НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ОБОРОНИ АЗЕРБАЙДЖАНСЬКОЇ РЕСПУБЛІКИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ "ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ М. Є. ЖУКОВСЬКОГО "ХАРКІВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ"

УНІВЕРСИТЕТ МІСТА ЖИЛІНА

СУЧАСНІ НАПРЯМИ РОЗВИТКУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЗАСОБІВ УПРАВЛІННЯ

Тези доповідей чотирнадцятої міжнародної науково-технічної конференції

25 – 26 квітня 2024 року

Том 2: **секції 3, 4, 5, 6**

Баку – Харків – Жиліна – 2024

УДК 004/681.3 doi: https://doi.org/10.32620/ICT.24.t2

У збірнику подано тези доповідей чотирнадцятої міжнародної науково-технічної конференції "Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління". Розглянуті питання за такими напрямами: теоретичні та прикладні аспекти систем прийняття рішень, оптимізації та управління системами і процесами; комп'ютерні методи та засоби інформаційно-комунікаційних технологій та управління; безпека функціонування комп'ютерних систем та мереж; інформаційні технології у цивільній безпеці; сучасні інформаційно-вимірювальні системи; інформаційні технології у цивільній безпеці.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ

AZERBAIJAN NATIONAL DEFENCE UNIVERSITY

NATIONAL TECHNICAL UNIVERSITY
KHARKIV POLYTECHNIC INSTITUTE

KHARKIV NATIONAL UNIVERSITY
OF RADIO ELECTRONICS

NATIONAL AEROSPACE UNIVERSITY
KHARKIV AVIATION INSTITUTE

UNIVERSITY OF ŽILINA

CURRENT DIRECTIONS OF DEVELOPMENT OF INFORMATION AND COMMUNICATION TECHNOLOGIES AND CONTROL TOOLS

Proceedings of 14-th International

Scientific and Technical Conference

April 25 – 26, 2024

Volume 2: sections 3, 4, 5, 6

Baku – Kharkiv – Žilina – 2024

UDC 004/681.3 doi: https://doi.org/10.32620/ICT.24.t2

Abstracts of reports of the 14-th international scientific and technical conference "Current directions of development of information and communication technologies and control tools" are presented in the collection. Considered issues in the following directions: theoretical and applied aspects of decision-making systems, optimization and control of systems and processes; computer methods and means of information and communication technologies and management; security of functioning of computer systems and networks; information technologies in civil security; modern information and measurement systems; information technologies in civil security.

ORGANIZING COMMITTEE

Чотирнадцята міжнародна науково-технічна конференція “Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління” проводиться 25 та 26 квітня 2024 року в режимі ONLINE. Тези доповідей доступні в INTERNET.

ТОМ 1

СЕКЦІЯ 1. Теоретичні та прикладні аспекти прийняття рішень, оптимізації та управління системами і процесами

СЕКЦІЯ 2. Комп’ютерні методи і засоби інформаційно-комунікаційних технологій та управління

ТОМ 2

СЕКЦІЯ 3. Методи швидкої та достовірної обробки даних в комп’ютерних системах та мережах

Керівник секції: д.т.н., проф. В. В. Косенко, НУ «ПП», Полтава
Секретарка секції: к.т.н. Бельорін-Еррера О.М., НТУ «ХПІ», Харків

СЕКЦІЯ 4. Безпека функціонування комп’ютерних систем та мереж

Керівник секції: д.т.н., проф. О. А. Смірнов, ЦНТУ, Кропивницький
Секретар секції: к.т.н., доц. О. В. Сєвєрінов, ХНУРЕ, Харків

СЕКЦІЯ 5. Сучасні інформаційно-вимірювальні системи

Керівник секції: д.т.н., проф. О. О. Можаєв, ХНУВС, Харків
Секретар секції: PhD І. Ю. Петровська, НТУ «ХПІ», Харків

СЕКЦІЯ 6. Інформаційні технології у цивільній безпеці

Керівник секції: д.т.н., проф. В. А. Глива, КНУБА, Київ
Секретар секції: PhD Д. М. Главчев, НТУ «ХПІ», Харків

