skij dom Gosudarstvennogo universiteta – Vysshej shkoly ekonomiki,. 571 p.

11. SHan'gin, V. F. (2017), ”Ynformatsyonnaia bezopasnost y zashchyta ynformatsyy” / M.: DMK Press, 702 p.

PhD Dzhulij A.V., PhD Chornenky V.I.

METHOD OF IMPROVING THE EFFICIENCY OF THE SAFE IR-TELEPHONY KEY DISTRIBUTION PROCEDURE BASED ON THE DIFFY-HELMAN ALGORITHM

The paper proposes a method to improve the efficiency of the secure IP-telephony key distribution protocol based on the Diffie-Hellman algorithm, which differs from the existing method for detecting an illegitimate subscriber by introducing an automated software and hardware verification of the authentication string. If several communication channels are used in this case, an appropriate check will reveal an illegitimate subscriber. Solves the following tasks: makes it possible to identify an active illegitimate correspondent using voice synthesis software; to identify an active illegitimate correspondent of IP - protocols in the communication channels of Internet telephony in the absence of previously distributed secret key information between the correspondents of the trusted center. The results of the study allow us to indicate that the most well-known IP-protocols for the distribution of general secret information need to be improved in two directions: increasing the information security of IP-telephony and improving the main indicators of IP-protocols of Internet networks. The most dangerous attack is a meeting-in-the-middle attack on IP protocols for the distribution of shared secret information. The task of forming general secret information in the context of a "meeting in the middle" attack of an illegitimate correspondent's invasion is relevant at the present stage. One of the methods to improve the security of the IP protocol for the formation of general secret information is to monitor and prohibit the execution of an attack of the "meeting in the middle" type due to the use of several parallel independent channels of communication sessions in the Internet IP - telephony networks. Knowing the vulnerability and the level of protection of the object for which it is necessary to carry out protection, an active illegitimate correspondent can perform a combination of attacks that can lead to gaining unauthorized access to the object's data.

A method for identifying an active illegitimate IP subscriber is proposed - protocols for the distribution of shared secret information based on the Diffie-Hellman key exchange algorithm, the feature of the method is the use of several open communication channels. Provides a decrease in the likelihood of a successful "meeting in the middle" attack by an active illegitimate subscriber, as well as the presence of a mechanism for identifying an active attacker in the communication channel in the absence of previously distributed shared secret information. The method imposes restrictions on the communication channels used, in the sense that the communication channels must be independent.

Key words: illegitimate correspondent, information interaction, Internet telephony, cryptographic protection, communication channels, key distribution.

УДК 004.56:61

д.т.н., проф. **Лукова-Чуйко Н.В.** (КНУ)
д.т.н., проф. **Толюпа С.В.** (КНУ)
к.є.н, доц. **Погасій С.С.** (ХНЕУ)
Лаптєва Т.О. (КНУ)
Лаптєв С.О. (КНУ)

DOI: https://doi.org/10.17721/2519-481X/2021/73-10

УДОСКОНАЛЕННЯ МОДЕЛІ ЗАХИСТУ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ

В Україні право на приватність – це конституційна гарантія, а захист персональних даних – одна із сфер, у якій така гарантія має реалізовуватись. Предметом нашого дослідження будуть не об'єкти взагалі, а динамічні системи захисту інформації в соціальних мережах у математичному розумінні цього терміну. Описи динамічних систем для різноманітних задач в залежності від закону еволюції різноманітні: за допомогою диференціальних рівнянь, дискретних відображень, теорії графів, теорії марківських ланцюгів тощо. Вибір одного із способів опису задає конкретний вигляд математичної моделі відповідної динамічної системи. Теоретичне дослідження динамічної поведінки реального об'єкта вимагає створення його математичної моделі. Більшість відомих підходів до моделювання, відрізняються тім, які параметри при моделюванні ними використовують в якості вхідної інформації та які характеристики модельованої системи розраховуються та надходять на вихід моделі. В роботі дослідження моделей захисту інформації. Продовжуються розробка математичної моделі захисту інформації в соціальної мережі в залежності від специфічних її параметрів. Модель удосконалюється за рахунок врахування специфіки соціальних мереж. Таких як: довіра, репутація, вплив загроз безпеки даних від розповсюдження інформації між користувачами, вплив загроз безпеки даних від взаємовпливів користувачів, вплив загроз безпеки даних від взаємодії користувачів та вплив загроз безпеки даних від довжини шляху між користувачами. Однак слід означити, що параметрів соціальної мережи значно більше. Але ці параметри ми вважаємо найбільш впливовими. Тому приділяємо увагу саме на цих специфічних параметрах.

Проведено математичне моделювання удосконаленої моделі захисту інформації у соціальної мережі в залежності від специфічних її параметрів. При моделювання введені обмеження та припущення які дозволили отримати графічні результати. Графічні результати відображають актуальну картину захисту інформації соціальної мережи від зовнішніх впливів. Отримані результати підтверджують адекватність розробленої математичної моделі захисту інформації у соціальної сеті.

Ключові слова: соціальна мережа, довіра, репутація, моделювання, коефіцієнт захисту, безпека, захист інформації

Вступ та постановка задачі. Виходячи з реалій сьогодення ефективність функціонування будь-якої організації, підприємства та держави залежить не тільки від надійності функціонування інформаційно - телекомунікаційних систем, а й у значній мірі від захищеності їх інформаційних ресурсів та інформації взагалі.

Предметом нашого дослідження будуть не об'єкти взагалі, а динамічні системи захисту інформації в соціальних мережах у математичному розумінні цього терміну.

Описи динамічних систем для різноманітних задач в залежності від закону еволюції різноманітні: за допомогою диференціальних рівнянь, дискретних відображень, теорії графів, теорії марківських ланцюгів тощо. Вибір одного із способів опису задає конкретний вигляд математичної моделі відповідної динамічної системи [1 - 4]. Теоретичне дослідження динамічної поведінки реального об'єкта вимагає створення його математичної моделі. У багатьох випадках процедура розробки моделі полягає в складанні математичних рівнянь на основі фізичних законів. Зазвичай ці закони формулюються на мові диференціальних рівнянь. В результаті координати стану системи і її параметри виявляються пов'язаними між собою, що дозволяє приступити до вирішення диференціальних рівнянь при різних початкових

умовах і параметрах. Тому розробка нових та удосконалених методів підвищення рівня захищеності інформаційного простору соціальних мереж, які базуються на математичних моделях динамічних систем є дуже актуальною.

Аналіз останніх досліджень. Більшість відомих підходів до моделювання, відрізняються тім, які параметри при моделюванні ними використовують в якості вхідної інформації та які характеристики модельованої системи розраховуються та надходять на вихід моделі (будують моделі з Використання теорії ймовірностей, випадкових процесів, мереж Петрі, теорії автоматів, теорії графів, нечітких множини, теорії катастроф, ентропійного підходу та ін.).

При цьому аналітичні моделі, що розглядаються з позиції теоретичної математики не тотожні реальної дійсності, зважаючи на обмежену точність результатів. [1,3].

У [2,4] розглядається модель інформаційної безпеки на основі Марковських випадкових процесів. Отримані чисельні значення, однак вони розглядають питання загрози уразливості. Питання загроз уразливості не торкається питання взаємозалежності основних параметрів моделі, що можливо призводить до ускладнення моделювання процесу.

У [5] звертається увага на нестійкість і отже, великі варіації отриманих рішень при поганій обумовленості систем лінійних алгебраїчних рівнянь і неточно заданих значень ефектів і результатів спостережень. Це пов’язане з питанням не врахування взаємозалежності основних параметрів

Разом з тим у всіх зазначених джерелах математичне моделювання розглядається як математична модель конкретних параметрів (деякі параметри мають імовірнісний характер) Питання взаємозв'язку вхідних параметрів при моделюванні процесів глибину їх взаємозв'язку моделі не розглядають. Ці чинники взаємозв'язку і взаємовпливу можуть істотно спотворити результати моделювання і поставити під сумнів адекватність моделі.

В роботах [6,11] досліджуються моделі окремих складових специфічних параметрів мережі. В роботі [7] розглянуто метод розрахунку захисту інформації від репутації користувачів при нелінійній залежності параметрів. В статях [8,12] досліджуються загальні параметри безпеки в мережах. В роботах [9] вказуються ризики безпеки в соціальних мережах. В статях [10,15] розглядається захист в соціальних мережах від небажаної інформації. В роботі [16] розглядається захист персональної інформації користувачів. В статті [17] - метод розрахунку захисту інформації від взаємовпливу користувачів в соціальних мережах.

Разом з тим у всіх зазначених джерелах математичне моделювання розглядається як математична модель конкретних параметрів (деякі параметри мають імовірнісний характер) Питання взаємозв'язку вхідних параметрів при моделюванні процесів глибину їх взаємозв'язку моделі не розглядають. Ці чинники взаємозв'язку і взаємовпливу можуть істотно спотворити результати моделювання і поставити під сумнів адекватність моделі

Таким чином, на даний час в практиці і теорії побудови та експлуатації соціальних мереж існує об’єктивне протиріччя між необхідністю підвищення рівня захищеності інформації в соціальних мережах та недосконалістю системи захисту інформації соціальних та можливостями існуючих методів, які використовуються системою захисту інформації в соціальних мережах. Тому розробка та удосконалення математичних моделей захисту інформації у соціальних мережах є актуальним завданням.

Метою роботи є удосконалення моделі захисту даних у соціальної мережи за рахунок врахування специфіки соціальних мереж. Таких як: довіра, репутація, вплив загроз безпеки даних від розповсюдження інформації між користувачами, вплив загроз безпеки даних від взаємовпливів користувачів, вплив загроз безпеки даних від взаємодії користувачів та вплив загроз безпеки даних від довжини шляху між користувачами.

Виклад основного матеріалу. Математична модель динамічної системи вважається заданою, якщо введені параметри (координати) системи, що визначають однозначно її стан, і зазначений закон еволюції. Залежно від ступеня наближення одній і тій самій системі можуть бути поставлені у відповідність різні математичні моделі.

Теоретичне дослідження динамічної поведінки реального об'єкта вимагає створення його математичної моделі. У багатьох випадках процедура розробки моделі полягає в складанні математичних рівнянь на основі фізичних законів. Зазвичай ці закони формулюються на мові диференціальних рівнянь. В результаті координати стану системи і її параметри виявляються пов'язаними між собою, що дозволяє приступити до вирішення диференціальних рівнянь при різних початкових умовах і параметрах.

У класичному підході до захисту даних розрізняють:

$$T_i = \left[D_j, D_n, D_m, D_k \right], \quad (1)$$

де T_i – множина загроз від втрати довіри між користувачами;

D_j – довіра на надання послуг, людина довіряє стороні в наданні якісних послуг провайдером послуг або ресурсів;

D_n – довіра делегування (delegation trust) описує довіру в користувача (представника), що діє і виносить рішення від імені сторони, якій довіряє;

D_m – довіра доступу (access trust) описує довіру довіряє зі сторони (провайдера) до користувача, яким надається доступ до ресурсів. Це – контроль доступу. Використовується в системах автентифікації;

D_k – контекстна довіра визначає міру віри учасника в необхідні системи та інституційні механізми, що підтримують транзакції і забезпечують безпеку мережі.

Втрата такої якості, як довіра – процес, який має часовий інтервал [4,11]. Позначимо кількість інформації в системі – I. Потік інформації за межі інформаційної системи через *dI*–, швидкість зміни цього потоку – $\frac{dI}{dt}$. Логічне, що якщо потік і швидкість зміни потоку дорівнюють нулю, то витоку інформації немає:

$$dI = 0; \frac{dI}{dt} = 0 \quad . \quad (2)$$

Витік інформації залежить від захищеності системи – вжитих заходів з нейтралізації загроз безпеки даних. Z – показник захищеності інформаційної системи. Загалом витік інформації залежить:

- від розміру інформаційної системи (отже, в якійсь мірі і від кількості даних);
- від швидкості витоку даних
- витік інформації купірується захищеністю системи (заходами щодо нейтралізації загроз безпеки інформації).

Тоді з урахуванням введених позначень, отримуємо рівняння для швидкості витоку інформації:

$$\frac{dI}{dt} = Z_p Z + (C_v + C_k) I \quad , \quad (3)$$

де Z_p – коефіцієнт, що відображає вплив заходів щодо захисту інформації;

Cv – коефіцієнт, що відображає вплив швидкості витоку даних;

C_k – коефіцієнт, що відображає вплив кількості даних на їх витік.

Для подальшого виведення моделі захисту інформації будемо розглядати захищеність системи (Z). Для цього визначимо захищеність системи як здатність системи протистояти несанкціонованому доступу до конфіденційної даних. Отже, захищеність системи буде залежати:

- від розмірів системи (як і від кількості даних);
- загроз безпеки інформації від втрати довіри між користувачами.

Тоді з урахуванням введених позначень, отримуємо рівняння для можливості швидкого захисту інформації від витоку:

$$\frac{dZ}{dt} = D_i - I(C_{d2} + C_{d1}) \ , \tag{4}$$

де D_i – коефіцієнт, що відображає вплив загроз безпеки даних від втрати довіри між користувачами на захищеність інформаційної системи.

C_{d2} – коефіцієнт, що відображає вплив розмірів системи на захищеність;

C_{d1} – коефіцієнт, що відображає вплив захищеності на витік даних.

Тоді отримуємо систему рівнянь. Яка складається з рівнянь (3) і (4):

$$\begin{cases} \frac{dI}{dt} = Z_p Z + (C_v + C_K) I \\ \frac{dZ}{dt} = D_i - I(C_{d2} + C_{d1}) \end{cases} . \tag{5}$$

Але система рівнянь (5) є базовою системою, має лінійних характер. Це відповідає процесу захисту інформації у де яких випадках. Які більш носять стаціонарні вже вивчені процеси впливу на захист інформації.

Тому головною відмінністю нашої моделі на першому етапі, е модель яка відрізняється наявністю «малого параметру». Тобто для рішення потрібно використовуватися спеціальні методи. Малий параметр у нашому випадку буде змінюватися по випадковому закону. Це обумовлено відсутністю чітко визначених законів витоку або пошкодження інформації. Система рівнянь прийме вигляд:

$$\begin{cases} \frac{dI}{dt} = Z_p Z + \varepsilon(C_v + C_K) I \\ \frac{dZ}{dt} = D_i - I(C_{d2} + C_{d1})\varepsilon \end{cases} , \tag{6}$$

Знайдемо стаціонарну позицію системи, що описується рівняннями (6). Умови стаціонарності $dI = 0; \frac{dI}{dt} = 0$. Отже:

$$\begin{cases} Z_p \bar{Z} + \varepsilon(C_v + C_K) \bar{I} = 0 \\ D_i - I(C_{d2} + Cd_1)\varepsilon = 0 \end{cases} . \tag{7}$$

З другого рівняння системи слідує:

$$\bar{I} = \frac{D_i}{(C_{d2} + C_{d1})\varepsilon} \ . \tag{8}$$

Далі з першого рівняння системи рівнянь (6) знаходимо $\bar{Z}$.

$$Z_p \bar{Z} - \frac{(C_v + C_K) D_i}{(C_{d2} + C_{d1})\varepsilon} = 0 \ , \tag{9}$$

$$\bar{Z} = \frac{(C_v + C_K) D_i)}{(C_{d2} + C_{d1})\varepsilon Z_p} \ . \tag{10}$$

Результати обрахунків за рівнянням (9)

Отже, умови позиції стаціонарності системи:

$$\begin{cases} \bar{I} = \dfrac{D_i}{(C_{d2} + Z_p)\varepsilon} \\ \bar{Z} = \dfrac{(C_v + C_K)D_i}{(C_{d2} + C_{d1})\varepsilon Z_p} \end{cases}. \quad (11)$$

Вирішимо систему рівнянь (6) методом «малих відхилень»

$I = \bar{I} + I; Z = \bar{Z} + Z$:, отже, система рівнянь прийме вигляд:

$$\begin{cases} \dfrac{dI}{dt} = Z_p(\bar{Z} + Z) + (C_v + C_K)(\bar{I} + I) \\ \dfrac{dZ}{dt} = D_i - (\bar{I} + I)(C_{d2} + C_{d1})\varepsilon \end{cases}, \quad (12)$$

$$\begin{cases} \dfrac{dI}{dt} = (C_{d1} + C_{d2})\varepsilon Z - (C_v + C_K)I \\ \dfrac{dZ}{dt} = -I(C_{d2} + C_k) + D_i) \end{cases}. \quad (13)$$

Ця система диференціальних рівнянь е математичною моделлю захисту інформаціє у соціальної мережи від такого параметра, як довіра між користувачами.