СЕКЦІЯ 3
МЕТОДИ ШВИДКОЇ ТА ДОСТОВІРНОЇ ОБРОБКИ ДАНИХ В КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ

Керівник секції: д.т.н., проф. В. В. Косенко, НУ «ПП», Полтава
Секретарка секції: к.т.н. Бельорін-Еррера О.М., НТУ «ХПІ», Харків

SELF-LEARNING COMPUTER SYSTEM BASED ON KNOWLEDGE TESTING IN A HYBRID EDUCATIONAL SYSTEM

Aliyeva A.E.
Institute of Control Systems, Baku, Azerbaijan

In contemporary society, the emergence of hybrid education systems blending traditional and remote learning necessitates fostering students' capacity for independent work. A modern expert must possess not just theoretical and practical proficiency in new technologies but also the ability to anticipate, predict, and resolve unconventional challenges in self-directed learning. Addressing these challenges through the development of an intelligent computer system is an urgent priority. Such a system would ensure students' autonomy in learning, as well as facilitate the assessment and evaluation of their knowledge [1, 2].

It's important to recognize that existing educational approaches should enhance both the quality of teaching materials and students' self-learning abilities.

Currently, students often memorize material without grasping its practical relevance, resulting in a cognitive overload that fails to develop practical skills. This phenomenon undermines the true essence of education, leading to dwindling interest among many students [3, 4]. **The aim of the article** is to analyze educational intellectual systems that exist in teaching and present the significance of the developed intellectual system was presented. The structure, functionality and interface of the intelligent teaching system developed for the application of hybrid teaching models in higher schools are shown.

References

1. Bryzgalina E. V. Artificial intelligence in education. *Analysis of implementation goals.* 2021, Volume 32 Issue No. 2. DOI: https://doi.org/10.31857/S023620070014856-8

2. Shubham J., Radha Krishna R., Prathamesh C. Evaluating artificial intelligence in education for next generation. *Journal of Physics: Conference Series* 1714 (2021), DOI: https://doi.org/10.1088/1742-6596/1714/1/012039

3. Aida-zade K., Aliyeva A. Computer System Concept of Self-Study, Testing and Knowledge Assessment. *5th International Conference on Problems of Cybernetics and Informatics (PCI)* / 28-30 Aug. 2023. DOI: https://doi.org/10.1109/PCI60110.2023

4. Алиева А. Э. Айда-заде К. Р. Анализ некоторых аспектов преподавания информатики в общеобразовательных школах // *Прикладная математика и фундаментальная информатика*, 2020, том 7, № 1, с. 15-22. DOI: https://doi.org/10.25206/2311-4908-2020-7-1-15-22

METHODS OF CALCULATING THE ANGULAR SIZE OF AN OBJECT IN A VIDEO CAMERA IMAGE

Alizada T.A.
Institute of Control Systems, Baku, Azerbaijan
Khaligov G.S.
State Border Service Academy, Baku, Azerbaijan

In some cases, in image processing [1], it becomes necessary to calculate the angular size of an object.

This need may arise for various reasons. One of such reasons is the use of a video camera mounted on a drone for the purpose of its navigation [2-4]. The object to be measured is pre-recognized in the image. This applies primarily to objects that are landmarks for navigation by video surveillance (the need for such a navigation method arises when GPS navigation is impossible, e.g., in combat zones).

The aim of the paper is to develop methods for calculating the angular size of an object in an image obtained from a video surveillance camera.

The paper proposes two methods to calculate the angular size of an object in an image obtained from a video surveillance camera.

The results presented in the paper show that both methods allow calculating the angular size of an object in an image quite accurately. Thus, either method can be used in practice. However, our computer experiments have shown that the second method is more accurate. The further away from the center of the image the measured object is, the more apparent is the advantage of the second method over the first.

The authors plan conducting further computer, semi-natural and full-scale experiments for a comprehensive comparative analysis of the methods presented in the paper.

References

1. Nixon M., Aguado A. Feature Extraction and Image Processing for Computer Vision. *Academic Press*, 4th Edition, December 2, 2020. DOI: https://doi.org/10.1016/C2017-0-02153-5

2. Alizada T., Sabziev E., Heydarov N. Improving the Efficiency of the MPU-6050 Sensor Module for Inertial Drone Navigation. *Modeling, Control and Information Technologies: Proceedings of International Scientific and Practical Conference*. 2023 (6), 83–86. DOI: https://doi.org/10.31713/MCIT.2023.023

3. Muradov S., Hashimov E., Sabziev E. Determining the location of the UAV equipped with a homing device based on radio beacons. *Modeling, Control and Information Technologies: Proceedings of International Scientific and Practical Conference*, 2023 (6), 54–56. DOI: https://doi.org/10.31713/MCIT.2023.013

4. Nabadova L., Sabziev E. Minimizing the time for UAV to reach a moving target. *Modeling, Control and Information Technologies: Proceedings of International Scientific and Practical Conference*. 2023 (6), 87–89. DOI: https://doi.org/10.31713/MCIT.2023.024

REPRESENTATION OF SOLUTIONS OF $\mathcal{M}$-SPECTRAL PROBLEM FOR DIFFUSION OPERATOR

Panahov E.S.
Military Scientific Research Institute Baku, Azerbaijan

In this article, we offer the $\mathcal{M}$-Sturm Liouville problem for the diffusion operator depending on initial condition. We obtain the representation of the solution of the $\mathcal{M}$-Sturm Liouville problem for diffusion operator through the $\mathcal{M}$-Laplace transform.

The purpose of this article is to advantage demonstrate a more generalized version of the representation of the solution of the Sturm Liouville problem for diffusion operator in classical analysis.

$$y'' + [E - V(X)]y = 0, x \geq 0.$$

The above equation reduces to the Klein Gordon s-wave equation. The Klein-Gordon equation is recognized as one of the most important in quantum field theory [5].

The equation is commonly used to describe dispersive wave phenomena. Consider the following form of the Klein-Gordon equation,

$$\left[\left(i\frac{\partial}{\partial t} - e\phi\right)^2 - \left(\frac{1}{i}\nabla - e\vec{A}\right)^2\right]\Psi = m^2\Psi.$$

This equation reduces to the diffusion equation [3],

$$\psi''(r) + [V^2 - 2EV]\psi(r) = -K^2\psi.$$

Bas, has been studied inverse nodal problem for the fractional diffusion equation [1].

Koyunbakan and Panakhov, have been proved that while q potential function for the diffusion operator in a finite range is determined in the range $\left[\frac{\pi}{2}, \pi\right]$ a single spectrum is sufficient to determine the potential function in the rest of the range [4].

Before coming to the main result, we offer some important definitions and properties about the $\mathcal{M}$-derivative.

Definition 1 [2] Let $f: [0, \infty] \to \mathbb{R}$ function be defined. The $\mathcal{M}$-derivative for $0 < \beta \leq 1$ is defined as follows

$$D_{\mathcal{M}}^{\beta,\gamma} f(t) = \lim_{\varepsilon \to 0} \frac{f\left(tE_\gamma\left(\varepsilon t^{-\beta}\right)\right) - f(t)}{\varepsilon},$$

where $E_\gamma\left(\varepsilon t^{-\beta}\right)$ is the Mittag-Leffler function [6].

Definition 2 [2] n-order linear non-homogeneous differential equation in terms of the $\mathcal{M}$-derivative is given as

$$a_0 D_{\mathcal{M}}^{n\alpha,\gamma} y + a_1 D_{\mathcal{M}}^{(n-1)\alpha,\gamma} y + \cdots + a_{n-1} D_{\mathcal{M}}^{\alpha,\gamma} y + a_n y = x(t),$$

where $0 < \alpha < 1$, $a_0 \neq 0$, $D_{\mathcal{M}}^{n\alpha,\gamma} y = D_{\mathcal{M}}^{\alpha,\gamma} D_{\mathcal{M}}^{\alpha,\gamma} \dots D_{\mathcal{M}}^{\alpha,\gamma}$ and a_0, a_1,…, a_n are constants or variables.