Удосконалена математична модель системи захисту даних в соціальної мережи з урахуванням взаємовідносин користувачів

З метою розробки математичної моделі системи захисту даних в соціальній мережі з урахуванням взаємовідносин користувачів, введемо параметри взаємовідносин. Тоді математична модель буде представлена такою системою диференціальних рівнянь:

$$\begin{cases} \dfrac{dI}{dt} = Z_p Z + (C_v + C_K)I \\ \dfrac{dZ}{dt} = (\alpha + \beta + \theta + \rho)V - I(C_{d2} + C_{d1})\varepsilon \end{cases}, \quad (14)$$

де V_i – коефіцієнт, що відображає вплив загроз безпеки даних від взаємодії між користувачами на захищеність інформаційної системи, параметр;

α - описує схильність суб'єкта до встановлення взаємодії;

β - описує привабливість або популярність;

θ – оцінка довіри;

ρ – характеристика тенденцій моделі до симетричності діад.

$$\begin{cases} \dfrac{dI}{dt} = Z_p Z + (C_v + C_K)I + L_2(I^2) + L_3(I^3) + \ldots \\ \dfrac{dZ}{dt} = (\alpha + \beta + \theta + \rho)V - I(C_{d2} + C_{d1}) + K_2(Z^2) + K_3(Z^3) + \ldots \end{cases}. \quad (15)$$

де L_2, L_3 і т.д. K_2, K_3 і т.д. деякі лінійні оператори. Будемо вважати не лінійність системи слабкою, що дозволяє шукати рішення для кожного рівняння системи (24) методом послідовного наближення, поклавши:

$$I = I_1 + I_2 + I_3 ...$$
$$Z = Z_1 + Z_2 + Z_3 + ...$$

Нехай при

$$dI = 0, \ \frac{dI}{dt} = 0, \text{ та } dZ = 0, \ \frac{dZ}{dt} = 0$$
$$I = I_0 \operatorname{Sin} \omega t, Z = Z_0 \operatorname{Sin} \omega t .$$

Отримаємо систему рівнянь:

$$\begin{cases} \frac{dI}{dt} = Z_p Z + (C_v + C_K) I - L_2 (I_0{}^2 \operatorname{Sin}^2 \omega t) - L_3 (I_0{}^3 \operatorname{Sin}^3 \omega t) - ... \\ \frac{dZ}{dt} = (\alpha + \beta + \theta + \rho) V - I (C_{d2} + C_{d1}) \varepsilon - K_2 (Z_0{}^2 \operatorname{Sin}^2 \omega t) - K_3 (Z_0{}^3 \operatorname{Sin}^3 \omega t) - ... \end{cases} . \quad (16)$$

Перепишемо систему і представимо її в такому вигляді:

$$\begin{cases} \frac{dI}{dt} = \alpha Z + \beta_1 I - \sum_{k=2}^{\infty} L_k I_0^k \sin^k \omega t, \\ \frac{dZ}{dt} = \beta_2 \varepsilon I + \gamma - \sum_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t, \end{cases} , \quad (17)$$

де $\alpha = Z_p$, $\beta_1 = C_v + C_K$, $\beta_2 = -\left(C_{d2} + C_{d1}\right)$, $\gamma = (\alpha + \beta + \theta + \rho) V$

Система рівнянь (17) є математичною моделлю захисту інформації в у соціальної мережи з урахуванням такого специфічного параметра як взаємовідносини між користувачами. Слід зазначити, що у нашої моделі присутній «малий параметр». Малий параметр у нашому випадку буде змінюватися по випадковому закону. Це обумовлено відсутністю чітко визначених законів витоку або пошкодження інформації у залежності від взаємовідносин користувачів. Тобто для рішення потрібно використовуватися спеціальні методи. Тому будемо використаємо метод винятків:

$$\frac{dZ}{dt} = \beta_2 I + \gamma - \sum_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t \Rightarrow I = \frac{1}{\beta_2} \left(\frac{dZ}{dt} - \gamma + \sum_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t \right) \Rightarrow$$
$$\frac{dI}{dt} = \frac{1}{\beta_2} \left(\frac{d^2 Z}{dt^2} + \frac{1}{\omega} \sum_{k=2}^{\infty} \left(k K_k Z_0^k \sin^{k-1} \omega t \cos \omega t \right) \right) . \quad (18)$$

Підставимо всі найдені вирази в перше рівняння системи (6):

$$\frac{1}{\beta_2} \left(\frac{d^2 Z}{dt^2} + \frac{1}{\omega} \sum_{k=2}^{\infty} \left(k K_k Z_0^k \sin^{k-1} \omega t \cos \omega t \right) \right) = \alpha Z + \frac{\beta_1}{\beta_2} \left(\frac{dZ}{dt} - \gamma + \sum_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t \right) -$$
$$- \sum_{k=2}^{\infty} L_k I_0^k \sin^k \omega t \ , \quad (19)$$

або:

$$\frac{d^2 Z}{dt^2} - \beta_1 \frac{dZ}{dt} - \alpha \beta_2 Z = -\frac{1}{\omega} \sum_{k=2}^{\infty} \left(k K_k Z_0^k \sin^{k-1} \omega t \cos \omega t \right) - \beta_1 \gamma + \beta_1 \sum_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t -$$

$$-\beta_2 \sum_{k=2}^{\infty} L_k I_0^k \sin^k \omega t \,. \tag{20}$$

Тепер знаходимо спільне рішення відповідного однорідного рівняння:

$$Z'' - \beta_1 Z' - \alpha\beta_2 Z = 0 \ . \tag{21}$$

Характеристичне рівняння має вигляд: $\lambda^2 - \beta_1\lambda - \alpha\beta_2 = 0$. Розглянемо випадок позитивного дискримінанту цього рівняння:

$$D = \beta_1^2 + 4\alpha\beta_2 > 0 \Rightarrow \lambda_{1,2} = \frac{\beta_1 \pm \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2} \,. \tag{22}$$

Звідкіля:

$Z_{одн}(t) = c_1 e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t} + c_2 e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}$ - спільне рішення однорідного рівняння.

Для знаходження загального рішення неоднорідного рівняння скористаємося методом варіації довільних сталих: $Z_{одн}(t) = c_1(t) e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t} + c_2(t) e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}$.

де $c_1'(t), c_2'(t)$ знаходяться із системи:

$$\begin{cases} c_1'(t) e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t} + c_2'(t) e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t} = 0, \\ c_1'(t) \dfrac{\beta_1 + \sqrt{\beta_1^2+4\alpha\beta_2}}{2} e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t} + c_2'(t) \dfrac{\beta_1 - \sqrt{\beta_1^2+4\alpha\beta_2}}{2} e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t} = N(t), \end{cases} \tag{23}$$

Остаточно:

$$\begin{aligned} Z(t) = \int N(t) - e^{\frac{-\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t} \frac{e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}}{\sqrt{\beta_1^2+4\alpha\beta_2}} dt - \\ - \int N(t) - e^{\frac{-\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t} \frac{e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}}{\sqrt{\beta_1^2+4\alpha\beta_2}} dt \end{aligned} \tag{24}$$

де

$$\begin{aligned} N = -\frac{1}{\omega} \sum_{k=2}^{\infty} \left(k K_k Z_0^k \sin^{k-1} \omega t \cos \omega t \right) - \\ - \beta_1 \gamma + \beta_1 \sum_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t - \beta_2 \sum_{k=2}^{\infty} L_k I_0^k \sin^k \omega t \end{aligned} \ . \tag{25}$$

Система рівнянь (24) є математично моделлю системи захисту інформації з урахуванням такого специфічного параметра, як взаємовідносини між користувачами.

Вираз (25) є остаточним математичним результатом побудови цей моделі.

Удосконалення моделі захисту інформації за рахунок урахування взаємозв'язку користувачів

Для розробки моделі захисту інформації в залежності від взаємовпливу користувачів, необхідно доповнити систему рівнянь (23) параметром, який буде враховувати взаємодію між користувачами.

З цей метою візьмемо за основу Марьківську модель, яка найбільш адекватна для вирішення цього питання. Це обумовлено тім , що графічні моделі графів Маркова цілком

відповідають взаємозв'язку між користувачами. Взаємозв'язок між користувачами в цих моделях, цілком залежить від кількості користувачів. Які у свою чергу будуть являтися вершинами графа. Це цілком відповідає поставленому завданню, визначенню взаємозв'язків між користувачами. В зв'язку з тім, що Моделі Маркова достатньо вивчені, повносю модель описувати не будемо, обмежимось тільки визначенням коефіцієнту взаємозв'язку. Який буде визначатися наступним виразом:

$$Kv = (\frac{\sum_{v \in V} C_{v1}}{n^2}). \quad (26)$$

де $\sum_{v \in V} C_{v1}$ – загальна кількість з'єднань в мережі,

n –кількість вершин в мережі.

Тоді удосконалена модель прийме вигляд:

$$\begin{cases} \frac{dI}{dt} = Z_p Z + (C_v + C_K) I \\ \frac{dZ}{dt} = (\alpha + \beta + \theta + \rho) V - I(C_{d2} + C_{d1})\varepsilon + (\frac{\sum_{v \in V} C_{v1}}{n^2}) \end{cases} . \quad (27)$$

Але специфіка соціальної мережи, специфічні параметри її потрібують більш ширшого розгляду. Наприклад соціальні мережи швидко розвіваються, але все ж таки мають обмеження. Це пов'язано з можливість мережи, зберігати та передавати дані. З цей метою будемо використовувати емпіричну модель. Особливістю застосування у нашому випадку буде те, що ми використовуємо епідемічну модель з ймовірністю передачі певної інформації, як функції відстані між джерелом і потенційною метою.

Тобто ймовірність, що m-й сусід передає цю інформацію особі, з яким він буде контактувати визначається як:

$$y = N_{knot}(r+1)^{-f} . \quad (28)$$

де: f>0 – ймовірна функція передачі інформації;

r –кількість користувачів з якими може поділитися даний користувач інформацією;

N_{knot} –користувач мережі, який знаходиться на визначеному вузлі.

З урахування вищевикладеного модель захисту параметрів у соціальної мережи прийме вигляд:

$$\begin{cases} \frac{dI}{dt} = Z_p Z + (C_v + C_K) I \\ \frac{dZ}{dt} = (\alpha + \beta + \theta + \rho) V - I(C_{d2} + C_{d1})\varepsilon + \\ +(\frac{\sum_{v \in V} C_{v1}}{n^2}) + N_{knot}(r+1)^{-f} \end{cases} . \quad (29)$$

Удосконалення моделі захисту інформації за рахунок урахування центральності мережі

Метрики центральності – це кількісна оцінка тієї чи іншої особи в соціальній мережі. Міра центральності описує випуклість конкретного вузла в порівнянні з іншими вузлами. Середня міра центральності також відома як централізована оцінка, вона вказує, наскільки щільний граф по відношенню до кожного вузла. Центральні метрики, як правило, обчислюються на підставі всієї структури мережі або під графа.

Ступінь (рівень) центральності вузла (degree centrality) – це число зв'язків даного вузла з іншими вузлами. Використовувати такий вид центральності найкраще, коли необхідно

визначити людей, які вибирають Вас і з яким Ви віддаєте перевагу взаємодії [10] або, навпаки, від яких хочете триматися подалі. Формально ступінь центральності вузла можна представити в наступному вигляді :

$$C_D(i) = \sum_{j=1}^{n} a(i, j), \tag{30}$$

де CD (*i*) – степінь центральності вузла *i*;

a(*i,j*) – зв'язок між вершинами *i* та *j*,

n – число вершин в мережі; *a*(*i,j*) =1 тоді коли вершини з'єднані ребром.

Щоб можна було порівнювати степінь центральності вузла не тільки всередині одного графа, але і між графами різної структури [2], необхідно розрахувати нормовану центральність вузла, вона визначається виразом:

$$C_D(i) = \frac{C_D(i)}{n-1} \ . \tag{31}$$

де C'D (*i*) – нормована степінь центральності вузла *i*;

CD (*i*) – степінь центральності вузла і;

n – число вершин в мережі.

Величина C'D (i) змінюється в інтервалі від 0 до 1 і говорить про те, наскільки добре вершина і безпосередньо пов'язана з усіма іншими вершинами мережі. По суті, нормована степінь центральності вузла і є аналогом індексу соціометричного статусу члена групи (C_i), а нормована ступінь вихідної центральності вузла є аналогом індексу емоційної експансивності члена групи.

Щоб мати можливість порівняти різні структури і визначити, яка з них забезпечує найкращу централізацію вузлів, знаходять степінь центральності всього графа за формулою Фрімана [3]

$$C_D = \frac{\sum_{i=1}^{n} (C_D^{'}(i) - C_D(i))}{(n-1)(n-2)} \ . \tag{32}$$

де C_D – степінь центральності всього графа;

$C_D^{'}(i)$ – максимальний ступінь центральності вузла в мережі;

$C_D(i)$ – степінь центральності вузла і;

n – число вершин в мережі.

Тоді остаточне система диференціальних рівнянь математичної моделі захисту інформації з урахуванням центральності мережі прийме вид:

$$\begin{cases} \dfrac{dI}{dt} = Z_p Z + (C_v + C_K) I \\ \dfrac{dZ}{dt} = (\alpha + \beta + \theta + \rho) V - I(C_{d2} + C_{d1})\varepsilon + \\ + (\dfrac{\sum_{v \in V} C_{v1}}{n^2}) + N_{knot}(r+1)^{-f} + \dfrac{\sum_{i=1}^{n} (C_D^{'}(i) - C_D(i))}{(n-1)(n-2)} \end{cases} . \tag{33}$$

Удосконалення моделі захисту інформації за рахунок урахування коефіцієнту довжени шляху інформації в соціальної мережі

З метою удосконалення моделі системи захисту соціальної мережі потрібно визначити, вплив коефіцієнта довжени шляху інформації на модель захисту інформації.

Для цього скористаємось моделлю Барабаш–Альберта. Середня довжина шляху в моделі Барабаш–Альберта збільшується в середньому, як логарифм розміру мережі. Точна форма має подвійну логарифмічну поправку і виглядає, як: $l \approx \frac{\ln n}{\ln \ln n}$.

Модель Барабаш–Альберта має систематично коротший середній шлях, ніж випадковий граф. Базуясь на цей моделі введемо коефіцієнт, якій враховує середню довжину шляху інформації у соціальної мережі: $\gamma = (\frac{\ln \ln n - n}{n(\ln \ln n)^2})$, де: n –кількість вершин в мережі.

Тоді математична модель прийме вигляд:

$$\begin{cases} \frac{dI}{dt} = Z_p Z + (C_v + C_K) I \\ \frac{dZ}{dt} = (\alpha + \beta + \theta + \rho) V - I(C_{d2} + C_{d1})\varepsilon + (\frac{\sum_{v \in V} C_{v1}}{n^2}) + \\ + N_{knot}(r+1)^{-f} + \frac{\sum_{i=1}^{n} (C_D^{'}(i) - C_D(i))}{(n-1)(n-2)} + (\frac{\ln \ln n - n}{n(\ln \ln n)^2}) \end{cases} . \quad (34)$$

Удосконалення моделі захисту інформації за рахунок урахування коефіцієнту взаємовпливу користувачів в соціальної мережі

З метою урахування взаємовпливу користувачів в соціальної мережі введемо коефіцієнт взаємовпливу:

$(P-N) \otimes (P+N)$ – коефіцієнт, що відображає вплив загроз безпеки інформації від взаємовпливу користувачів на захищеність інформаційної системи,

де P_{ij} –позитивний вплив між користувачами,

N_{ij} – негативний вплив між користувачами.

У цьому виразі ми використовуємо згортку двох функцій. Тому що взаємовплив не може бути визначено якимось цілим числом, тільки функціей. Це ще одно із головних відмінностей розробленої моделі. Система диференціальних рівнянь математичної моделі з урахуванням взаємовпливу користувачів прийме вигляд:

$$\begin{cases} \frac{dI}{dt} = Z_p Z + (C_v + C_K) I \\ \frac{dZ}{dt} = (\alpha + \beta + \theta + \rho) V - I(C_{d2} + C_{d1})\varepsilon + (\frac{\sum_{v \in V} C_{v1}}{n^2}) + \\ + N_{knot}(r+1)^{-f} + \frac{\sum_{i=1}^{n} (C_D^{'}(i) - C_D(i))}{(n-1)(n-2)} + (\frac{\ln \ln n - n}{n(\ln \ln n)^2}) + (P-N) \otimes (P+N) \end{cases} . \quad (35)$$

Вирішуючи систему диференціальних рівнянь (35) відносно параметру захисту соціальної мережі, визначимо коефіцієнт захисту соціальної мережі:

$$K_z = \frac{\sum_{i=1}^{n}(C_D{}'(i) - C_D(i))}{(n-1)(n-2)} + D_i + DR + (N(r+1)\wedge(-f)) - (\frac{\sum_{v\in V} C_{v1}}{n^2}) + \\ + (P-N)*(P+N) + (\alpha+\beta+\theta+\rho)V + \frac{\ln\ln n - n}{n(\ln\ln n)^2} \quad , \qquad (36)$$

де D_i – коефіцієнт, що відображає вплив загроз безпеки даних від втрати довіри між користувачами на захищеність інформаційної системи;

DR – коефіцієнт, що відображає вплив загроз безпеки даних від втрати репутації між користувачами на захищеність інформаційної системи; $N(r+1)\wedge(-f)$ – коефіцієнт, що відображає вплив загроз безпеки даних від розповсюдження інформації між користувачами на захищеність інформаційної системи;

$\frac{\sum_{v\in V} C_{v1}}{n^2}$ – коефіцієнт, що відображає вплив загроз безпеки даних від коефіцієнта кластеризації мережі на захищеність інформаційної системи; - $(P-N)\otimes(P+N)$ – коефіцієнт, що відображає вплив загроз безпеки даних від взаємовпливу користувачів на захищеність інформаційної системи; $(\alpha+\beta+\theta+\rho)V$ – коефіцієнт, що відображає вплив загроз безпеки даних від взаємодії користувачів на захищеність інформаційної системи;

$\frac{\ln\ln n - n}{n(\ln\ln n)^2}$ – коефіцієнт, що відображає вплив загроз безпеки даних від довжини шляху між користувачами на захищеність інформаційної системи.

Вираз (36) остаточно визначає математичну модель захисту інформації в соціальної мережі від специфічних параметрів. Таких як: довіра, репутація, вплив загроз безпеки даних від розповсюдження інформації між користувачами, вплив загроз безпеки даних від взаємовпливу користувачів, вплив загроз безпеки даних від взаємодії користувачів та вплив загроз безпеки даних від довжини шляху між користувачами. Слід означити , що параметрів соціальної мережи значно більше. Але ці параметри ми вважаємо найбільш впливові.

Використовуючи удосконалену модель, проведемо моделювання процесу захисту інформації в соціальної мережи з урахуванням специфічних параметрів соціальної мережи. При моделюванні використовували обмеження: усі коефіцієнти нормовані та не перевищують одиницю. Припущення усі специфічні параметри соціальної мережи підпорядковуються нормальному закону розповсюдження. З застосуванням цих припущень та обмежень проведемо моделювання. Результати моделювання наведемо в вигляди рисунку. Результати моделювання представлені у графічному вигляді на рис. 1.

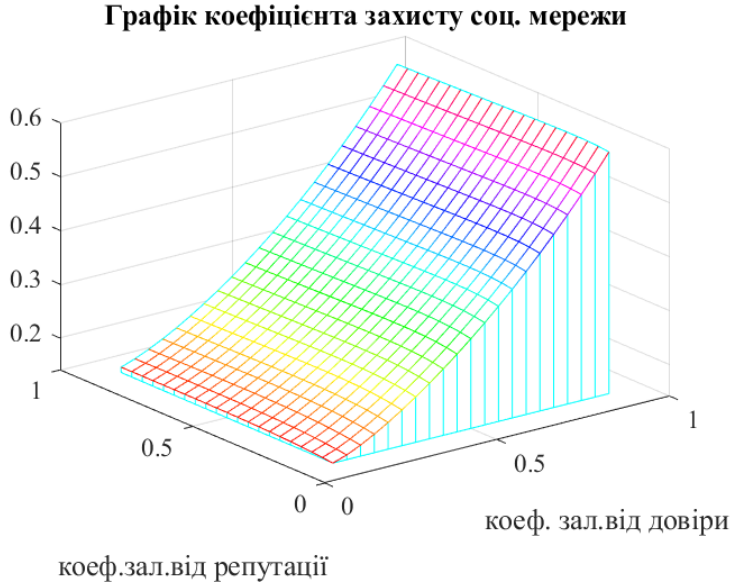


Рисунок 1 – Залежність коефіцієнта захисту соціальної мережі від коефіцієнтів пов'язаних з довірою та репутацією

Як бачимо з графіка коефіцієнт захисту соціальної мережи не приймає нулеві значення, що цілком відповідає реальності. Не може бути захист інформації при відсутності довіри до інформації, інформація у такому випадку просто існує та не потрібує захисту бо користувачу інформація не потрібна. Бачимо що коефіцієнті ,які залежать від репутації на багато менш впливають на коефіцієнт захисту ніж коефіцієнти. Які залежать від довіри. Це теж цілком відповідає сенсу, бо параметр репутації це необхідна умова, але не достатня. Достатній умовою е довіра.

Таким чином результати моделювання остаточно довели, що головним параметром який впливає на захист інформації є параметр довіри. Другі специфічні параметри соціальної мережи впливають на коефіцієнт захисту у значно менший мірі.

Висновки. Розроблено удосконалена математичної моделі захисту інформації в соціальної мережі в залежності від специфічних її параметрів. Таких як: довіра, репутація, вплив загроз безпеки даних від розповсюдження інформації між користувачами, вплив загроз безпеки даних від взаємовплив користувачів, вплив загроз безпеки даних від взаємодії користувачів та вплив загроз безпеки даних від довжини шляху між користувачами.