In this work our aim is to show that the $\mathcal{M}$- Sturm Liouville problem for diffusion operator more general version of the Sturm Liouville problem for diffusion operator in classical analysis.

Consider the $\mathcal{M}$- Sturm Liouville problem for diffusion operator

$$- D_{\mathcal{M}}^{\alpha,\gamma} D_{\mathcal{M}}^{\alpha,\gamma} y(x) + [q(x) + 2\lambda p(x)] y(x) = \lambda^2 y(x),$$

where the function $q(x)$ real and continuous and also $0 < \alpha \leq 1$.

Let us express the main result obtained in this study,

Theorem 1. Consider the $\mathcal{M}$- Sturm Liouville problem for diffusion operator, where the initial conditions are $y(0,\lambda) = 1$, $D_{\mathcal{M}}^{\alpha,\gamma} y(0,\lambda) = -h$ and $h = -\cot\alpha$. Then representation of the solution

$$y(x,\lambda) = \cos\left(\lambda\Gamma(\gamma+1)\frac{x^\alpha}{\alpha}\right) - \frac{h}{\lambda}\sin\left(\lambda\Gamma(\gamma+1)\frac{x^\alpha}{\alpha}\right)\frac{\Gamma(\gamma+1)}{\lambda} \times$$

$$\times \int_0^x \sin\left(\lambda\Gamma(\gamma+1)\left(\frac{x^\alpha}{\alpha} - \frac{\tau^\alpha}{\alpha}\right)\right)[q(\tau) + 2\lambda p(\tau)] y(\tau,\lambda)\, d_\alpha \tau.$$

References

1. Bas, E., (2015), The Inverse Nodal problem for the fractional diffusion equation. Acta Scientiarum. Technology, 37(2), 251-257.

2. Jarad, Fahd, Abdeljawad, Thabet, (2020), Generalized fractional derivatives and Laplace transform, Discrete and Continuous Dynamical Systems - Series S, Vol. 13, No. 3, pp. 709-722.

3. Jaulent, M., Jean, C., (1972), The inverse s-wave scattering problem for a class of potentials depending on energy, Communications in mathematical Physics, 28(3), 177-220.

4. Koyunbakan, H., Panakhov, E. S., (2007), Half-inverse problem for diffusion operators on the finite interval, Journal of Mathematical Analysis and Applications, 326(2), 1024-1030.

5. Sharma, L. K., Luhanga, P. V., Chimidza, S., (2011), Potentials for the Klein-Gordon and Dirac equations, Chiang Mai Journal of Science, 38(4), 514-526.

6. Vanterler, Jose, Capelas de Oliveira, Edmundo, (2017), A new truncated M-fractional derivative unifying some fractional derivatives with classical properties, International Journal of Analysis and Applications.

STEGANOGRAPHIC METHODS OF INFORMATION PROTECTION IN TELECOMMUNICATION SYSTEMS SPECIAL PURPOSE

Ibrahimov B.G.
Azerbaijan Technical University; National Defense University;Azerbaijan, Baku
Tahirova K.M.
Azerbaijan Technical University, Baku

Today, there are two main methods for ensuring information confidentiality in distributed automated information processing and management systems: cryptography and steganography [1].

Cryptography (or encryption) can be defined as secret recording. Its main function is to transfer information between two parties and prevent it from being read by a third party [1, 2].

Steganography (secret writing) assumes that the transmitted text “dissolves” into a larger message with a completely “extraneous” meaning. Therefore, recently the ability to hide additional information in transferred files has been used to protect transferred data from illegal copying.

This task has become especially relevant in connection with the rapid development of global computer networks, through which a huge amount of information is transmitted without the permission of the authors to copy and distribute it. Steganography is the ancient art of infiltrating private messages by hiding them in seemingly harmless messages in such a way that a third party is unaware of the existence of any hidden information [2, 3].