Проведено математичне моделювання удосконаленої моделі захисту інформації у соціальної мережі в залежності від специфічних її параметрів. Графічні результати відображають актуальну картину захисту інформації соціальної мережи від зовнішніх впливів. Отримані результати для узагальненого коефіцієнта захисту соціальної мережи, показують що коефіцієнт захисту не приймає нулеві значення, що цілком відповідає реальності. Не може бути захист інформації при відсутності довіри до інформації, інформація у такому випадку просто існує та не потрібує захисту бо користувачу інформація не потрібна. Результати моделювання показали, що коефіцієнті ,які залежать від репутації на багато менш впливають на коефіцієнт захисту ніж коефіцієнти, які залежать від довіри. Це доводить, що параметр репутації це необхідна умова, але не достатня. Достатній умовою е довіра. Отримані результати підтверджують адекватність розробленої математичної моделі захисту інформації у соціальної сеті

Подальший розвиток запропонованого методу полягає у більш детальному розгляді специфіки соціальної мережи та параметрів інформаційного захисту.

ЛІТЕРАТУРА:

1. Akhramovich V.M. Limit probabilities of data security and user interaction in the social network. Magyar Tudományos Journal. Budapest, Hungary. 2020. № 41. pp 25–31. www.magyar–journal.com.

2. Akhramovich V.M. Communication and influence of users in social networks. Colloquium–journal. Warszawa, Polska. 2020. №3 (55). pp. 21–25.

3. Oleg Barabash, Oleksandr Laptiev, Oksana Kovtun, Olga Leshchenko, Kseniia Dukhnovska, Anatoliy Biehun. The Method dynavic TF-IDF. International Journal of Emerging Trends in Engineering Research (IJETER), Volume 8. No. 9, September 2020.pp 5713-5718. DOI:10.30534/ijeter/2020/130892020

4. Barabash Oleg, Laptiev Oleksandr, Tkachev Volodymyr, Maystrov Oleksii, Krasikov Oleksandr, Polovinkin Igor. The Indirect method of obtaining Estimates of the Parameters of Radio Signals of covert means of obtaining Information. International Journal of Emerging Trends in Engineering Research (IJETER), Volume 8. No. 8, August 2020. Indexed- ISSN: 2278 – 3075. pp4133 – 4139. DOI:10.30534/ijeter/2020/17882020

5. Vitalii Savchenko, Oleh Ilin, Nikolay Hnidenko, Olga Tkachenko, Oleksandr Laptiev, Svitlana Lehominova, Detection of Slow DDoS Attacks based on User's Behavior Forecasting. International Journal of Emerging Trends in Engineering Research (IJETER) Volume 8. No. 5, May 2020. Scopus Indexed - ISSN 2347 – 3983. pp.2019 – 2025. DOI:10.30534/ijeter/2020/90852020

6. Lubov Berkman, Oleg Barabash, Olga Tkachenko, Andri Musienko, Oleksandr Laptiev, Ivanna Salanda The Intelligent Control System for infocommunication networks. International Journal of Emerging Trends in Engineering Research (IJETER) Volume 8. No. 5, May 2020. Scopus Indexed - ISSN 2347 – 3983. pp.1920 – 1925. DOI:10.30534/ijeter/2020/73852020

7. Laptiev Oleksandr, ShuklinGerman, Savchenko Vitalii, Barabash Oleg, MusienkoAndrii and Haidur Halyna, The Method of Hidden Transmitters Detection based on the Differential Transformation Model. International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE) Volume 8 No. 6 .November - December 2019. Scopus Indexed - ISSN 2278 – 3091.pp.2840 – 2846. DOI: 10.30534/ijatcse/2019/26862019

8. Olexandr Laptiev, German Shuklin, Spartak Hohonianc, Amina Zidan, Ivanna Salanda. Dynamic model of Ceber Defence Diagnostics of information Systems with the Use of Fozzy Technologies IEEE ATIT 2019 Conference Proceedings Kyiv, Ukraine, December 18-20, pp.116 –120.

9. Serhii Yevseiev, Roman Korolyov, Andrii Tkachov, Oleksandr Laptiev, Ivan Opirskyy, Olha No. 5, September-Oktober 2020, pp 8725-8729. DOI: 10.30534/ijatcse/2020/261952020 Soloviova. Modification of the algorithm (OFM) S-box, which provides increasing crypto resistance in the post-quantum period. International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE) Volume 9.

10. Oleksandr Laptiev, Oleh Stefurak, Igor Polovinkin, Oleg Barabash, Savchenko Vitalii, Olena Zelikovska. The method of improving the signal detection quality by accounting for interference. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, November 25-27. pp.172 –176.

11. Oleksandr Laptiev, Savchenko Vitalii, Serhii Yevseiev, Halyna Haidur, Sergii Gakhov, Spartak Hohoniants. The new method for detecting signals of means of covert obtaining information. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, November 25-27. pp.176 –181.

12. Valentyn Sobchuk, Volodymyr Pichkur, Oleg Barabash, Oleksandr Laptiev, Kovalchuk Igor, Amina Zidan. Algorithm of control of functionally stable manufacturing processes of enterprises. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, November 25-27. pp.206 –211.

13. Vitalii Savchenko, Oleksandr Laptiev, Oleksandr Kolos, Rostyslav Lisnevskyi, Viktoriia Ivannikova, Ivan Ablazov. Hidden Transmitter Localization Accuracy Model Based on Multi-Position Range Measurement. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, November 25-27. pp.246 –251

14. Oleg Barabash, Andrii Musienko, Spartak Hohoniants, Oleksandr Laptiev, Oleg Salash, Yevgen Rudenko, Alla Klochko. Comprehensive Methods of Evaluation of Efficiency of Distance Learning System Functioning. International Journal of Computer Network and Information Security(IJCNIS), IJCNIS Vol. 13, No. 1, Feb. 2021. pp 16–28. DOI: 10.5815/ijcnis.2021.01.02

15. Serhii Yevseiev, Oleksandr Laptiev, Sergii Lazarenko, Anna Korchenko, Iryna Manzhul. Modeling the protection of personal data from trust and the amount of information on social networks. Number 1 (2021), «EUREKA: Physics and Engineering» pp.24–31. DOI:10.21303/2461-4262.2021.001615

16. Laptiev O., Savchenko V., Kotenko A., Akhramovych V., Samosyuk V., Shuklin G., Biehun A. Method of Determining Trust and Protection of Personal Data in Social Networks. International Journal of Communication Networks and Information Security (IJCNIS), Vol. 13, No. 1, 2021. pp.15-21.

17. Oleksandr Laptiev, Vitalii Savchenko, Andrii Pravdyvyi, Ivan Ablazov, Rostyslav Lisnevskyi, Oleksandr Kolos, Viktor Hudyma. Method of Detecting Radio Signals using Means of Covert by Obtaining Information on the basis of Random Signals Model. International Journal of Communication Networks and Information Security (IJCNIS), Vol. 13, No. 1, 2021. pp.48-54.

18. O. Svynchuk, O. Barabash, J. Nikodem, R. Kochan, O. Laptiev. Image compression using fractal functions.Fractal and Fractional, 2021, 5(2), 31.pp.1-14. DOI:10.3390/fractalfract5020031 - 14 Apr 2021

19. Oleg Barabash, Oleksandr Laptiev, Valentyn Sobchuk, Ivanna Salanda, Yulia Melnychuk, Valerii Lishchyna. Comprehensive Methods of Evaluation of Distance Learning System Functioning. International Journal of Computer Network and Information Security (IJCNIS). Vol. 13, No. 3, Jun. 2021. pp.62-71, DOI: 10.5815/ijcnis.2021.03.06

20. Bataeva I.P. Information protection and information security. NiKa. 2012№. URL: https://cyberleninka.ru/article/n/zaschita-informatsii-i-informatsionnaya (10.06.2019).

21. Пампуха І.В., Самолов І.В., Толюпа С.В., Берназ Н.М. Інтелектуальний підхід до управління мережними відмовами систем передачі даних. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. К: ВІКНУ, 2008. № 20. С. 18 – 21.

22. A.O. Korchenko, V.O. Breslavskyi, S.P Yevseiev, N.K. Zhumangalieva, A.O. Zvarych, S.V. Kazmirchuk, O.A. Kurchenko, O.A. Laptiev, O. V. Severinov, S. S. Tkachuk. Development of a method for construction of linguistic standards for multicriterial evaluation of HONEYPOT efficiency. Eastern-European journal of enterprise technologies. Vol.1№2 (109), 2021 pp. 14–23. ISSN (print)1729 - 3774. ISSN (on-line) 1729-4061. DOI: 10.15587/1729-4061.2021.225346

REFERENCES:

1. Akhramovich V.M. Limit probabilities of data security and user interaction in the social network. Magyar Tudományos Journal. Budapest, Hungary. 2020. № 41. pp 25–31. www.magyar–journal.com.

2. Akhramovich V.M. Communication and influence of users in social networks. Colloquium–journal. Warszawa, Polska. 2020. №3 (55). pp. 21–25.

3. Oleg Barabash, Oleksandr Laptiev, Oksana Kovtun, Olga Leshchenko, Kseniia Dukhnovska, Anatoliy Biehun. The Method dynavic TF-IDF. International Journal of Emerging Trends in Engineering Research (IJETER), Volume 8. No. 9, September 2020.pp 5713-5718. DOI:10.30534/ijeter/2020/130892020

4. Barabash Oleg, Laptiev Oleksandr, Tkachev Volodymyr, Maystrov Oleksii, Krasikov Oleksandr, Polovinkin Igor. The Indirect method of obtaining Estimates of the Parameters of Radio Signals of covert means of obtaining Information. International Journal of Emerging Trends in Engineering Research (IJETER), Volume 8. No. 8, August 2020. Indexed- ISSN: 2278 – 3075. pp4133 – 4139. DOI:10.30534/ijeter/2020/17882020

5. Vitalii Savchenko, Oleh Ilin, Nikolay Hnidenko, Olga Tkachenko, Oleksandr Laptiev, Svitlana Lehominova, Detection of Slow DDoS Attacks based on User's Behavior Forecasting. International Journal of Emerging Trends in Engineering Research (IJETER) Volume 8. No. 5, May 2020. Scopus Indexed - ISSN 2347 – 3983. pp.2019 – 2025. DOI:10.30534/ijeter/2020/90852020

6. Lubov Berkman, Oleg Barabash, Olga Tkachenko , Andri Musienko, Oleksandr Laptiev, Ivanna Salanda The Intelligent Control System for infocommunication networks. International Journal of Emerging Trends in Engineering Research (IJETER) Volume 8. No. 5, May 2020. Scopus Indexed - ISSN 2347 – 3983. pp.1920 – 1925. DOI:10.30534/ijeter/2020/73852020

7. Laptiev Oleksandr, ShuklinGerman, Savchenko Vitalii, Barabash Oleg, MusienkoAndrii and Haidur Halyna, The Method of Hidden Transmitters Detection based on the Differential Transformation Model. International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE) Volume 8 No. 6 .November - December 2019. Scopus Indexed - ISSN 2278 – 3091.pp.2840 – 2846. DOI: 10.30534/ijatcse/2019/26862019

8. Olexandr Laptiev, German Shuklin, Spartak Hohonianc, Amina Zidan, Ivanna Salanda. Dynamic model of Ceber Defence Diagnostics of information Systems with the Use of Fozzy Technologies IEEE ATIT 2019 Conference Proceedings Kyiv, Ukraine, December 18-20, pp.116 –120.

9.Serhii Yevseiev, Roman Korolyov, Andrii Tkachov, Oleksandr Laptiev, Ivan Opirskyy, Olha Soloviova. Modification of the algorithm (OFM) S-box, which provides increasing crypto resistance in the post-quantum period. International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE) Volume 9. No. 5, September-Oktober 2020, pp 8725-8729. DOI: 10.30534/ijatcse/2020/261952020

10. Oleksandr Laptiev, Oleh Stefurak, Igor Polovinkin, Oleg Barabash, Savchenko Vitalii, Olena Zelikovska. The method of improving the signal detection quality by accounting for interference. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, November 25-27. pp.172 –176.

11. Oleksandr Laptiev, Savchenko Vitalii, Serhii Yevseiev, Halyna Haidur, Sergii Gakhov, Spartak Hohoniants. The new method for detecting signals of means of covert obtaining information. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, November 25-27. pp.176 –181.

12. Valentyn Sobchuk, Volodymyr Pichkur, Oleg Barabash, Oleksandr Laptiev, Kovalchuk Igor, Amina Zidan. Algorithm of control of functionally stable manufacturing processes of enterprises. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, November 25-27. pp.206 –211.

13. Vitalii Savchenko, Oleksandr Laptiev, Oleksandr Kolos, Rostyslav Lisnevskyi, Viktoriia Ivannikova, Ivan Ablazov. Hidden Transmitter Localization Accuracy Model Based on Multi-Position Range Measurement. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, November 25-27. pp.246 –251

14. Oleg Barabash, Andrii Musienko, Spartak Hohoniants, Oleksandr Laptiev, Oleg Salash, Yevgen Rudenko, Alla Klochko. Comprehensive Methods of Evaluation of Efficiency of Distance Learning System Functioning. International Journal of Computer Network and Information Security(IJCNIS), IJCNIS Vol. 13, No. 1, Feb. 2021. pp 16–28. DOI: 10.5815/ijcnis.2021.01.02

15. Serhii Yevseiev, Oleksandr Laptiev, Sergii Lazarenko, Anna Korchenko, Iryna Manzhul. Modeling the protection of personal data from trust and the amount of information on social networks. Number 1 (2021), «EUREKA: Physics and Engineering» pp.24–31. DOI:10.21303/2461-4262.2021.001615

16. Laptiev O., Savchenko V., Kotenko A., Akhramovych V., Samosyuk V., Shuklin G., Biehun A. Method of Determining Trust and Protection of Personal Data in Social Networks. International Journal of Communication Networks and Information Security (IJCNIS), Vol. 13, No. 1, 2021. pp.15-21.

17. Oleksandr Laptiev, Vitalii Savchenko, Andrii Pravdyvyi, Ivan Ablazov, Rostyslav Lisnevskyi, Oleksandr Kolos, Viktor Hudyma. Method of Detecting Radio Signals using Means of Covert by Obtaining Information on the basis of Random Signals Model. International Journal of Communication Networks and Information Security (IJCNIS), Vol. 13, No. 1, 2021. pp.48-54.

18. O.Svynchuk, O. Barabash, J.Nikodem, R. Kochan, O. Laptiev. Image compression using fractal functions.Fractal and Fractional, 2021, 5(2), 31.pp.1-14. DOI:10.3390/fractalfract5020031 - 14 Apr 2021

19. Oleg Barabash, Oleksandr Laptiev, Valentyn Sobchuk, Ivanna Salanda, Yulia Melnychuk, Valerii Lishchyna. Comprehensive Methods of Evaluation of Distance Learning System Functioning. International Journal of Computer Network and Information Security (IJCNIS). Vol. 13, No. 3, Jun. 2021. pp.62-71, DOI: 10.5815/ijcnis.2021.03.06

20. Bataeva I.P. Information protection and information security. NiKa. 2012№. URL: https://cyberleninka.ru/article/n/zaschita-informatsii-i-informatsionnaya (10.06.2019).

21. Pampukha I.V., Samolov I.V., Toliupa S.V., Bernaz N.M. (2008), "Intelektualnyi pidkhid do upravlinnia merezhnymy vidmovamy system peredachi danykh" [An intelligent approach to network failure management of data transmission systems]. Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. Kyiv: VIKNU, 2008. No. 20. P. 18 – 21.

22. A.O. Korchenko, V.O. Breslavskyi, S.P Yevseiev, N.K. Zhumangalieva, A.O. Zvarych, S.V. Kazmirchuk, O.A. Kurchenko, O.A. Laptiev, O. V. Severinov, S. S. Tkachuk. Development of a method for construction of linguistic standards for multicriterial evaluation of HONEYPOT efficiency. Eastern-European journal of enterprise technologies. Vol.1№2 (109), 2021 pp. 14–23. ISSN (print)1729 - 3774. ISSN (on-line) 1729-4061. DOI: 10.15587/1729-4061.2021.225346

D.Sci.Tech. Lukova-Chuiko N.V., D.Sci.Tech. Toliupa S.V., Phd Pogasiy S.S., Laptieva T.O., Laptiev S.O.

IMPROVEMENT OF THE MODEL OF INFORMATION PROTECTION IN SOCIAL NETWORKS

In Ukraine, the right to privacy is a constitutional guarantee, and the protection of personal data is one of the areas in which such a guarantee should be implemented. The subject of our research will not be objects in general, but dynamic systems of information protection in social networks in the mathematical sense of the term. Descriptions of dynamical systems for various problems depending on the law of evolution are various: by means of differential equations, discrete mappings, the theory of graphs, the theory of Markov chains, etc. The choice of one of the methods of description determines the specific form of the mathematical model of the corresponding dynamic system. Theoretical study of the dynamic behavior of a real object requires the creation of its mathematical model. Most of the known approaches to modeling differ in what parameters they use as input information in modeling and what characteristics of the simulated system are calculated and output to the model. The article presents the development of an improved mathematical model of information protection in a social network depending on its specific parameters. Such as trust, reputation, the impact of data security threats from the dissemination of information between users, the impact of data security threats from user interactions, the impact of data security threats from user interaction, and the impact of data security threats from the length of the path between users. However, it should be noted that the parameters of the social network are much more. But we consider these parameters to be the most influential. Therefore, we pay attention to these specific parameters.

Mathematical modeling of the improved model of information protection in the social network depending on its specific parameters is carried out. Graphic results reflect the current picture of protection of social network information from external influences. The obtained results confirm the adequacy of the developed mathematical model of information protection in the social network.

Keywords: social network, trust, reputation, modeling, protection factor, security, information protection.

УДК 681.5

к.т.н., доц. **Муляр І.В.** (ХмНУ)
к.т.н., доц. **Орленко В.С.** (ХмНУ)
Островський І.І. (ХмНУ)
Ряба Л.О. (ВІКНУ)

DOI: https://doi.org/10.17721/2519-481X/2021/73-11

АДАПТИВНИЙ МЕТОД КЕРУВАННЯ АВТОМАТИЗОВАНИМИ ТЕХНІЧНИМИ СИСТЕМАМИ

У статті запропоновано підхід до процесу керування технічними об'єктами на основі інтеграції обробки сенсорних даних.

Інтелектуальні методи управління знайшли застосування в різних завданнях, зокрема в робототехніці. У системах, що працюють в режимі реального часу, робот-агент повинен раціонально вирішувати задачі, які перед ним поставлені з мінімальними витратами ресурсів. У реальному часі використання високоточних багатокритеріальних методів оптимізації утруднене, тому агенти часто вирішують задачу наближеними методами з використанням проблемно-орієнтованої евристики. Аналіз матеріалів з проблеми управління показує, що створення ефективної системи управління потребує використання якісно нових підходів до обробки інформації, які мають базуватися на пошуку особливостей дій у минулому, їх адаптації на основі ієрархічного представлення дій. Найбільш перспективним напрямком у створенні таких систем є використання сучасних нейронних мереж для класифікації прецедентів та формування нових дій на основі підходу прецедентів.

При розробці моделі поведінки агенту пропонується розширити стандартні рішення, використавши елементи біологічного підходу в штучному інтелекті. Для цього агентська діяльність здійснюється через взаємодію класифікаційної та виконавчої сторін. В якості класифікаційної частини використовуються сучасні типи штучних нейронних мереж, згорткових в нашому випадку. За виконавчу частину відповідають моделі на основі ланцюгів Маркова. Штучна нейронна мережа отримує та класифікує інформацію від різних типів зовнішніх сенсорів і внутрішніх рецепторів агенту, щоб ідентифікувати початкові умови дії агенту, мету дії та визначити на їх основі послідовність дій, які виконує агент. Використання адаптивного методу полягає в підміні мети та початкових умов обраного прецеденту новою задачею і початковими умовами і забезпечені виконання плану після підміни. Деякі кроки початкового плану можуть виявитися непотрібними, так як змінилася мета, досягнення якої вони прагнули. Основні дії можна виконувати окремо або комбінувати в послідовності в залежності від успішності поставленої мети.

Ключові слова: інтелектуальне керування, багатоагентні системи, сенсорна інформація.

Вступ. Робототехніка (від робот та техніка; англ.robotics) – прикладна наука, яка опікується проектуванням, розробкою, будівництвом, а також експлуатацією та використанням роботів, спеціалізованих комп'ютерних систем для їх контролю, сенсорного (на основі аналізу вихідних сигналів давачів) зворотного зв'язку і опрацювання інформації автоматизованих технічних систем (роботів) [1]. Перші роботи керувалися простими командами, запозиченими разом із приводами в станках. Для промислових зразків це стало можливим із-за крайнього детермінізму умов промислового виробництва. З розвитком науки і техніки, підтримкою інноваційних технологій робототехніка перетворилася в самостійну наукову сферу. Головною особливістю будь-якого механізму і робота є його корисність. Залежно від корисності автоматизованих технічних систем в тій чи іншій сфері життя заведено виділяти такі різновиди роботів:

– медичні;
– побутові;
– бойові;
– дослідні;
– промислові та будівельні;

– ігрові та ін.

Також їх можна розділити на керовані і автономні; мобільні та стаціонарні.

У сучасній медицині роботи виготовляються серійно, і без багатьох із них складні діагностичні процедури були б майже неможливі. У 1985 році робот Unimation Puma 200 приймав участь у взятті біопсії мозку в пацієнта, що стало значним проривом робототехніки у медицині. Пізніше, через 7 років спеціалізований робот ProBot зробив вперше у світі самостійно операцію

Однак, коли робототехніка розпочинає розповсюджуватися в інших областях з більшою невизначеністю та мінливістю зовнішніх впливів, із програмного керування довелося перейти до управління від оператора, доповнюючи програмне управління диспетчерським управлінням.

Наступним етапом стала розробка на цій основі адаптивних систем управління з використанням подальших методів штучного інтелекту та переходу до парадигми багатоагентних систем. Останні, крім керування, використовувалися для виконання інших функцій роботів, таких як обробка сенсорної інформації та формування моделей взаємодії навколишнього середовища з оператором.

Багатоагентна система (англ. Multi-agent system) – це система, що утворена декількома взаємодіючими інтелектуальними агентами. Ці системи можуть бути використані для вирішення таких проблем, які складно або неможливо розв’язати за допомогою одного агента чи монолітної системи. Прикладами таких завдань є керування критичною інфраструктурою, онлайн-торгівля, ліквідація надзвичайних ситуацій, та моделювання соціальних структур [2].

Штучний інтелект (англ. artificial intelligence, AI) – розділ інформатики та комп'ютерної лінгвістики, що опікується формалізацією проблем та завдань, що подібні до дій, які виконує людина. Подальша перспектива - технічний розвиток формалізації вмінь та творчих здібностей людини - креативності і її взаємодоповнюваність методами штучного інтелекту. Це дозволить повноцінно відтворити в конкретних прикладних областях розумові здібності людини, які реалізуються двома півкулями нашого мозку - лівим, де зосереджено переважно логічне мислення, і правим, що відповідає за творчі здібності та креативність людини. Зрозуміло, інтелектуальні системи управління значно розширюють можливості агентів з освоєння все більш складних операцій. Однак інтелектуальний агент як і раніше вимагає постійного спостереження з боку людини, особливо в зв'язку з можливістю виникнення аварійних та нештатних ситуацій [3, 4].

Він не може тривалий час автономно функціонувати в нестаціонарному середовищі, тому що всі його дії строго формалізовані, і в цих умовах обов'язково вимагається інтуїції, креативність, творчість.

У системах, що працюють в режимі реального часу, особливо в критичній інфраструктурі, агент-робот повинен раціонально вирішувати поставлені перед ним завдання з мінімальними витратами необхідних ресурсів. Передбачається, що робот може виконувати деякі базові дії. Він намагається виконувати свої дії таким чином, щоб поставлена перед ним мета була досягнута. Використання високоточних методів багатокритеріальної оптимізації в реальному часі утруднено, тому агенти зазвичай вирішують задачу апроксимаційними методами з використанням проблемно-орієнтованих евристичних підходів [5].

Проблемами розробки агентів є використовувані ресурсомісткі алгоритми, висока складність і узгодженість моделей. Ці фактори мають негативний вплив на якість агентів, знижують їх обслуговування і продуктивність, а також збільшують витрати на розробку. Додатковим ускладненням є динамічний характер середовища, в якому повинен працювати агент, оскільки стан середовища може значно змінитися в процесі прийняття рішення. Агент повинен адаптуватися до таких змін в найкоротші терміни.

Крім того, досить складно розробити програму, яка була б планом дій для агенту. Тому що зазвичай існує багато способів досягнення цієї мети, і вам потрібно знайти найкращий можливий план. Пошук рішення займає багато часу, тому що це означає повний пошук.

Очевидно, що це не раціонально, тому розробляються складні евристики, які можуть зменшити область пошуку до розумного розміру.

Аналіз наукових досліджень та постановка задачі. Аналіз матеріалів з проблеми керування за допомогою ШІ показує, що створення ефективної системи управління вимагає використання якісно нових підходів до обробки інформації, які повинні ґрунтуватися на виявленні особливостей дій у минулому та їх адаптації на основі ієрархічного представлення дії [5, 6]. Найбільш перспективним напрямом створення таких систем є використання сучасних нейронних мереж для класифікації прецедентів та формування нових дій на їх основі.

Розглянувши підходи до керуванні технічними об’єктами можна зробити висновок, що більшість з них сильно формалізовані і спираються при цьому на формальну обробку предикатів. Вони практично не інтегровані з реальним середовищем, з яким стикається агент.

Технічні штучні нейронні мережі: основний і незмінний засіб роботи з такою інформацією, хоча б тому, що вони, хоча й досі дуже спрощені, але аналогічні "елементарній основі" мозкової діяльності. Накопичення, зберігання та обробка інформації зображення можуть бути реалізовані за допомогою нейронних мереж, які базуються на формальних нейронних мережах з традиційною пороговою логічною обчислювальною базою. Однак традиційні версії нейронних мереж, такі як багатошарові персептрони, мережі Хопфілда або Кохонена, неефективні при роботі зі складними динамічними зображеннями з невизначеністю, що особливо актуально для систем управління роботами [7, 8].

Згорткова (конволюційна) нейронна мережа складається з локальних мереж, які моделюють окремі ділянки рецептивного поля, в яких виконується однакова процедура послідовного узагальнення відповідних компонентів вихідного зображення [9].

Тому метою роботи є розробка підходу до інтелектуального управління технічними об’єктами, який базується на інтеграції сенсорних даних та їх обробці сучасними нейронними мережами.

Основна частина. Ми розглядаємо управління складними технічними об'єктами з точки зору парадигми агентно-орієнтованого моделювання штучного інтелекту.

Ключове відмінність між агентно-орієнтованим підходом полягає в тому, що агенти є суб'єктами в процесі моделювання і мають бажання, мету і здатність виконувати дії, в той час як об'єктно-орієнтований підхід передбачає, що програма виконує операції з об'єктними об'єктами.

Багатоагентні системи реального часу - ефективний інструмент для моделювання складних процесів, в яких задіяна велика кількість активних автономних одиниць. Ці процеси включають міські транспортні потоки, логістичні системи, соціальні явища і епідемії. Методи багатоагентного моделювання також використовуються для пошуку і обробки даних в інформаційних мережах, автономних системах управління. Перспективним напрямком подальшого розвитку мультиагентних систем є розробка безпілотних літальних апаратів і автомобілів.

У багатоагентних системах реального часу агент повинен раціонально вирішувати поставлені перед ним завдання з мінімумом ресурсів. Використання високоточних методів багатокритеріальної оптимізації в реальному часі утруднено, тому агенти зазвичай вирішують задачу апроксимаційними методами з використанням проблемно-орієнтованих евристик [10].

Проблеми розробки агенту - це алгоритми, які використовують багато ресурсів, висока складність та узгодженість моделей. Ці фактори досить негативно впливають на якість агентів, знижують їх утримання та продуктивність, збільшують вартість розробки. Додатковим ускладненням є динамічний характер середовища, в якому агент повинен діяти, оскільки стан навколишнього середовища може значно змінюватися під час прийняття рішень. Агент повинен пристосуватися до таких змін у найкоротші терміни.

На рис. 1 зображена функціональна схема агента-робота зі штучним інтелектом [11]. Його основний та обов’язковий компонент - наявність розвиненої пам’яті, основа розумних дій робота та рівень його інтелекту. блок пам'яті пов'язаний з іншими системами, що обробляють інформацію, і він включає базу знань про зовнішнє середовище у вигляді його

моделі та базу даних про це середовище, самого робота та операції, які вона може виконувати. Крім того, деякі неспеціалізовані оперативні бази знань та дані, пов'язані з центральною пам'яттю, можуть знаходитися в окремих роботосистемах.

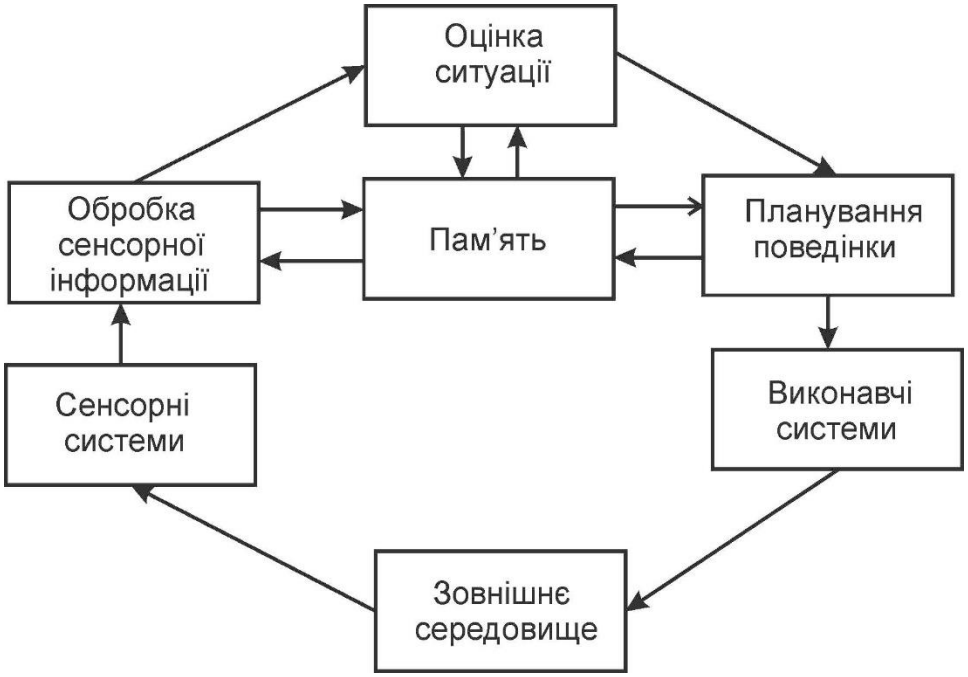


Рисунок 1 - Функційна схема інтелектуального агента-робота

База знань зовнішнього середовища містить апріорну інформацію, введену до початку роботи, та оперативну сенсорну інформацію, отриману в процесі сприйняття навколишнього середовища, коли робот виконує різні дії, а також у процесі своїх особливих пізнавальних дій вивчити це середовище. Сама інформація містить опис геометричних та інших фізичних характеристик об'єктів навколишнього середовища та їх взаємозв'язків. Цей опис має ієрархічну структуру у вигляді рівнів послідовного узагальнення вихідної інформації. Наприклад, опис робочої зони маніпулятора містить набір площин цієї області та її частин, які відрізняються масштабом і точністю, та ступенем узагальнення первинної сенсорної інформації (виділення контурів, об'єктів, поверхонь, груп об'єктів, визначення різних властивостей та фізико -хімічних властивостей цих об'єктів тощо).

Додавання до цих планів часу як параметру, дає зображення зовнішнього середовища в динаміці з урахуванням взаємодії його об'єктів між собою та з роботом. База знань зовнішнього середовища також містить правила, які дозволяють моделювати можливі зміни в цьому середовищі.

Всі інші блоки схеми мають деяку ієрархічну структуру, рівні якої з'єднані між собою вертикально знизу вгору у напрямку узагальнення інформації. У свою чергу, це показано на блок-схемі з'єднання в загальному багатоканальному випадку у вигляді з'єднань між тими ж рівнями по горизонталі.

Блок опрацювання сенсорної інформації отримує від блоку пам'яті екстраполяцію змін стану навколишнього середовища і передає йому виправлення цього стану на рівні прямого сенсорного зображення навколишнього середовища.

Блок оцінки стану та блок планування поведінки зчитують з блоку пам'яті поточну модель середовища та передають їй відповідно свою оцінку за певними критеріями та синтезований план управління рухом робота згідно із завданнями. Завдання модулю оцінки ситуації також включає швидке коригування цілей та пріоритетів управління. Це найвищий рівень в ієрархії керування роботами.

Загалом, інтерфейсний блок може бути двосторонньо пов'язаний з усіма перерахованими функціональними одиницями. Окрім оператора -людини, він забезпечує спілкування з іншими командами, які працюють разом, включаючи іншу роботу.

У міру вдосконалення систем управління робототехнічними агентами перелік операцій, в яких домінують роботи, постійно розширюється. Однак навіть у сучасній промисловості все ще існує значна кількість технологічних операцій, які не повністю автоматизовані. Особливо це стосується непромислових роботів, таких як екстремальна робототехніка. Крім того, прогресуюче ускладнення технічних систем та функцій, які вони виконують, безперервно загострює цю ситуацію, тому людина продовжуватиме залишатися необхідною складовою роботизованих систем, головним чином вищим рівнем управління. Її завдання - керувати операціями, які неможливо автоматизувати, і навчити роботів виконувати ці операції з поступовим переходом до автоматичного режиму [12].

В цілому проблема створення "штучного інтелекту" виходить за межі робототехніки як глобальної проблеми, можна сказати, розвитку людської цивілізації. Той факт, що вона найгостріше зіткнулася з робототехнікою, пояснюється самою історією та сутністю робототехніки, для якої людина була еталоном з самого початку.

Робот має двосторонню інформаційну та енергетичну взаємодію із зовнішнім середовищем. І в цьому сенсі вона повинна бути схожою на живих істот і, отже, здатна до самонавчання та вдосконалення особистості.

В загальному опис завдання планування полягає в тому, що активний елемент (агент) виконує послідовність лій в деякому середовищі і прагне досягти поставленої мети.

У кожен проміжок часу середовище знаходяться в деякому стані, при цьому дії агента можуть змінюють стан середовища.

Завдання планування - знайти послідовність дій, які дозволяють агенту перевести систему з початкового стану в заданий цільовий стан.

У загальному випадку ціль може складатися з кількох станів, досягнення будь-якого з них означає досягнення мети. Також можливо, що жоден з цих станів є недоступним. Формально в задачі планування дається система агент-середовище [12]:

$$M = (Q , A , q_0, \Gamma_M), \quad (1)$$

де Q - множина спостережуваних станів;

A – множина можливих дій;

q_0 – початковий стан;

I - початкові умови;

G - множина цільових станів;

$\Gamma_M : Q \times A => Q$ функція переходу, яка визначає для кожного стану $q \in Q$ і дії $a \in A$ наступний стан $q' = \Gamma_M (q, a)$.

Потрібно знайти план, який є впорядкованою множиною дій $P = \{ a_1 , .., a_n \}$, який є суперпозицією функцій переходу $\Gamma_M (\Gamma_M (... \Gamma_M (\Gamma_M (q_0, a_1) a_2) ..., a_{n-1}), a_n)$ і належить G при $q_0 \in I$.

Відповідно до формули 1 процес керування роботом виглядає так. Існують початкові умови $q_o \in I$ для ініціалізації процесу керування. Якщо брати до уваги процес управління роботом-агентом, то це може бути, наприклад, розряд батареї робота або технічний зір робота при небезпечному швидкому переміщенні великого об'єкта в напрямку робота.

Початкові умови визначають мету операції робота $g \in G$. У першому випадку мета визначається як отримання заряду акумулятора. У другому випадку метою може бути переміщення робота на безпечну відстань від об’єкта загрози (зменшення розмірів об’єкта в полі зору робота).

Залежно від початкового стану та цілі керування необхідно знайти суперпозицію функцій переходу між станами Γ_M (впорядкована множина дій $P = \{ a_1,...,a_n \}$), яка призводить робота в кінцевий стан.

Тобто агент повинен визначити початковий стан. У разі заряду батареї внутрішні сенсори необхідні для визначення ступеня розряду батареї, в останньому випадку зовнішні - для організації технічного зору.

Далі необхідно визначити і класифікувати датчики індикаторів. В організмі людини це здійснюється за допомогою нейронних мереж, як із зовнішнього середовища, так і з індикаторів внутрішнього стану робота-агенту.

Використовуючи адаптивний підхід, для ідентифікації початкового стану доцільно використовувати штучні нейронні мережі. На сьогоднішній день розроблено багато типів нейронних мереж. Нам потрібно вибрати серед них дуже схожі на обробку інформації людським мозком, і з їх успішною реалізацією в області обробки зображень. Для цього ми вибираємо згорткові нейронні мережі, які сьогодні досить успішно використовують Google, Facebook, Pinterest та багато інших [6].

На виході нейронної мережі отримуємо клас початкових умов, за якими можна сформулювати мету і вивести порядок роботи робота.

Тут необхідно робити логічні висновки і планувати дії. Тут також потрібно використовувати аналогію з розумними біологічними системами.

Сучасні нейронні мережі часто вирішують стандартні завдання класифікації, але методи планування дій відокремлені від проблеми класифікації і є високоформалізованими. Тому актуальним завданням є розробка підходу до інтеграції підсистеми планування з існуючими нейронними мережами.

Якщо розглянути дії інтелектуального робота-агенту в небезпечній ситуації, коли великий об’єкт швидко рухається на нього, то нейронна мережа в першу чергу має бути налаштована на ідентифікацію великих об’єктів. Робот повинен розвернутися і якомога швидше відійти від джерела небезпеки, але при цьому необхідно врахувати низький заряд батареї робота. Інші параметри менш важливі і можуть бути оброблені пізніше.

При розробці адаптивного підходу ми будемо використовувати аналогії в діяльності людського мозку. Діяльність людського мозку ще далеко не розкрита, але деякі моменти загально відомі і вже використовуються в сучасних системах штучного інтелекту.

Ми формулюємо основні принципи адаптивного підходу до управління агентами:

1. Нейронна мережа здійснює прийом та класифікацію інформації як від зовнішніх датчиків, так і від внутрішніх сенсорів агенту, щоб ідентифікувати початкові умови дії агенту, мету дії та визначити на основі мети послідовність дій, що виконує агент.

2. Нейронна мережа може обробляти дані від різних типів датчиків (оптичних, акустичних тощо).

3. Існує перелік елементарних дій, що може виконувати агент.

4. Ці дії можуть виконуватися окремо або об'єднуватися в послідовності дій на основі досягнення мети.

5. Нейронна мережа зчитує характеристики послідовності дій через рецептори для організації зворотного зв’язку та ідентифікації поточного стану.