Global informatization society and intensive Strong information exchange requires the development of telecommunication systems, wired and wireless data transmission.

Telecommunication systems, in accordance with the ITU-T recommendation, must meet the requirements of information security, including confidentiality, integrity and availability information [2, 3, 4]. To solve the problem of protecting information from being read, The attacker uses cryptographic coding that is highly resistant to cryptanalysis.

However, when using open channels, an attacker can destroy encrypted messages or the communication channel. In this case, information protection can be ensured by steganographic methods, which allow secret transmission of important information over an open communication channel so that an attacker does not record the fact transmission and does not destroy the message.

The need to use steganography also arises if the use cryptographic methods is prohibited or is ineffective.

Thus, steganography is an effective protection when transmitting information used in real time, as well as when introducing digital watermarks, during the hidden transmission of control signals, for hidden storage information in other cases. The above emphasizes the relevance steganography research. Today, the use steganography is not standardized due to the lack standards for its use. This is

explained by the variety steganographic algorithms and their complexity classification and steganalysis [3, 4].

The development digital steganography requires the formation of a theoretical basis and the creation sustainable methods for embedding hidden information into a covering signal.

This, in the future, will allow us to standardize steganographic methods.

The analysis of steganographic methods, algorithms and tools showed that the known steganographic containers are single-component and are described by the expression:

$$F_i(u_i) = W[u_i, K, s_i], \ i = 1, N, \quad (1)$$

where $F_i(u_i)$ – counting the signal of a filled container; u_i – hidden message; s_i – empty container signal countdown.

From (1) it is clear that the process extracting a message is reduced to solving an equation with two unknowns. To solve this problem, one of two message embedding approaches is used.

Also, to increase the reliability of the transmitted message, the sending and receiving parties can use an additional key, K.

Thus, the following requirements are imposed on steganographic systems [1-5]:

1. High quality stego container.
2. The maximum possible amount of hidden data.
3. High speed of information hiding.
4. Possibility of their use for graphic files of other formats.
5. Possibility of introducing additional means of protecting hidden information (for example, encryption, skipping unimportant bits, etc.).

After completing the stage embedding information into the audio container, it is necessary to evaluate the distortions obtained during file modification. To do this, certain metrics are used, which can be divided into two broad categories: objective and subjective.

References

1. Shelukhin O.I., Kanaev S.D. Steganography, Algorithms and software implementation, Moscow, Hotline, Telecom. 2018. 592 p.

2. Ibrahimov B.G., Orujov A.O., Hasanov A.H., Tahirova K.M. (2021) Research and analysis efficiency fiber optical communication lines using quantum technology. *T-Comm*, vol. 15, no.10, pp. 50-54. DOI: 10.36724/2072-8735-2021-15-10-50-54

3. Wu, Zhijun, et al. Steganography and Steganalysis in Voice over IP: A Review// Sensors. Vol. 21, No 4. 2021. pp 10 - 32.

4. Solodukha R. A. Steganalysis of Bit Plane Complexity Segmentation algorithm//Information and Control Systems. 2023, no. 2, pp. 27–38. doi:10.31799/1684-8853-2023-2-27-38.

5. Hasanov A. H., Hashimov E. G. Analysis of the effectivness of communication and automated management systems //Modern directions of development of information and communication technologies and management tools, Abstracts of reports of the 12th Int. Scientific and Technical Conf. – 2022. – T. 1. – C. 1-4.

APPLICATIONS OF GRAPHS IN COGNITIVE MODELS

Sadiqli N.E.
Baku State University, Baku, Azerbaijan

The cognitive model approach offers an essential methodological framework for the deeper analysis of human thought and behavior. This approach enables the modeling of complex mental processes such as decision-making, problem-solving, and learning [1]. The application of these models opens up new ways to understand and solve complex issues in various fields.

These models are used in experimental psychology research, analysis of user behaviors, and product design. Furthermore, cognitive models are applied in areas such as artificial intelligence and machine learning to simulate human thought and develop complex problem-solving strategies.