6. Компоненти штучної нейронної мережі можуть класифікувати різні показники об’єктів навколишнього середовища з різною швидкістю. Наприклад, ви можете класифікувати розмір і швидкість об’єкта швидше, ніж вказувати, який об’єкт знаходиться в ієрархії, поступово деталізуючи оброблені показники.

7. Початкові умови і мета мають ступінь важливості, яка може змінюватися і безпосередньо впливати на порядок дій.

На рис. 2 наведено загальну схема агенту, який працює згідно запропонованого адаптивного методу з врахуванням принципів адаптивного підходу.

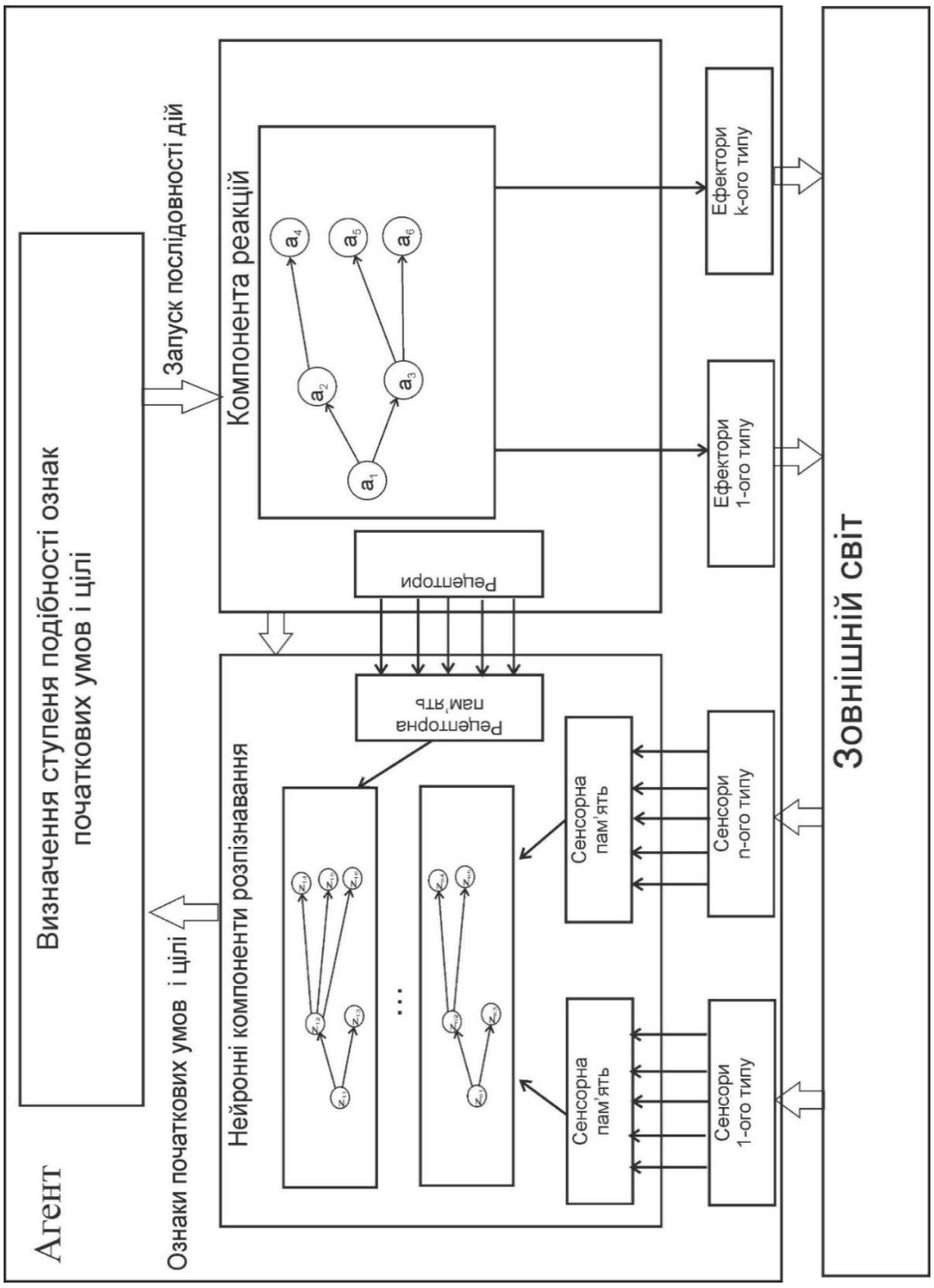


Рисунок 2 – Схема організації інтелектуального управління при адаптивному підході

Функціонування агента складається з послідовності елементарних дій $a_1, a_2, a_3, \ldots, a_n$, що можуть бути використані агентом. Всі елементарні дії в загальному випадку мають певний скінчений набір вхідних параметрів для необхідного налаштування її функціонування $x_1, x_2, .., x_m$. Прикладами елементарних дій робота є рухи робота вперед, назад та повороти, а параметрами можуть виступати швидкість, тривалість руху та ін.

При проектуванні робота виділяються стандартні послідовності дій, що формують бібліотеку і відповідають певним рефлекторним реакціям людини на різні вхідні умови для досягнення мети. Стандартні послідовності дій спрацьовують при активізації певного набору ознак на вихідному шарі мережі.

Послідовність дій агенту може бути описана орієнтованим графом на основі ланцюга Маркова, де стани графу відповідають елементарним діям, а ребра відповідають вазі зв'язку між ними [13]. Знаки початкової умови q пов’язані з першою вершиною, з якої починається послідовність дій. Ознаки мети g пов’язані з останньою вершиною послідовності дій. Коли вага зв'язку між вершинами дорівнює одиниці, тоді перехід між вершинами строго визначений. Коли він відмінний від одиниці, перехід у загальному випадку не є строго обумовленим.

Успішне досягнення мети так чи інакше впливає на вагу ребер. Тобто збільшує вагу всіх ребер на шляху при успішному досягненні мети і навпаки.

На рис. 3 наведено граф послідовності дій на основі ланцюга Маркова, яким можна представити безумовний рефлекс.

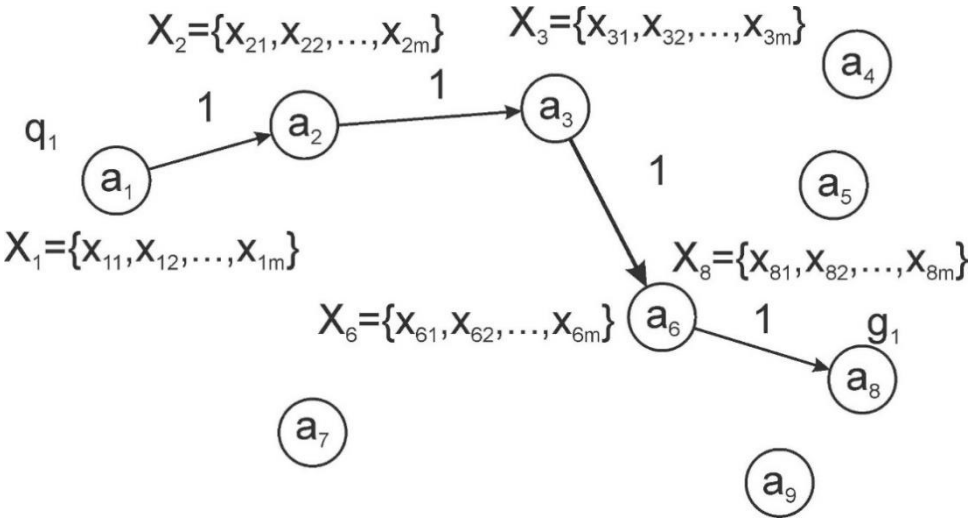


Рисунок 3 - Граф, який моделює безумовний рефлекс послідовності дій агенту

Тобто з рисунку чітко видно, що при деякій початковій умові виконується послідовність дій a_1,a_2,a_3,a_6,a_8, показана на графі.

На рис. 4 наведено граф послідовності дій, яка може відповідати умовному рефлексу агенту. Тобто з вершини може бути кілька сценаріїв, ваги кількох ребер з вершини в сумі повинні дорівнювати одиниці [12]. За замовчуванням вибирається наступна елементарна дія, яка надходить з вершини з найбільшою вагою.

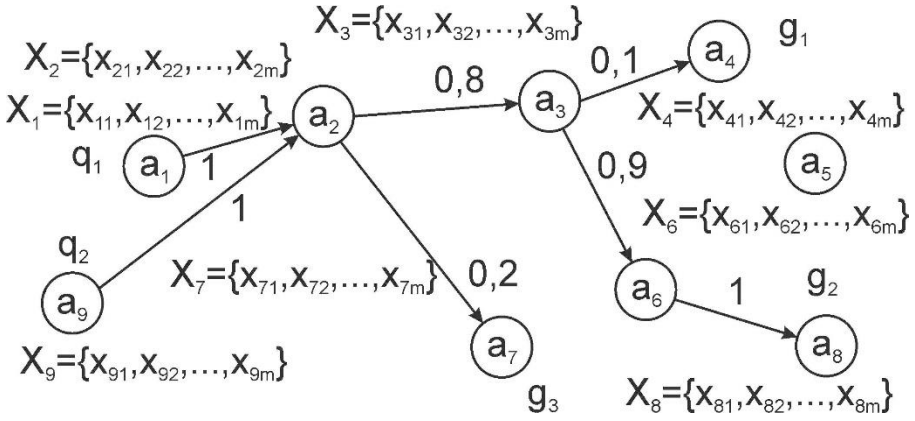


Рисунок 4 - Граф, який моделює умовний рефлекс послідовності дій агенту

У цьому випадку при розвитку подій, яка розпочинається з початкової умови q_1, виконується послідовність дій a_1,a_2,a_3,a_6,a_8, яка закінчується досягненням мети g_2.

Але в цьому випадку агент може проаналізувати поточний стан сенсорів і вибрати перехід по ребрах з меншою вагою, якщо ребра з більшою вагою не приводять до досягнення цілі.

Плануючи послідовність дій, необхідно дозволити агенту використовувати як елементарні дії, так і деяку послідовність цих дій.

Плани дій, представлені попередньою моделлю, повинні бути адаптовані до нової ситуації.

Використання адаптивного методу полягає в підміні мети та початкових умов обраного прецеденту новою задачею і початковими умовами і забезпечені виконання плану після підміни. Деякі кроки початкового плану можуть виявитися непотрібними, так як змінилася мета, досягнення якої вони прагнули.

Висновки. При розробці моделі поведінки агенту доцільно розширити стандартні рішення, використавши елементи біологічного підходу в штучному інтелекті. Для цього агентська діяльність здійснюється через взаємодію класифікаційної та виконавчої сторін. В якості класифікаційної частини використовуються сучасні типи штучних нейронних мереж, згорткових у нашому випадку. За виконавчу частину відповідають моделі на основі ланцюгів Маркова.

Штучна нейронна мережа отримує та класифікує інформацію від різних типів зовнішніх сенсорів і внутрішніх рецепторів агенту, щоб ідентифікувати початкові умови дії агенту, мету дії та визначити на їх основі послідовність дій, які виконує агент.

Штучна нейронна мережа складається з багатьох паралельних компонентів, які генерують класифікатори з різним ступенем деталізації та швидкості обробки для визначення початкових умов роботи.

Існує багато основних дій, які може виконувати агент. Основні дії можна виконувати окремо або комбінувати в послідовності в залежності від успішності поставленої мети.

ЛІТЕРАТУРА:

1. Робототехніка [Електронний ресурс] Режим доступу: https://uk.wikipedia.org/wiki/Робототехніка. Дата звернення: 08.05.2021

2. Stephen Marsland. Machine Learning: An Algorithmic Perspective / Stephen Marsland. – 2015. – 452 p.,

3. Deep Learning / Ian Goodfellow, Yoshua Bengio, AaronCourville. – 2016. – 800 p

4. Mariya Yao Applied Artificial Intelligence: A Handbook For Business Leaders Kindle Edition, Publisher: TOPBOTS, 2018, 246 p.

5. В.О. Бойчук, І.В. Муляр, Ю.О. Царьов. Біокомп'ютери та методики їх програмування. Сучасна спеціальна техніка. - 2014. - № 2(37). - С. 54-60.

6. Рассел, С. Искусственный интеллект: современный подход / С. Рассел, П. Норвиг. - М.: Вильямс, 2016. - 578 с.

7. Слэйгл, Дж. Искусственный интеллект / Дж. Слэйгл. - М.: Мир, 2016. - 320 с.

8. Акинин, М.В. Нейросетевые системы искусственного интеллекта в задачах обработки изображений / М.В. Акинин, М.Б. Никифоров, А.И. Таганов. - М.: ГЛТ, 2016. - 152 с.

9. Ayyadevara, V.K. Convolutional Neural Network. In: Pro Machine Learning Algorithms / V.K Ayyadevara - Berkeley, CA: Apress, 2018. - С. 179–215.

10. A.M. Aibinu, A.J. Onumanyi, A.P. Adedigba, M. Ipinyomi, T.A. Folorunso, M.J.E. Salami, «Development of hybrid artificial intelligent based handover decision algorithm», Engineering Science and Technology an International Journal, 2017. – V.20 (2), pp. 381–390

11. Graves, A. Long Short-Term Memory. In: Supervised Sequence Labelling with Recurrent Neural Networks. Studies in Computational Intelligence, Springer, Berlin, Heidelberg, 2021 (Vol. 385)

12. Бойчук В.О. Метод формування послідовності дій систем реального часу / В.О. Бойчук, М.В. Бойчук, С.М. Жовнір // Наука й економіка: наук.-теорет. журн. / Хмельниц. екон. ун-т. – Хмельницький, 2018. – Вип. 4 (48). – С. 133-137

13. Kravari K., Bassiliades N.A Survey of Agent Platforms. Journal of Artificial Societies and Social Simulation. 2015. Vol. 18, no. 1. P. 1–18.

REFERENCES:

1. Robototekhnika [Elektronnyi resurs] Rezhym dostupu: https://uk.wikipedia.org/wiki/Robototekhnika. Data zvernennia: 08.05.2021

2. Stephen Marsland. Machine Learning: An Algorithmic Perspective / Stephen Marsland. – 2015. – 452 p.,

3. Deep Learning / Ian Goodfellow, Yoshua Bengio, AaronCourville. – 2016. – 800 p

4. Mariya Yao Applied Artificial Intelligence: A Handbook For Business Leaders Kindle Edition, Publisher: TOPBOTS, 2018, 246 p.

5. Boichuk V. O., Muliar I. V., Tsarov Yu. O. (2014), "Biokompiutery ta metodyky yikh prohramuvannia" [Biocomputers and methods of their programming]. Modern special equipment. No 2(37). - pp. 54-60.

6. Rassel, S, Norvyh. P. (2016), "Yskusstveniiy intellekt: sovremenniy podkhod" [Artificial Intelligence: A Modern Approach] Vyliams, Moskva, 578 p.

7. Slэihl, Dzh. (2016), "Yskusstvennby intellekt" [Artificial Intelligence] Myr, Moskva, 320 p.

8. Akynyn, M.V., Nykyforov M.B., Tahanov A.Y. Akynyn, M.V., Nykyforov M.B., Tahanov A.Y. (2016), "Neirosetevii systemi iskusstvennoho intellekta v zadachakh obrabotky izobrazhenyi" [Artificial intelligence neural network systems in image processing tasks] GLT, Moskva, 152 p

9. Ayyadevara, V. K. (2018). Convolutional Neural Network. In: Pro Machine Learning Algorithms. Apress, Berkeley, CA, 179–215.

10. A.M. Aibinu, A.J. Onumanyi, A.P. Adedigba, M. Ipinyomi, T.A. Folorunso, M.J.E. Salami, (2017) «Development of hybrid artificial intelligent based handover decision algorithm», Engineering Science and Technology an International Journal, V.20(2), - pp. 381–390

11. Graves, A. (2012). Long Short-Term Memory. In: Supervised Sequence Labelling with Recurrent Neural Networks. Studies in Computational Intelligence, (Vol. 385). Springer, Berlin, Heidelberg

12. Boichuk V. O., Boichuk, M. V., Zhovnir S. M. (2018), "Metod formuvannia poslidovnosti dii system realnoho chasu" [The method of forming a sequence of actions of real-time systems]. Nauka i ekonomika: nauk.-teoret. zhurn. / Khmelnyts. ekon. un-t. – Khmelnytskyi, No 4(48). - pp. 133-137.

13. Kravari K., Bassiliades N. (2015.) A Survey of Agent Platforms. Journal of Artificial Societies and Social Simulation. Vol. 18, no. 1. - pp. 1–18.

PhD Muliar I.V., PhD Orlenko V.I., Ostrovskiy I.I., Riaba L.O.

ADAPTIVE METHOD OF CONTROLLING AUTOMATED TECHNICAL SYSTEMS

The article proposes an approach to the process of managing technical objects based on the integration of sensor data processing.

Intelligent control methods have found application in various tasks, in particular in robotics. In systems that work in real time, the robot agent must rationally solve the tasks that are set before him with minimal resource costs. In real time, the use of high-precision multicriteria optimization methods is difficult, so agents often solve the problem by approximate methods using problem-oriented heuristics. Analysis of materials on the problem of management shows that the creation of an effective management system requires the use of qualitatively new approaches to information processing, which should be based on finding features of action in the past, their adaptation based on hierarchical representation. The most promising direction in the creation of such systems is the use of modern neural networks for the classification of precedents and the formation of new actions based on the precedent approach. When developing a model of agent behavior, it is proposed to expand the standard solutions, using elements of the biological approach in artificial intelligence. To do this, agency activities are carried out through the interaction of the classification and executive parties. As a classification part modern types of the artificial neural networks convoluted in our case are used. Models based on Markov chains are responsible for the executive part.

An artificial neural network receives and classifies information from different types of external sensors and internal receptors of the agent to identify the initial conditions of the agent, the purpose of the action and determine on their basis the sequence of actions performed by the agent. The use of the adaptive method is to replace the purpose and initial conditions of the selected precedent with a new task and initial conditions and ensure the implementation of the plan after the replacement. Some of the steps in the original plan may not be necessary, as the goal they have sought has changed. The main actions can be performed separately or combined in sequence depending on the success of the goal.

Keywords: control inteligente, multi-agent system, información sensorial.

УДК 004.771

Процик В.О. (КНУБА)
д.т.н., проф. **Хлапонін Ю.І.** (КНУБА)
к.т.н., доц. **Вишняков В.М.** (КНУБА)
к.т.н., доц. **Касім Н.Х.** (КНУБА)

DOI: https://doi.org/10.17721/2519-481X/2021/73-12

МЕТОДИ ВИРІШЕННЯ ПРОБЛЕМИ ПРИМУСУ В ЕЛЕКТРОННИХ СИСТЕМАХ ГОЛОСУВАННЯ

У сучасних умовах стрімкого розвитку інформаційних технологій та збільшення кількості користувачів глобальної мережі Інтернет, впровадження електронної демократії є одним з ключових завдань для забезпечення соціального та економічного розвитку суспільства. Одним з інструментів електронної демократії є електронне голосування. Електронне голосування з'явилося як заміна паперовому, оскільки такий вид голосування може бути економічно вигідним, прозорим і неупередженим. Проте досвід використання електронного голосування у низці країн за останні три десятиліття свідчить про те, що впровадження таких систем було не надто успішним через недоліки безпеки та конфіденційності, які спостерігалися протягом тривалого часу. Однією з найбільших проблем систем голосування є загроза примусу, який змушує виборців змінити своє волевиявлення або взагалі утриматися від голосування проти їх волі. І, хоча на сьогоднішній день у багатьох системах електронного голосування впроваджено функціонал захисту від примусу, наслідками цього стають використання складних алгоритмів підрахунку, обтяження користувачів необхідністю зберігати матеріал криптографічного ключа та перекладання відповідальності на них введення в оману своїх примушувачів. Причиною цього є те, що в умовах електронного голосування важко контролювати, чи примушують виборця голосувати проти його волі. Тому створення електронної системи голосування, яка могла б забезпечити стійкість до примусу, прозорість та надійний захист, є справжнім викликом для багатьох науковців та інженерів. Через це було запропоновано декілька методів, які спрямовані на вирішення цієї проблеми. Однак більшість із запропонованих методів залишаються в основному теоретичними. Метою даної статті є аналіз цих методів вирішення проблеми примусу, а також визначення рівня стійкості до примусу, який вони забезпечують.