Several methods and approaches exist for the construction and description of cognitive models. Examples include algorithms, simulations, and mathematical models. Algorithms are typically used to codify specific decision-making process-es, simulations are effective in modeling various scenarios and outcomes, and mathematical models provide a quantitative analysis of mental processes.

The aim of the paper is to use graphs to build and describe cognitive models.

Graphs are mathematical tools we use to describe the structure of information and relationships [2]. In the context of cognitive modeling, graphs play a crucial role in analyzing thought processes, decision-making mechanisms, and knowledge net-works. Through vertices and edges, graphs will show the relationships between in-dividual concepts and how they interconnect.

We implement the graph representation in computers using the C# programming language, utilizing the .NET platform and Windows Forms Application. Initially, we create a list. In the process of graph representation in computers, the fac-tors listed serve as vertices of the graph. We use the weight matrix method to digitally express the relationships and connections between these factors. The weight matrix is a numerical table showing the strength (weight) of connections existing between the vertices of the graph. In this table, the columns and rows correspond to the vertices of the graph, and eventually, each cell will note the degree of relation between the factors.

The representation of cognitive models with graphs is a good tool for us to more comfortably understand and analyze these models.

References

1. Busemeyer, Jerome R., Adele Diederich. Cognitive modeling. *Sage*, 2010. 215 p.
2. Riaz F., Ali K. M., Applications of Graph Theory in Computer Science. *Third International Conference on Computational Intelligence, Communication Systems and Networks, Bali, Indonesia*, 2011, pp. 142-145, DOI: https://doi.org/10.1109/CICSyN.2011.40.

FAULT TOLERANCE OF COMPUTER SYSTEMS BASED ON NON-POSITIONAL CORRECTION CODES

Yanko A., Martynenko A., Kruk O.
National University «Yuri Kondratyuk Poltava Polytechnic», Poltava, Ukraine

One of the promising areas for ensuring fault tolerance of computer systems (CS) is the widespread use of correction codes capable of detecting and correcting errors that occur in the dynamics of the data processing process [1].

A characteristic feature of such codes is the presence in the structure of constructing corrective codes of interdependent parts: information and control. The non-arithmetic nature of the procedures for obtaining check bits of the correcting code does not allow monitoring the results of arithmetic operations [2].

Thus, it is obvious that the use of positional correcting codes when implementing arithmetic operations in a CS operating in a positional number system is impossible. Non-positional codes, in particular codes in the system of residual classes (SRC), do not have this drawback. The equality of residues in the structure of the correcting code in the SRC is the basis for constructing codes capable of detecting and correcting errors in the process of implementing modular operations [3]. In addition, this property of non-positional codes serves as the basis for the implementation of exchange operations between accuracy, fault tolerance and speed of implementation of arithmetic operations in the dynamics of the CS computing process.

The purpose of the report is to conduct research on the effectiveness of using non-positional correction codes to ensure fault tolerance of computer systems.

The report argues that the specificity of representing numbers in the SRC allows, in some cases, not only to detect an error, but also to find the place of its occurrence, using only a single control base, which is impossible with existing methods of monitoring and correcting errors in the SRC. In some cases, error correction at a minimum code distance can be carried out either by projection method or by using the concept of an alternative set of numbers.

References

1. Krasnobayev V., Yanko A., Fil I. Research of the possibility of fault-tolerant operation of a computer system in a non-positional number system in residual classes. XI *International Scientific and Practical Conference "Information Control Systems &Technologies (ICST-Odessa-2023)"* 21th – 23th September, 2023, Odessa. P. 175–177. URL: http://icst-conf.com/2023.pdf

2. Krasnobayev V. A., Yanko A. S., Kovalchuk D. M. Control, Diagnostics and Error Correction in the Modular Number System. *The Sixth International Workshop on Computer Modeling and Intelligent Systems (CMIS 2023)*. 2023. P. 199–213. DOI: 10.32782/cmis/3392-17. URL: https://ceur-ws.org/Vol-3392/