Ключові слова: електронна демократія, електронне голосування, таємне електронне голосування у мережі Інтернет, стійкість до примусу в системах електронного голосування, довіра громадян до систем електронного голосування.

Вступ. Голосування грає важливу роль в побудові демократичного суспільства. Електронне голосування - це нова концепція онлайн-виборів, заснована на криптографії. Система підтримує повнофункціональне онлайн-голосування на будь-яких пристроях, а результати опитування будуть розраховуватися автоматично і анонімно. У порівнянні з традиційним голосуванням, електронне голосування - це більш економічна, прозоріша і неупереджена система.

Однією з основних вимог демократичних виборів є те, що виборець повинен мати можливість вільно висловлювати свої справжні уподобання, тобто без примусу. Можна виділити такі основні вимоги до голосування:

• Конфіденційність гарантує, що ніхто не може дізнатися, як голосував виборець.

• Безпримусовість гарантує, що виборець матиме можливість голосувати, відображаючи свої справжні уподобання, навіть якщо він знаходиться під наглядом примушувача протягом періоду голосування. Також безпримусовість означає що примушувач не зможе примусити виборця утримуватися від виборів або віддати невалідний голос, а також віддати валідний голос, якщо він отримає доступ до обліковий даних виборця [1].

• Відсутність відображення результату голосування (квитанції) гарантує, що зловмисник не зможе отримати доказів результату голосу, що робить примус по суті неефективним.

Методи вирішення проблеми примусу. Багато факторів можуть мати вплив на загрозу примусу: тип виборів, властивості протоколу голосування, характеристики системи та середовища голосування, обізнаність виборців, можливості нападника тощо.

Як правило, протоколи голосування, спрямовані на певну форму опору примусу, повинні йти на компроміс між різними цілями. Нижче описано деякі протоколи голосування, стійкі до примусу, їх переваги та недоліки, зручність використання та застосування на практиці.

Метод фальшивих облікових даних. Протоколи JCJ та Civitas. Початком дослідження проблеми примусу в системах електронного голосування можна вважати 2002 рік випуском статті А. Джулза, Д. Каталано та М. Якобссона [2]. В цій статті вони дали визначення опору примусу та запропонували перше рішення, яке його задовольняло та пізніше стало відоме як протокол JCJ. Це рішення передбачає використання фальшивих облікових даних, які виборці можуть використовувати під примусом, але примушувач не зможе відрізнити від справжніх.

У 2008 році протокол JCJ був покращений М. Кларксоном, С. Чонгом та Е. Майерсом шляхом введення розподіленої децентралізованої моделі довіри і поліпшення продуктивності. Покращений протокол отримав назву Civitas [3].

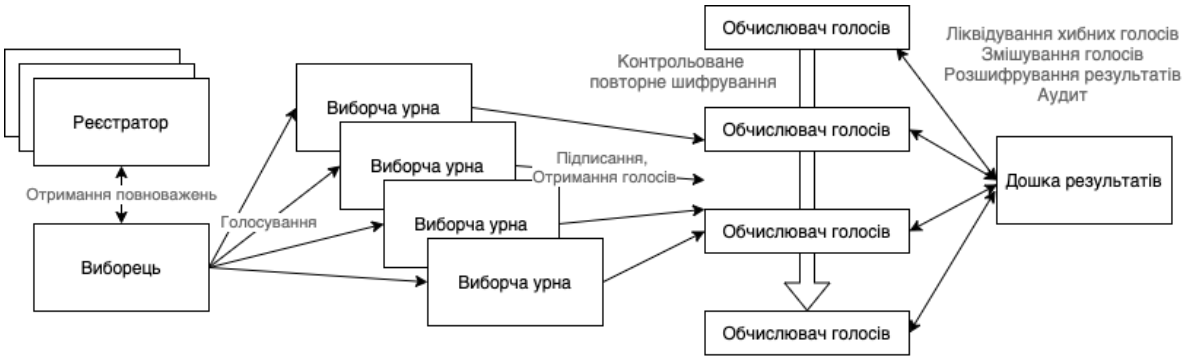


Рисунок 1 – Архітектура протоколу Civitas

Ні один з цих двох протоколів не визначає, як саме виборцю слід обрати відповідні облікові дані. С. Нейманн і М. Волкамер відзначили у своїй статті 2012 року [4], що ця дія є нетривіальною та може призвести до проблем як у використанні, так і у безпеці, якщо вона буде реалізована недбало. Вони запропонували реалізацію Civitas на основі смарт-карт і зчитувачів з PIN-кодами. Вибір між фальшивими та справжніми обліковими даними буде здійснено шляхом введення в зчитувач справжнього або підробленого PIN-коду.

По суті, пропозиція Неймана та Волкамера інкапсулює всі важливі операції на стороні виборців у спеціальне обладнання, якому потрібно довіряти. Хоча в принципі такий підхід може зробити обробку облікових даних більш безпечною, він насправді не наближає нас до практичної реалізації. В принципі, сучасні смарт-карти мають достатню продуктивність, необхідну для реалізації таких функцій. Однак продуктивність - не єдине вузьке місце в практичному застосуванні. Програмне забезпечення, що реалізує функціональність протоколу, має якось потрапити на картки.

Також в рамках процедури реєстрації протокол також залежить від наявності анонімних каналів. Як варіант, автори пропонують використовувати мережу Tor як анонімний канал зв'язку.

Ще один різновид протоколу JCJ розробили Р. Арауйо та співавт. у своїй праці [5] у 2010 р. Вони запровадили коротші облікові дані та формально доказали стійкість до примусу, хоча їхній доказ спирався на нестандартний теоретико-числовий метод. У 2018 році А. Нето та співавт. [6] провели дослідження зручності використання для системи CIVIS, що є реалізацією протоколу, запропонованого Арауйо та співавт. та показали, що більше 90% учасників тесту не розуміють як працює функціонал подання підроблених голосів. Крім того їм був

незрозумілий результат, чи їх поданий голос був справжнім чи підробленим. Це вводить під сумнів всю концепцію використання підроблених облікових даних.

Метод повторного голосування. Естонська система електронного голосування. Повторне голосування - це метод, який надає виборцю можливість змінити свій голос у разі, якщо його примусили під час перших спроб. Найбільш популярним прикладом системи, заснованої на повторному голосуванні, є естонська система голосування, де це єдиний застосований захід проти примусу [7].

Найбільша проблема такого методу є те, що виборець може бути під примусом до кінця періоду голосування для того, щоб особа, яка примушує виборця, запевнилась що не було повторного голосування. Щоб уникнути цієї загрози, Естонія вирішила припинити подання голосів через Інтернет за дві години до закриття виборчих дільниць в останній день періоду голосування. Обґрунтування полягає в тому, що якщо виборець під примусом, у нього ще є час, щоб подати свій голос на папері, і голосування на папері скасовує електронне голосування. Однак, якщо виборець проживає далеко від будь-якої виборчої дільниці, він не може проголосувати без примусу. Вся система діє за умови, що частка таких подій є незначною.

Крім того, функція повторного голосування може вплинути на цілісність голосування, оскільки зловмисник може використовувати його для перезапису попереднього голосування.

Перевагою даного підходу є те, що можливість повторного голосування не потребує додаткових налаштувань на стороні клієнта, а також що цей процес легко зрозуміти для пересічного виборця.

Метод перевірки права на голос. Група протоколів Helios. Перша версія протоколу Helios була описана в роботі Б. Адіди [8] та орієнтована на середовища з низькою вірогідністю примусу. У ході пізніших досліджень було розроблено кілька розширень, щоб посилити його опір примусу.

О. Кулик, В. Тігуе та В. Фолкамер розширили протокол Helios, щоб забезпечити приватну перевірку права на обрання, що означає що серед усіх поданих голосів до підрахунку включені лише голоси виборців, які мають право на голос, не показуючи, хто їх фактично подав[9]. Як побічний продукт, вони досягають відсутності отримання квитанції результату голосування в тому сенсі, що виборець не може довести, як він голосував, оскільки може непомітно переголосувати. Однак автори заявили, що протокол сприйнятливий до атаки рандомізації. Слідуючи ініціалам авторів, схема відома як KTV-Helios.

В оригінальній версії Helios виборці можуть представити випадковий рандомізований підпис голосу як квитанцію результату голосування для примушувача. Протокол BeleniosRF використовує повторно рандомізовані шифровані підписи, причому частина рандомізації відбувається на стороні серверу, який приймає голос, що не дасть можливості виборцю надати будь яку квитанцію про результат голосування [10].

Широкі суспільно-правові дебати щодо конституційності повторного голосування відбувалися в Естонії, коли там було запроваджено голосування в Інтернеті. За кілька місяців до перших Інтернет виборів Президент Естонії подав до Верховного Суду положення про голосування в Інтернеті для перевірки конституційності повторного голосування, стверджуючи, що можливість зміни голосів в Інтернеті дає переваги Інтернет-виборцям у порівнянні з виборцями на папері. Рішення Верховного суду не підтримало цю точку зору, прийшовши до висновку, що просто технічна можливість подання повторних голосів не дає виборцям Інтернету жодної переваги [11].

Хоча результати подібної дискусії можуть бути різними, повторне голосування як простий у реалізації та відносно ефективний захід проти примусу є досить важливим для перегляду деяких законодавчих принципів.

Метод кільцевих підписів. Протокол Eos. С. Патачі та К. Шурманн запропонували протокол голосування Eos на основі умовно пов’язаних кільцевих підписів [12]. Всі виборці умовно зв’язуються між собою в кільце що дозволяє підписувати їх голоси анонімно. Eos використовує дві фази перемішування з метою розірвати зв'язок між виборцем і голосом,

роблячи майже неможливим для примушувача відстеження за голосом через таблицю результатів.

В Eos є дві основні заходи боротьби з примусом. По-перше, виборець може використовувати підсвідому підказку під час підготовки зашифрованого голосу. На практиці така підказка реалізується шляхом пред'явлення справжнього або псевдо-PIN-коду спеціальному апаратному пристрою для голосування або примушувачеві, який контролює цей пристрій.

По-друге, якщо активно примушуваний виборець проголосував, використовуючи дійсний PIN-код, він може пізніше проголосувати повторно, щоб оновити результати голосування. Однак в цьому випадку публічна дошка оголошень буде містити кілька зашифрованих голосів, відданих одним і тим же псевдоідентифікатором, який може бути відомий примушувачеві. В цьому випадку виборцю, можливо, доведеться збрехати примушувачеві, що він був останнім, хто віддав свій голос.

Протокол робить кілька нетривіальних припущень. По-перше, щоб позбутися від побічних каналів при передачі голосів, підписаних кільцево, необхідно використовувати анонімні канали, але на практиці це досить складно.

По-друге, для реалізації операцій на стороні клієнта будуть потрібні спеціальні апаратні токени. У статті пропонується використовувати в цій ролі апаратні гаманці, призначені для зберігання ключів криптовалют.

Рисунок 2 – Апаратний гаманець для криптовалют Trezor

Можливо, таке обладнання можна перепрограмувати, але поширення обладнання або закритих ключів серед виборців - завдання нетривіальне.

Оскільки вибір відбуватиметься шляхом введення реального або псевдо-PIN, ми також маємо всі звичайні проблеми управління псевдо-PIN. Якщо користувач введе неправильний PIN, пристрій не зможе дати ніякої зворотного зв'язку, і спокійно відправить голос, який виборець не збирався віддавати (наприклад, в сценарії, коли виборець хотів використовувати псевдо-PIN, але випадково використав справжній).

Метод "паролів паніки". Протокол Selections. Дж. Кларк і У. Хенгартнер в 2008 році [13] запропонували особливу форму підроблених облікових даних, названих "паролями паніки". Суть панічних паролів полягає в тому, що користувач може вибрати істинний пароль разом з набором альтернативних, які можуть бути використані для прихованого оповіщення системи про те, що користувач знаходиться в ненормальних обставин, наприклад, примус.

Останнє є важливим сценарієм загрози в разі віддаленого голосування, тому ті ж автори побудували схему голосування, стійку до примусу, під назвою Selections на основі своєї основної ідеї [14].

На жаль, змусити запам’ятовані людиною паролі працювати в якості підроблених облікових даних проблематично.

По-перше, необхідний складний процес реєстрації. Звичайно, він повинен відбуватися в контрольованому середовищі без примусу, але це стандартне припущення. У контрольованій реєстраційній кабіні все одно потрібно комп’ютер з доступом в Інтернет, щоб роздрукувати бюлетень виборця. Це передбачено в якості контрзаходу.

Єдиний спосіб, яким примушувач може домогтися цього, - обшукати речі виборця і пройти разом з ним до дверей реєстраційної кабінки.

У процесі реєстрації раніше обрані і зашифровані паролі паніки повторно рандомізують. Виборець вибирає один з повторно рандомізованих шифрів, який публікується в державному реєстрі. У протоколі передбачається, що виборець видаляє випадковість, використану для повторної рандомізації, і не записує її. Побудова властивостей безпеки на припущенні, що деяке значення буде видалено, завжди сумнівно. Можуть існувати побічні канали, якими примушувач змусить виборця користуватись для запису або передачі значення. Якщо примушувач брав участь в створенні бюлетеня виборця і має до нього доступ, то повторно зашифрований пароль паніки в публічному списку може бути зіставлений з зашифрованим словом паніки на бюлетені. Таким чином, випадковість дає можливість довести достовірність пароля, переданого примушувачеві.

Крім того, Selections страждає від типових проблем систем, заснованих на паролі. Ідея [14] полягає в тому, щоб пройти складний процес реєстрації один раз, а потім використовувати облікові дані протягом декількох заходів. Однак вибори, як правило, проходять лише раз в кілька років, і багато виборців, швидше за все, за цей час забудуть свої паролі, незалежно від того, наскільки хороший пароль використовується. Щоб вирішити цю проблему, люди зазвичай записують паролі, що збільшує ризик примусовості.

Висновки. Розробка протоколу електронного голосування, який відповідав би всім вимогам безпеки є досить складною задачею. З одного боку, хотілося б, щоб протокол був захищений від всіх атак, але за це доводиться платити підвищеною складністю технічної реалізації та користування цим протоколом.

У даній роботі розглядаються властивості стійкості до примусу різних протоколів голосування. В ході дослідження було описано п’ять методів вирішення проблеми примусу в електронному голосуванні, деякі з яких (наприклад можливість повторного голосування) достатньо прості в реалізації. У той же час, вимоги щодо організації анонімних каналів чи створення спеціалізованого обладнання легко записати на папері, але досить складно реалізувати.

Метод з використанням фальшивих облікових даних - один з найстаріших методів досягнення доведених властивостей стійкості до примусу, але деякі дослідження, як, наприклад, стаття А. Нето та співавт. [6], показують, що для більшості користувачів даний метод викликає труднощі у розумінні як правильно користуватись цими обліковими даними. Це ставить під сумнів всю ідею використання підроблених облікових даних. В цілому, бракує досліджень зручності використання, які були б присвячені аспектам стійкості протоколів голосування до примусу.

ЛІТЕРАТУРА:

1. Juels, A., Catalano, D., Jakobsson, M. Coercion-resistant electronic elections. *Proceedings of WPES 2005*. ACM 2005. pp. 61–70.

2. Juels, A., Catalano, D., Jakobsson, M. Coercion-Resistant Electronic Elections. Cryptology ePrint Archive, Report 2002/165 2002. [Електронний ресурс]. Режим доступу: https://eprint.iacr.org/2002/165.

3. Clarkson, M.R., Chong, S., Myers, A.C. Civitas: Toward a Secure Voting System. *2008 IEEE Symposium on Security and Privacy (S&P 2008)*. IEEE Computer Society 2008. pp. 354–368.

4. Neumann, S., Volkamer, M. Civitas and the Real World: Problems and Solutions from a Practical Point of View. *ARES 2012*. IEEE 2012. pp. 180–185.

5. Araújo, R., Rajeb, N.B., Robbana, R., Traoré, J., Youssfi, S. Towards practical and secure coercion-resistant electronic elections. *CANS 2010, Proceedings. LNCS*. Springer 2010. vol. 6467. pp. 278–297.

6. Neto, A.S., Leite, M., Araújo, R., Mota, M.P., Neto, N.C.S., Traoré, J. Usability Considerations For Coercion-Resistant Election Systems. *Proceedings of the 17th Brazilian Symposium on Human Factors in Computing Systems*. IHC 2018. pp. 40:1– 40:10.

7. Madise, Ü., Martens, T. E-voting in Estonia 2005. The first Practice of Country - wide binding Internet Voting in the World. *Krimmer, R. (ed.) Electronic Voting 2006.* GI 2006. vol. 86, pp. 15–26.

8. Adida, B. Helios: Web-based Open-Audit Voting. *Proceedings of the 17th USENIX Security Symposium*. USENIX Association 2008. pp. 335–348.

9. Kulyk, O., Teague, V., Volkamer, M. Extending Helios Towards Private Eligibility Verifiability. *VoteID 2015, Proceedings. LNCS*. Springer 2015. vol. 9269. pp. 57–73.

10. Chaidos, P., Cortier, V., Fuchsbauer, G., Galindo, D. BeleniosRF: A Non-interactive Receipt-Free Electronic Voting Scheme. *Proceedings of 2016 ACM CCS*. ACM, New York, NY, USA 2016. pp. 1614–1625.

11. Madise, Ü., Vinkel, P. Internet voting in Estonia: from constitutional debate to evaluation of experience over six elections. *Regulating eTechnologies in the European Union. Normative Realities and Trends*. Springer 2014. pp. 53–72.

12. Patachi, S., Schürmann, C. Eos a universal verifiable and coercion resistant voting protocol. *E-Vote-ID 2017, Proceedings. LNCS*. Springer 2017. vol. 10615. pp. 210–227.

13. Clark, J., Hengartner, U. Panic Passwords: Authenticating under Duress. HotSec'08, Proceedings. [Електронний ресурс] USENIX Association 2008. Режим доступу: http://www.usenix.org/events/hotsec08/tech/full_papers/clark/clark.pdf.

14. Clark, J., Hengartner, U. Selections: Internet Voting with Over-the-Shoulder Coercion-Resistance. *Danezis, G. (ed.) FC 2011, Revised Selected Papers. LNCS.* Springer 2011. vol. 7035. pp. 47–61.

REFERENCES:

1. Juels, A., Catalano, D. and Jakobsson, M. (2005), "Coercion-resistant electronic elections", Proceedings of WPES 2005, ACM, pp. 61–70.