3. Krasnobayev V., Kuznetsov A., Yanko A., Kuznetsova K. Correction codes in the system of residual classes. *6th International Scientific-Practical Conference PIC S&T 2019*. 2019. P. 488–492. DOI: https://doi.org/10.1109/PICST47496.2019.9061253

МЕТОД ВИЯВЛЕННЯ ТА ВИПРАВЛЕННЯ ПОМИЛОК НА ОСНОВІ ЧАСОВИХ ЧИСЛОВИХ ПЕРЕРІЗІВ

Янко А.С., Сабельнікова П.С.
Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна

Специфіка представлення чисел в непозиційній системі числення в системі залишкових класів (СЗК) дозволяє у ряді випадків не тільки виявити помилку, але й знайти місце її виникнення, використовуючи лише контрольну основу (модуль), що неможливо при існуючих методах контролю та виправлення помилок у позиційних системах числення [1, 2].

Запропоновані методи на основі альтернативної сукупності чисел (АСЧ) не можуть бути продуктивно використані у короткому ланцюжку обчислювального процесу комп'ютерних систем (КС) [3].

Тому виникає необхідність розробки процедур визначення АСЧ, за допомогою яких можлива ефективна корекція помилок у короткому ланцюжку процесу обробки інформації КС. У зв'язку з цим необхідно прагнути до зменшення числа k чисел, що перевіряються за рахунок підвищення інформативності альтернативного набору, тобто зменшення в АСЧ основ, по яких можлива помилка.

Метою доповіді є розробка ефективного методу визначення альтернативної сукупності чисел, що дозволяють підвищити інформативність, що скорочує час виправлення помилок у СЗК.

В доповіді наводяться результати на основі розробленого методу часових числових перерізів.

На його основі можлива ефективна корекція помилок у короткому ланцюжку процесу обробки інформації КС. Розроблений метод часових числових перерізів дозволяє суттєво скоротити кількість основ, по яких виникла помилка.

У результаті скорочується кількість чисел, що перевіряються, тобто скорочується час визначення та виправлення помилкової основи СЗК.

Список літератури

1. Krasnobayev V.A., Yanko A.S., Koshman S.A. The method of error detection and correction in the system of residual classes. *Computer science and cybersecurity*. 2016. Issue 1(1). P. 58–66. URL: https://periodicals.karazin.ua/cscs/article/view/6203

2. Krasnobayev V., Kuznetsov A., Yanko A., Kuznetsova K. Correction codes in the system of residual classes. *6th International Scientific-Practical Conference PIC S&T 2019*. 2019. P. 488–492. DOI: https://doi.org/10.1109/PICST47496.2019.9061253

3. Krasnobayev V., Kuznetsov A., Yanko A., Kuznetsova T. The analysis of the methods of data diagnostic in a residue number system. *3rd International Workshop on Computer Modeling and Intelligent Systems (CMIS-2020)*. 2020. P. 594–609. DOI: 10.32782/cmis/2608-46. URL: http://ceur-ws.org/Vol-2608/paper46.pdf

ВІДМОВОСТІЙКА КОМП'ЮТЕРНА СИСТЕМА В ЗАЛИШКОВИХ КЛАСАХ, ЗАСНОВАНА НА ПРОЦЕДУРІ ПОСТУПОВОЇ ДЕГРАДАЦІЇ

Янко А.С., Філь І.В., Крук О.О.
Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна

Непозиційна система числення в залишкових класах є ефективним засобом підвищення відмовостійкості комп'ютерних систем (КС) [1]. Це зумовлено наступними обставинами. Вихідна (без введення додаткової надмірності) структура КС, що функціонує у системі залишкових класів (СЗК) має попередню схильність до можливості відмовостійкого функціонування КС, це зумовлено впливом основних властивостей СЗК на структуру КС. Структура КС у СЗК подібна до структури багатопроцесорних КС у позиційній системі числення (ПСЧ).