2. Juels, A., Catalano, D. and Jakobsson, M. (2002), "Coercion-Resistant Electronic Elections", Cryptology ePrint Archive, Report 2002/165, https://eprint.iacr.org/2002/165 (accessed 23 October 2021).

3. Clarkson, M.R., Chong, S. and Myers, A.C. (2008), "Civitas: Toward a Secure Voting System", 2008 IEEE Symposium on Security and Privacy (S&P 2008), IEEE Computer Society, pp. 354–368.

4. Neumann, S. and Volkamer, M. (2012), "Civitas and the Real World: Problems and Solutions from a Practical Point of View", ARES 2012, IEEE, pp. 180–185.

5. Araújo, R., Rajeb, N.B., Robbana, R., Traoré, J. and Youssfi, S. (2010), "Towards practical and secure coercion-resistant electronic elections", CANS 2010, Proceedings. LNCS, Springer, vol. 6467, pp. 278–297.

6. Neto, A.S., Leite, M., Araújo, R., Mota, M.P., Neto, N.C.S. and Traoré, J. (2018), "Usability Considerations For Coercion-Resistant Election Systems", Proceedings of the 17th Brazilian Symposium on Human Factors in Computing Systems, IHC 2018, pp. 40:1– 40:10.

7. Madise, Ü. and Martens, T. (2006),"E-voting in Estonia 2005. The first Practice of Country - wide binding Internet Voting in the World", Krimmer, R. (ed.) Electronic Voting 2006, GI, vol. 86, - pp. 15–26.

8. Adida, B (2008), "Helios: Web-based Open-Audit Voting", Proceedings of the 17th USENIX Security Symposium, USENIX Association, pp. 335–348.

9. Kulyk, O., Teague, V. and Volkamer, M (2015), "Extending Helios Towards Private Eligibility Verifiability", VoteID 2015, Proceedings. LNCS, Springer, vol. 9269, pp. 57–73.

10. Chaidos, P., Cortier, V., Fuchsbauer, G. and Galindo, D. (2016)," BeleniosRF: A Non-Interactive Receipt-Free Electronic Voting Scheme", Proceedings of 2016 ACM CCS, ACM, New York, NY, USA, pp. 1614–1625.

11. Madise, Ü. and Vinkel, P (2014), "Internet voting in Estonia: from constitutional debate to evaluation of experience over six elections", Regulating eTechnologies in the European Union. Normative Realities and Trends, Springer, pp. 53–72.

12. Patachi, S. and Schürmann, C (2017), "Eos a universal verifiable and coercion resistant voting protocol". E-Vote-ID 2017, Proceedings. LNCS, Springer, vol. 10615, pp. 210–227.

13. Clark, J. and Hengartner, U. (2008), "Panic Passwords: Authenticating under Duress", HotSec'08, Proceedings. USENIX Association, ttp://whww.usenix.org/events/hotsec08/tech/full_papers/clark/clark.pdf (accessed 23 October 2021).

14. Clark, J. and Hengartner, U. (2011), "Selections: Internet Voting with Over-the-Shoulder Coercion-Resistance", Danezis, G. (ed.) FC 2011, Revised Selected Papers. LNCS, Springer, vol. 7035, pp. 47–61.

Protsyk V.O., D.Sci. Tech. Khlaponin Y.I., PhD Vyshniakov V.M., PhD Qasim N.H.

COERCION RESISTANCE METHODS IN ELECTRONIC VOTING SYSTEMS

In today's condition of rapidly evolving information technologies and increasing number of users of the Internet, building e-democracy is one of the key tasks to ensure the social and economic progress of society. One of the tools of e-democracy is electronic voting. Electronic voting has emerged as a replacement for paper voting, as this type of voting can be cost-effective, transparent and objective. However, the experience of using electronic voting in several countries over the past three decades shows that the implementation of such systems has not been very successful due to long-standing security and privacy shortcomings. One of the biggest problems with voting systems is the threat of coercion, that can force voters to change their will or abstain from voting against their will. And although many e-voting systems today have coercion protection, the consequences are the use of heavyweight counting algorithms, burdening users with the need to store cryptographic key material, and shifting responsibility to mislead their enforcers. The reason for this is that in the conditions of electronic voting it is difficult to control whether the voter is forced to vote against his will. Therefore, the creation of an electronic voting system, which could provide coercion resistance, transparency and reliable protection, is a real challenge for many scientists and engineers. Therefore, several methods have been proposed to solve this problem. However, most of the proposed methods remain largely theoretical. The purpose of this article is to analyze these methods of solving the problem of coercion, as well as to determine the level of resistance to coercion that they provide.

Keywords: e-democracy, e-voting, secret e-voting on the Internet, coercion resistance in e-voting systems, citizens' trust in e-voting systems.

УДК 004.94:355

к.військ.н., с.н.с. **Федченко О.П.** (ВІКНУ)
к.т.н., с.н.с. **Крайнов В.О.** (НУОУ)
к.п.н. **Заїка Л.А.** (НУОУ)

DOI: https://doi.org/10.17721/2519-481X/2021/73-13

ОСНОВНІ ПІДХОДИ ЩОДО ВИБОРУ ПОКАЗНИКІВ ЯКОСТІ ПРИ ПРОЕКТУВАННІ КОНЦЕПТУАЛЬНОЇ БАЗИ ДАНИХ ДЛЯ АВТОМАТИЗОВАНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНУ ВІЙСЬКОВОГО УПРАВЛІННЯ

Автоматизовані інформаційні системи органу військового управління, що орієнтовані на конкретні програми, не відповідають вимогам споживачів, оскільки процес обробки масивів даних ними є недосконалий. Ці обставини обумовили необхідність розробки бази даних, застосування якої сприяло їх інтенсивному використанню. База даних накопичує в своєму середовищі інформацію, необхідну для аналізу обстановки та проведення оперативно-тактичних розрахунків. Процес її проектування та створення є багатоетапним та трудомістким, і включає обробку, інтеграцію, перетворення територіально і функціонально розподілених даних за рахунок залучення висококваліфікованих фахівців в різних областях (аналітиків, програмістів, офіцерів-користувачів). Цей процес відрізняється високим ступенем складності, що обумовлено необхідністю врахування великої кількості параметрів, які характеризують склад і структуру бази даних, а також умови її експлуатації.

Якість і терміни створення баз даних багато в чому визначаються методами і засобами, що застосовуються для проектування, а їх характеристики істотно залежать від прийнятої архітектури інформаційної системи, засобів моделювання предметної області і умов функціонування автоматизованої інформаційної системи органу військового управління.

У роботі розглянуті основні підходи щодо вибору показників якості при проектуванні структури баз даних для автоматизованої інформаційної системи органу військового управління, особливість яких базується на розробці єдиного інтегрованого підходу до проектування, який на етапі концептуального проектування не буде залежати від специфіки конкретної системи управління базою даних (СУБД) і в той же час буде формально охоплювати весь цикл проектування. Також, до числа недостатньо досліджених до теперішнього часу проблем, відноситься проблема, пов'язана з розбіжністю обмежень цілісності здатних підтримуватися СУБД без залучення процедур баз даних. Тобто, виникає завдання отримання формальних критеріїв, які дозволять ще на початкових етапах проектування баз даних визначити – чи підтримується дана система обмежень цілісності засобами СУБД. Крім того, отримання таких критеріїв, також дозволить вирішити важливу задачу логічного проектування баз даних – поділ специфікованих в концептуальній моделі обмежень цілісності на дві підмножини: підмножину обмежень цілісності, яка повністю підтримується СУБД, і підмножину обмежень цілісності, для підтримки якої необхідно використання процедур баз даних.

Ключові слова: концептуальна структура, база даних, автоматизована інформаційна система, СУБД, показники ефективності, орган військового управління.

Вступ. Досвід використання обчислювальної техніки в області обробки даних вказує, що в автоматизованих інформаційних системах військового призначення функція обчислювальної системи полягає в пошуку і накопиченні інформації, тоді як інтелектуальні завдання (прийняття рішення) в основному вирішуються людиною. Інформаційні системи, що орієнтовані на конкретні програми, не відповідають вимогам споживачів, оскільки процес обробки масивів даних ними є недосконалий. Ці обставини обумовили необхідність розробки теорії баз даних (БД), застосування якої сприяло їх інтенсивному використанню [1-5].

Якість і терміни створення БД багато в чому визначаються методами і засобами що застосовуються для проектування, характеристик, які істотно залежать від прийнятої архітектури інформаційної системи, засобів моделювання предметної області і умов функціонування автоматизованої інформаційної системи органу військового управління (АІС ОВУ) [6-11].

Постановка проблеми. Кінцевою метою створення БД для АІС ОВУ є своєчасне і повне задоволення інформаційних потреб посадових осіб органу військового управління (ОВУ). Цей процес відрізняється високим ступенем складності, що обумовлено необхідністю врахування великої кількості параметрів, які характеризують склад і структуру БД, а також умови її експлуатації. Цю мету можна умовно розділити на дві складові (два блоки):

забезпечити подання інформації посадовим особам з максимальною швидкістю ($t_{piш} \rightarrow min$);

забезпечити повноту і достовірність інформації для вироблення рішення ($V_{інф} \approx V_{необх}$).

Блок 1: може бути досягнутий максимальною продуктивністю БД (субблок 1.1), мінімальної надмірністю даних (субблок 1.2), мінімальної надмірністю зв'язків (субблок 1.3) і максимальною простотою представлення даних користувачам (субблок 1.4).

Блок 2: досягається правильним вибором об'єктів і процесів, відомості про які необхідні посадовим особам ОВУ для прийняття рішень (субблок 2.1), відсутністю спотворень інформації, які можуть виникати в БД при неодночасному оновленні даних, і наявністю засобів контролю запису інформації (субблок 2.2).

Аналіз останніх досліджень та публікацій. Теоретичні основи проектування баз даних у своїх працях розглядали В. Карпуша, Б. Панченко, С. Діго, С.Здонік, Г.Гайна, Д.Майер, Т. Конноллі, К. Бегг, У. Вольфенгаген, Л. Кузін, В. Саркісян. Проблеми проектування баз даних досліджували Є. Зіндер, Л. Калініченко, Дж. Мартін, В. Меллінг, Д.Цикриітзиіс, Ф. Лоховскі. Проблемам проектування й опрацювання баз даних присвячені роботи Г. Цибко, Т. Щепакіної, М. Ареф'євої, А. Змитровича, Є. Морозова, Г. Ревункова, Ю. Рамського, Н. Сазонової, О. Ткачева, В. Фреймана. Формування проектувальних умінь майбутніх інженерів-педагогів досліджували В. Кошелева, В. Беспалько.

Виклад основного матеріалу дослідження. За ступенем досягнення зазначених цілей можна робити висновок стосовно ефективності бази даних, що створюється. Виходячи з цього визначимо основні *цільові показники*, відповідно до яких доцільно здійснювати проектування БД ОВУ, а також розглянемо їх взаємозв'язок з *конкретними показниками ефективності* БД, які можуть бути використані на етапі логічного проектування.

Надмірність і достовірність даних істотно впливають на ефективність БД та відсутність спотворень в ній в ході процесу збору даних обстановки, тому що саме на цьому етапі циклу управління витрачається час на додаткові операції з корекції даних, які дублюються, та на перевірку відповідності значень даних до заданої множини допустимих значень. Надмірність може бути двох типів: *функціональна* (дублювання даних) і *операційна* (дублювання зав'язків між даними). Будь-який тип надмірності призводить до необхідності застосування операцій контролю за даними, що записуються (коректуються) в ході даного рівня оновлення.

Цільовий показник *максимальної підтримки обмежень цілісності* [5] безпосередньо пов'язаний з властивістю достовірності інформації, в базі даних, та оперативності її корекції. Максимальній автоматичній підтримці СУБД обмежень цілісності відповідає максимальна достовірність даних в інформаційній системі, після виконання операцій оновлення даних, тому що при цьому в значній мірі обмежується можливість внесення помилок персоналом АСУ.

Як показано в [7], здатність *автоматичної підтримки цілісності* є основною властивістю БД. Це властивість можна інтерпретувати як коректне і адекватне відображення в БД інформації про оперативну обстановку, що цікавить посадових осіб ОВУ. Порушення автоматичної підтримки цілісності призводить до можливості виникнення в базі даних суперечливої інформації. У зв'язку з цим, у якості основного цільового показника проектування БД, узгодженого із загальним критерієм синтезу єдиної СУБД ОВУ, доцільно розглядати *максимальну підтримку обмежень цілісності*.

Водночас, для автоматизованих інформаційних систем військового призначення, важливе значення має *середній час реакції БД на типові запити посадових осіб* ОВУ. В інтересах досягнення першої складової (блок 1) кінцевої мети створення БД ОВУ, логічна структура даних повинна забезпечувати такий вплив на доступ до даних, щоб час реакції

єдиної СУБД на запити посадових осіб – був мінімальним. Однак критерій мінімального середнього часу реакції БД на етапах концептуального і логічного проектування відіграє другорядну роль, тому оптимізація концептуальної схеми та логічної структури БД відповідно до нього, може вестися лише в тих межах, в яких забезпечується максимальна підтримка обмежень цілісності засобами СУБД.

Крім того, на ефективність БД опосередковано (через оператора, що працює з БД ОВУ) впливає простота уявлення користувача про склад і структуру інформації, що зберігається в БД. З огляду на той факт, що з БД буде працювати не системний програміст, а офіцер ОВУ, який не володіє інформацією про існуючу структуру даних, що може значно збільшити час на формулювання запиту до БД і, в свою чергу, знизити оперативність роботи єдиної системи бази даних ОВУ. Тому, в процесі проектування БД, бажано намагатись дотримуватись максимальної простоти та наочності структури БД.

Таким чином, відповідно до основних цілей, для проектування БД ОВУ може бути запропонована наступна система загальних показників якості її концептуального і логічного проектування (рис. 1):

максимальна підтримка обмежень цілісності засобами СУБД;

мінімальний середній час реакції БД на типові запити посадових осіб ОВУ;

максимальна простота та наочність структури БД;

мінімальний обсяг пам'яті, займаної БД.

На логічному рівні, перевірку досягнення цілей доцільно провести з використанням конкретних (розрахункових) показників показаних на рис. 1.

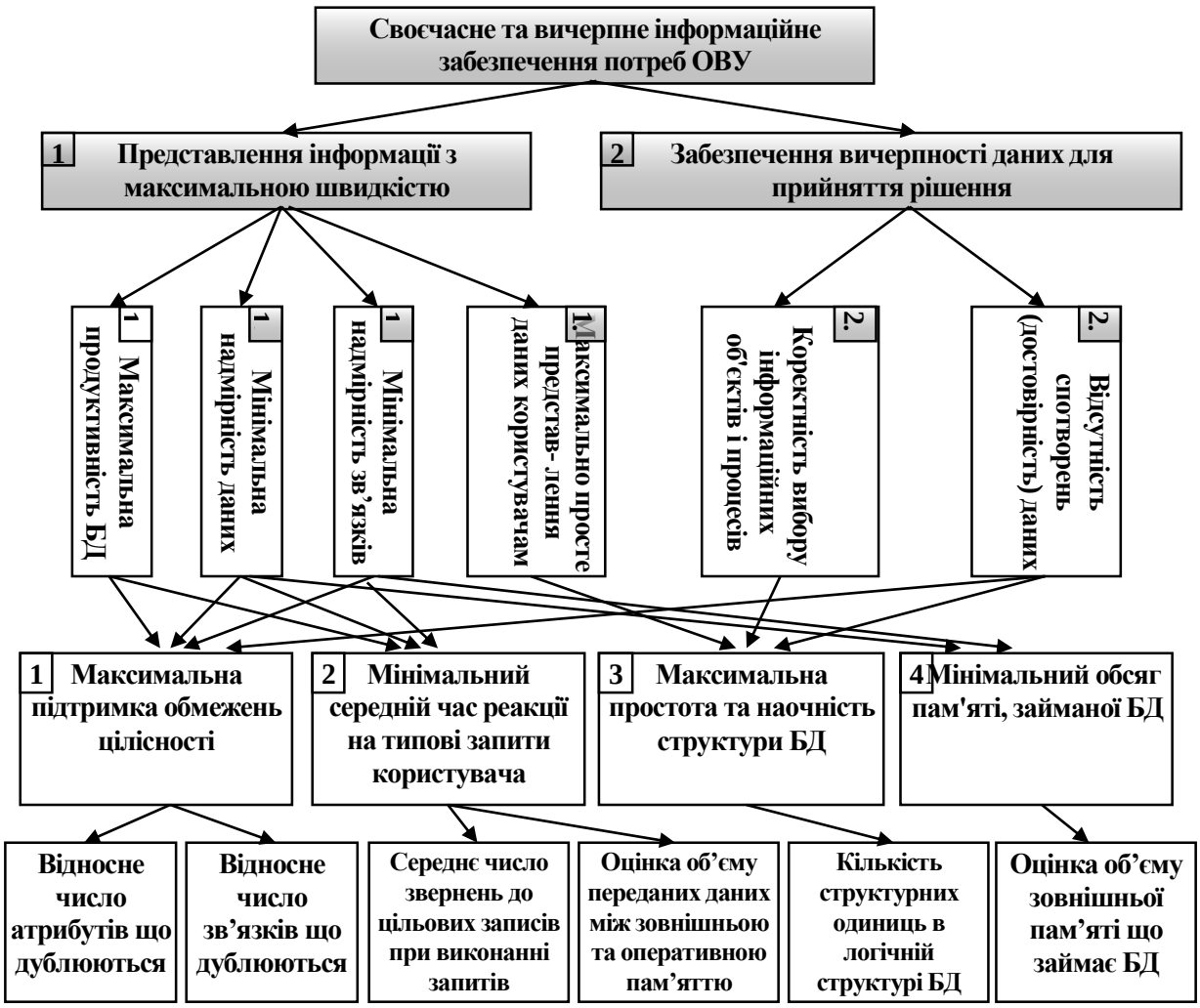


Рисунок 1 – Дерево цілей та система показників проектування БД

На основі запропонованих цільових показників, та виходячи з досвіду практичної реалізації БД [1-4], в загальній моделі даних, в рамках якої проектується БД ОВУ, доцільно застосовувати нормальне представлення даних, реалізоване з використанням *реляційного підходу до* проектування БД [8-9].

Важливим аргументом на користь застосування реляційного підходу є факт наявності в реляційній теорії потужного математичного апарату що використовує теорії множин і дозволяє створювати процедури аналізу властивостей даних, усувати надмірності та проектувати схеми на формальній основі.

Ще однією причиною вибору реляційного підходу при побудові БД ОВУ є просте і наочне вирішення питання ненадмірного представлення даних при використанні цього підходу.

З іншого боку, відповідно до введеної вище системи цільових показників (рис.1) синтезу БД, критерій максимальної підтримки обмежень є основним. Тому, на етапі концептуального проектування цілком доцільно вирішувати питання забезпечення ненадмірності представлення даних з використанням реляційного підходу, тим більше, що властивість ненадмірності є інваріантною до моделей СУБД, що використовувались, але при умові, якщо логічна структура відповідає одній і тій же реляційній схемі, яку підтримує СУБД.

На відміну від ненадмірного представлення даних в БД, час реакції системи на типові запити посадових осіб ОВУ істотно залежить від вибору моделі даних СУБД, способу їх представлення, мови, що використовується для маніпулювання і т. і. Вплив структури БД на цей показник, головним чином, проявляється на етапі логічного проектування, коли здійснюється відображення отриманої концептуальної схеми на модель даних СУБД, оскільки в перспективній АІС системи підтримки прийняття рішення (СППР), в якості технічного забезпечення передбачається широке застосування ПЕОМ з'єднаних за допомогою локальних мереж [2]. Тому ще одним аргументом на користь використання реляційного підходу при побудові БД ОВУ є той факт, що переважна більшість СУБД на ПЕОМ орієнтована на використання реляційної моделі даних [11].

Нарешті, при застосуванні реляційного підходу, під час проектування елементів АІС ОВУ, також виконується вимога щодо економії зовнішньої пам'яті, оскільки в нормальному представленні можна звести до мінімуму фрагментацію реляційної схеми, а це в значній мірі впливає на обсяг зовнішньої пам'яті, що займається БД.

Підводячи підсумок розглянутого вище, можна запропонувати наступну послідовність синтезу логічної структури бази даних АІС ОВУ.

На етапі концептуального проектування на основі реляційного підходу, у визначених межах забезпечується досягнення максимальної ненадмірності представлення даних користувачів АІС ОВУ, в цих же межах мінімізується фрагментарність схеми. В результаті концептуального проектування створюється базова концептуальна схема, що отримує властивість ненадмірності представлення даних. Відносини в цій реляційній схемі максимально масштабовані.

На етапі логічного проектування базова концептуальна схема перетвориться (відобразиться) в логічну структуру бази даних, що підтримується СУБД реляційного типу (маються на увазі багатофайлові СУБД для ПЕОМ та ін.). При цьому крім інтерпретації єдиної реляційної схеми на фрагменти (файли) логічної структури, та генерації описів структур файлів БД на мові опису даних СУБД вирішується завдання оптимізації логічної структури БД за критерієм мінімального середнього часу виконання типових запитів посадових осіб ОВУ.

Висновки. Наявний розрив між рівнем розвитку методичного апарату проектування БД та сучасними вимогами до нього, очікувана масовість розробки і застосування БД в ОВУ обумовлюють необхідність переходу від оптимізації окремих процедур розробки БД до створення комплексної методики їх проектування. Це дозволить впорядкувати працю фахівців різного профілю (офіцерів-операторів, аналітиків, програмістів), виключить дублювання в їх роботі і створить передумови для повної автоматизації процесу проектування. Процес проектування БД АІС ОВУ носить ітераційний характер. Тому в ньому передбачена

можливість повернення на попередні етапи, накопичення і порівняння результатів з метою отримання оптимального варіанта структури бази.

З урахуванням запропонованої системи показників, за якими оцінюється база даних, і відповідно до рівнів деталізації її опису розроблена поетапна технологія проектування бази даних АІС ОВУ. Основу цієї технології складає єдиний методичний підхід послідовного перетворення вихідних даних і отриманих в процесі проектування результатів з урахуванням обмежень і критеріїв ефективності, специфічних для кожного етапу.

ЛІТЕРАТУРА:

1.Томас Коннолли. Базы данных: проектирование, реализация и сопровождение. Теория и практика 3-е изд. Україна від найдавніших часів до сьогодення: хронол. довід. /Томас Коннолли, Каролин Бегг. – : Вильямс, 2017. – 1440с.

2. Бази даних та інформаційні системи. Навчальний посібник / С.В. Шаров, В.В.Осадчий. – Мелітополь: Вид-во МДПУ ім. Б. Хмельницького, 2014. – 352с.

3. К. Дж. Дэйт. Введение в системы баз данных / К. Дж. Дэйт – изд.: Вильямс, 2017. – 1328с.

4. Берко А. Ю., Верес О. М., Пасічник В. В. Системи баз даних та знань. Книга1.Організація баз даних та знань : підручник.–Львів: «Магнолія-2006»,2015.–440с.

5. Берко А. Ю., Верес О. М., Пасічник В. В. Системи баз даних та знань. Книга2.Системи управління базами даних та знань: навч. посібник. –в: «Магнолія-2006»,2012. –584с.

6. Інформаційні системи і технології: навч. посіб. / [П. М. Павленко, С.Ф.Філоненко, К.С.Бабічтаін.].К.:НАУ, 2013.324с.

7. Застосування інформаційних технологій та інновацій у воєнній сфері. Навчальний посібник. Крайнов В.О., Солонніков В.Г., Лаврінчук О.В. та ін. – Київ: Національний університет оборони України імені Івана Черняховського, 2021. – 480 с.

8. Інформаційні технології інформаційно-аналітичного забезпечення органів управління військами (силами): Підручник / [С.А. Микусь, В.Г. Солонніков, В.О. Крайнов, та ін.].– К.: НУОУ ім. І. Черняховського, 2018. − 352 с.

9. Організація інформаційно-аналітичного забезпечення органів управління військами (силами): Підручник / [С. А. Микусь, В. Г. Солонніков, В.О. Крайнов та ін.].– К.: НУОУ ім. І. Черняховського, 2019. − 237 с.

10. Застосування сучасних інформаційних технологій у науковій діяльності: Підручник / [С. А. Микусь, В. Г. Солонніков, В.О. Крайнов, Т. П. Пащенко та ін.].– К.: НУОУ ім. І. Черняховського, 2019. − 237 с.

11. Крайнов В.О. Методика проектування бази даних для автоматизованої інформаційної системи органу військового управління. Сучасні інформаційні технології в сфері безпеки та оборони-2020.- № 2 (38). С.103…106.

REFERENCES:

1. Connolly, T. and Begg, C. (2017), *Databases: design, implementation and maintenance. Theory and Practice 3rd ed. Ukraine from the found hours to the present day: chronol. dovid.*, Williams, 1440 p.

2. Sharov, S.V. and Osadchy, V.V. (2014), *"Bazy danykh ta informacijni systemy. Navchaljnyj posibnyk" [Databases and information systems. Tutorial]*, Bogdan Khmelnitsky Melitopol State Pedagogical University, Melitopol, 352 p.

3. Date, C. J. (2017), *Introduction to database systems*, Williams, 1328 p.

4. Berko, A.Y., Veres, O.M. and Pasichnyk, V.V. (2015), *"Systemy baz danykh ta znanj. Knygha 1. Orghanizacija baz danykh ta znanj: pidruchnyk" [Database and knowledge systems. Book 1. Organization of databases and knowledge: manual]*, Magnolia-2006, Lviv, 440 p.

5. Berko, A.Y., Veres, O.M. and Pasichnyk, V.V. (2012), *"Systemy baz danykh ta znanj. Knygha 2. Systemy upravlinnja bazamy danykh ta znanj: navch. posibnyk" [Database and knowledge systems. Book 2. Database and knowledge management systems: tutorial]*, Magnolia-2006, Lviv, 584 p.

6. Pavlenko, N. M., Filonenko, S.F and Babichtain, K.S. (2013), *"Informacijni systemy i tekhnologhiji: navch. posib." [Information systems and technologies: tutorial]*, NAU, Kyiv, 324 p.

7. Kraynov, V.O., Solonnikov, V.G. and Lavrinchuk, O.V. (2021), *"Zastosuvannja informacijnykh tekhnologhij ta innovacij u vojennij sferi. Navchaljnyj posibnyk" [Application of information technologies and innovations in the military sphere. Tutorial]*, National University of Defense of Ukraine named Ivan Chernyakhovsky, Kyiv, 480 p.

8. Mikus, S.A., Solonnikov, V.G. and Krainov, V.O. (2018), *"Informacijni tekhnologhiji informacijno-analitychnogho zabezpechennja orghaniv upravlinnja vijsjkamy (sylamy): Pidruchnyk" [Information technologies of information-analytical support of troops (forces) management bodies: Textbook]*, National University of Defense of Ukraine named Ivan Chernyakhovsky, Kyiv, 352 p.

9. Mikus, S.A., Solonnikov, V.G. and Krainov, V.O. (2019), *"Orghanizacija informacijno-analitychnogho zabezpechennja orghaniv upravlinnja vijsjkamy (sylamy): Pidruchnyk" [Organization of information and analytical support of troops (forces): Textbook]*, National University of Defense of Ukraine named Ivan Chernyakhovsky, Kyiv, 237 p.

10. Solonnikov, V.G., Krainov, V.O. and Pashchenko, T. P. (2019), *"Zastosuvannja suchasnykh informacijnykh tekhnologhij u nakovij dijaljnosti: Pidruchnyk" [Application of modern information technologies in scientific activity: Textbook]*, National University of Defense of Ukraine named Ivan Chernyakhovsky, Kyiv, 237 p.

11. Kraynov, V.O. (2020), *"Metodyka proektuvannja bazy danykh dlja avtomatyzovanoji informacijnoji systemy orghanu vijsjkovogho upravlinnja" [Database design methods for the automated information system of the military administration]*, Current information technologies in the field of security and defense, No. 2 (38), pp. 103–106.

PhD Fedchenko O.P., PhD Krainov V.O., PhD Zaika L.A.

BASIC APPROACHES FOR SELECTING QUALITY INDICATORS DURING CONCEPTUAL DATABASE DESIGNING FOR AUTOMATED INFORMATION SYSTEM OF MILITARY CONTROL BODY

Automated information systems of the military control body (AIS MCB), which are focused on specific programs, do not meet the requirements of consumers, because the process of processing data arrays is imperfect. These circumstances necessitated the development of its database (DB), using which contributed to their intensive use. The database accumulates in its environment necessary information for analysis of situation and organization operational and tactical calculations. The process of its design and creation is multi-stage and time-consuming and requires processing, integration, the transformation of territorially and functionally distributed data through the involvement of highly qualified specialists in various fields (analysts, programmers, user officers). This process has a high degree of complexity, due to the need to take into account parameters that characterize the composition and the structure of the database, as well as conditions of its operation. The quality and timing of database creation are largely determined by methods and tools used for design, their characteristics significantly depend on the adopted architecture of the information system, subject area modeling tools, and operating conditions of the AIS MCB.

The authors considered the main approaches choosing quality indicators when designing the database structure of the automated information system of the military control; this feature is based on the development of a single integrated design approach, which at the conceptual design stage will not depend on the specific database management system. It can also be noted that among insufficiently researched problems so far the problem related to the discrepancy of integrity constraints that can be maintained by the database without the involvement of database procedures is. That is, there is a task of obtaining formal criteria that will allow at initial stages of database design to determine – whether this system of integrity restrictions is supported by the database. In addition, obtaining such criteria will also solve an important problem of logical database design – the division of specified in the conceptual model of integrity constraints into two subsets: a subset of integrity constraints that are fully supported by the database, and a subset of integrity constraints that require database procedures.

Keywords: conceptual structure, automated information system, DBMS, indicators efficiency, of military control body.

ДАНІ ПРО АВТОРІВ

Бабій Юлія Олександрівна, доктор технічних наук, головний редактор редакційного відділення видавництва, Національна академія Державної прикордонної служби України імені Богдана Хмельницького, ORCID: 0000-0001-7310-8715.

Барабаш Олег Володимирович, доктор технічних наук, професор, провідний науковий співробітник науково-дослідного відділу проблем застосування авіації та ППО інституту авіації та протиповітряної оборони Національного університету оборони України імені Івана Черняховського, ORCID: 0000-0003-1715-0761.

Вишняков Володимир Михайлович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва і архітектури, ORCID: 0000–0003-4668-712X.

Гунченко Юрій Олександрович, доктор технічних наук**,** професор, завідуючий кафедри Одеського національного університету, ORCID: 0000-0003-4423-8267.

Джулій Андрій Володимирович, кандидат технічних наук, доцент Університету економіки і підприємництва (м Хмельницький).

Дуля Олександр Олександрович, аспірант кафедри телекомунікацій Інституту телекомунікаційних систем Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», ORCID: 0000-0002-9769-3178.

Заїка Людмила Анатоліївна, кандидат педагогічних наук старший науковий співробітник центру імітаційного моделювання Національного університету оборони України імені Івана Черняховського, ORCID: 0000-0003-4386-4004.

Зайцев Дмитро Володимирович, кандидат військовий наук, доцент, доцент кафедри, факультет післядипломної освіти, Військовий інститут Київського національного університету імені Тараса Шевченка. ORCID: 0000-0002-3784-5790.

Заславський Володимир Анатолійович, доктор технічних наук, професор кафедри математичної інформатики факультету комп'ютерних наук та кібернетики Київського національного університету імені Тараса Шевченка, ORCID:0000-0001-6225-1313.

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.

Кіреєнко Володимир Володимирович, кандидат військових наук, доцент кафедри Повітряних Сил інституту авіації та протиповітряної оборони Національного університету оборони України імені Івана Черняховського, ORCID: 0000-0003-0230-9450.

Крайнов Валерій Олександрович, кандидат технічних наук, СНС старший науковий співробітник центру імітаційного моделювання Національного університету оборони України імені Івана Черняховського, Київ, Україна, ORCID: 0000-0002-7314-2056.

Крихта Віталій Вікторович, кандидат технічних наук, провідний інженер інституту високих технологій Київського національного університету імені Тараса Шевченка, ORCID: 0000-0002-2847-4246.

Кульскій Олександр Леонідович, кандидат техничних наук, старший науковий співробітник, старший науковий співробітник інституту високих технологій Київського національного університету імені Тараса Шевченка, ORCID: 0000-0002-8065-6338.

Лаптєв Сергій Олександрович, аспірант, Кафедра кібербезпеки та захисту інформації, Київський національний університет імені Тараса Шевченка, Факультет інформаційних технологій. ORCID: 0000-0002-7291-1829.

Лаптєва Тєтяна Олександрівна, аспірант, Кафедра кібербезпеки та захисту інформації, Київський національний університет імені Тараса Шевченка, факультет інформаційних технологій, ORCID: 0000-0002-5223-9078.

Лєнков Євген Сергійович, кандидат технічних наук, старший дослідник, старший науковий співробітник наукового центру Центрального науково-дослідного інституту Збройних Сил України, ORCID: 0000-0001-5819-2656.

Лєнков 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, Військовий інститут Київського національного університету імені Тараса Шевченка, ORCID: 0000-0001-7689-239X.

Лоза Віталій Миколайович, кандидат технічних наук, старший дослідник, начальник відділу науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка, ORCID: 0000-0002-8050-3614.

Лукова-Чуйко Наталія Вікторівна, доктор технічних наук, професор, завідучка кафедри кібербезпеки та захисту інформації, Факультет інформаційних технологій, Київського національного університету імені Тараса Шевченка, ORCID:0000-0003-3224-4061.

Мартинюк Віктор Петрович, старший викладач кафедри прикордонної служби, Національна академія Державної прикордонної служби України імені Богдана Хмельницького, ORCID: 0000-0001-9569-1112

Мартинюк Олександр Васильович, старший викладач кафедри прикордонної служби, Національна академія Державної прикордонної служби України імені Богдана Хмельницького, ORCID: 0000-0002-0216-1356

Міночкін Дмитро Анатолійович, кандидат технічних наук, старший науковий співробітник, доцент кафедри телекомунікацій Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», ORCID: 0000-0003-4988-7098

Муляр Ігор Володимирович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки Хмельницького національного університету, ORCID: 0000-0002-6659-605X.

Нікіфоров Микола Миколайович, кандидат військових наук, старший дослідник, провідний науковий співробітник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка, ORCID: 0000-0002-2849-5688

Опенько Павло Вікторович, кандидат технічних наук, старший науковий дослідник, начальник науково-дослідного відділу проблем застосування авіації та ППО інституту авіації та протиповітряної оборони Національного університету оборони України імені Івана Черняховського, ORCID: 0000-0001-7777-5101.

Орленко Вікторія Сергіївна, кандидат технічних наук, доцент кафедри кібербезпеки Хмельницького національного університету, ORCID: 0000-0001-9601-1916.

Островський Ілля Ігорович, магістр кафедри кібербезпеки Хмельницького національного університету, ORCID: 0000-0003-1307-6082.

Погасій Сергій Сергійович, кандидат економічних наук, доцент, Кафедра кібербезпеки та інформаційних технологій, Харківський національний економічний університет ім. С. Кузнеця, ORCID: 0000-0002-4540-3693.

Поліщук Віктор Вікторович, кандидат військових наук, доцент кафедри прикордонної служби, Національна академія Державної прикордонної служби України імені Богдана Хмельницького, ORCID: 0000-0002-9654-9015.

Попков Борис Олексійович, кандидат військових наук, старший науковий співробітник, провідний науковий співробітник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка, ORCID: 0000-0001-9750-1220.

Процик Віталій Олексійович, студент Київського національного університету будівництва і архітектури, ORCID: 0000-0001-5755-5945.

Прохоров Олег Анатолійович, кандидат педагогічних наук, доцент, заступник начальника інституту з навчальної роботи, Військовий інститут Київського національного університету імені Тараса Шевченка, ORCID: 0000-0002-3246-8850.

Пушкаренко Юрій Валерійович, аспірант кафедри математичної інформатики факультету комп'ютерних наук та кібернетики Київського національного університету імені Тараса Шевченка

Ряба Людмила Олександрівна, науковий співробітник науково-дослідного центру, Військовий інститут Київського національного університету імені Тараса Шевченка, ORCID: 0000-0002-7436-4443.

Семеха Сергій, заступник начальника факультету післядипломної освіти з навчальної та наукової роботи, Військовий інститут Київського національного університету імені Тараса Шевченка.

Сєлюков Олександр Васильович, доктор технічних наук, старший науковий співробітник, Лауреат Державної премії України в галузі науки і техніки, професор кафедри Київський національний університет будівництва та архітектури. ORCID: 0000-0001-7979-3434.

Солодєєва Людмила Василівна, науковий співробітник науково-дослідного центру, Військовий інститут Київського національного університету імені Тараса Шевченка. ORCID: 0000-0002-7979-8443.

Степаненко Євген Олександрович, кандидат технічних наук, командувач військ зв'язку та кібербезпеки Збройних Сил України, ORCID: 0000-0003-1993-2441.

Толок Ігор Вікторович, кандидат педагогічних наук, доцент, Заслужений працівник освіти України, Лауреат Державної премії України в галузі освіти, начальник Військового інституту Київського національного університету імені Тараса Шевченка, ORCID: 0000-0001-6309-9608.

Толюпа Сергій Васильович, доктор технічних наук, професор, професор кафедри кібербезпеки та захисту інформації, Факультет інформаційних технологій,Київського національного університету імені Тараса Шевченка, ORCID: 0000-0002-1919-9174.

Федченко Олексій Петрович, кандидат військових наук, старший науковий співробітник старший, науковий співробітник науково-дослідного відділу геоінформаційних технологій науково-дослідного центру ВІКНУ, Київ, Україна, ORCID: 0000-0003-1343-3828.

Хлапонін Юрій Іванович, доктор технічних наук, професор, завідувач кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва і архітектури, ORCID: 0000–0002-9287-0817.

Черноусов Дмитро Олександрович, викладач кафедри прикордонної служби, Національна академія Державної прикордонної служби України імені Богдана Хмельницького, ORCID: 0000-0002-9012-2372.

Чорненький Віталій Іванович, кандидат технічних наук, доцент Університету економіки і підприємництва.

Алфавітний покажчик

Наукове видання

ЗБІРНИК НАУКОВИХ ПРАЦЬ

Військового інституту

Київського національного університету імені Тараса Шевченка

№ 73

Усі матеріали надруковані в авторській редакції.

Підписано до друку 17.12.21 р.
Авт. друк. Арк. 11. Формат 60х90/8
Безкоштовно. Замовлення № 10-2012

Надруковано у навчальному картографічному комплексі ВІКНУ

03189, Київ, вул. Ломоносова 81

т. 521-32-89