Існує пряма аналогія структури КС у СЗК зі структурою резервованої системи ПСЧ, дана обставина, використовуючи відомі в теорії надійності підходи та математичні співвідношення для відповідних методів та способів резервування в ПСЧ, дозволяє синтезувати математичну модель для проведення оцінки та порівняльного аналізу відмовостійкості КС у СЗК. У СЗК застосування одного виду резервування зумовлює одночасну наявність інших видів резервування [2].

Метою доповіді є проведення аналізу процесу відмовостійкого функціонування комп'ютерної системи на основі використання непозиційної системи числення в залишкових класах.

В доповіді наводяться результати аналізу прикладу функціонування КС у СЗК, заданою інформаційними основами (модулями) $m_1=3$, $m_2=4$, $m_3=5$, $m_4=7$ і тільки однією контрольною основою $m_k=m_5=23$, які показали, що використання СЗК забезпечує більшу кількість працездатних станів КС з зниженою якістю (більша кількість рівнів деградації) функціонування, ніж кількість працездатних станів КС у двійковій ПСЧ.

Список літератури

1. Krasnobayev V., Kuznetsov A., Yanko A., Kuznetsova K. Correction codes in the system of residual classes. *6th International Scientific-Practical Conference PIC S&T 2019*. 2019. P. 488–492. DOI: https://doi.org/10.1109/PICST47496.2019.9061253

2. Янко А.С., Філь І.В. Забезпечення відмовостійкості комп'ютерних систем на основі коригувальних властивостей непозиційних кодових структур. *Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління*: тези доповідей тринадцятої міжнародної наук.-техн. конф. 26 – 27 квітня 2023 р. Т. 2. С. 51. DOI: https://doi.org/10.32620/ICT.23.t2

3. Yanko A., Fil I. Fault-resistant management information systems functioning in the modular number system. *XXXII International scientific and practical conference «Modern development of scienceand the latest perspectives»*. 2022. P. 319–322.

ЗНЕШУМЛЕННЯ МОВНИХ СИГНАЛІВ З ВИКОРИСТАННЯМ ДКП-ФІЛЬТРАЦІЇ

Брисін П.В., Лукін В.В.
Національний аерокосмічний університет ім. М. Є. Жуковського "Харківський авіаційний інститут", Харків, Україна

Шумозаглушення є одним із ключових питань у галузі обробки мовних сигналів, оскільки часто під час реєстрації (запису) на такі сигнали накладаються завади від різних джерел.

Одним із методів шумозаглушення є фільтрація на основі дискретного косинусного перетворення (ДКП). ДКП, як один із методів перетворення сигналів, надає зручну інструментальну основу для аналізу та обробки аудіосигналів. Використовуючи ДКП, мовний сигнал може бути представлений у вигляді набору коефіцієнтів, що відображають його локальний спектр. Застосовуючи порогову обробку ДКП-коефіцієнтів, можна суттєво придушити шум та підвищити якість мовного сигналу.

Метою доповіді є аналіз методу придушення адитивного білого гаусового шуму в мовних сигналах за допомогою ДКП-фільтрації. В **доповіді** надано оцінку доцільності застосування такого типу шумозаглушення та ефективності його в різних сценаріях.

Для аналізу ефективності фільтрації [1] використано як традиційне відношення сигнал/шум (ВСШ), так і метрику якості аудіосигналу PESQ [2].

Показано, що для тестових мовних сигналів ефективність залежить щонайменше від трьох чинників [3]: вхідного ВСШ, типу порога та параметра β, який використовується для встановлення порога.

Проведені дослідження показують, що:

1) поліпшення ВСШ за рахунок придушення шумів є найбільшим для низького вхідного ВСШ;

2) існують оптимальні значення β, що мають тенденцію до зростання при зменшенні вхідного ВСШ;

3) комбінований поріг, уперше протестований для мовних сигналів, працює краще, ніж жорсткий поріг.

Список літератури

1. M. Torcoli, T. Kastner and J. Herre, "Objective Measures of Perceptual Audio Quality Reviewed: An Evaluation of Their Application Domain Dependence, IEEE/ACM Transactions on Audio, Speech, and Language Processing, vol. 29, pp. 1530-1541, 2021.

2. Y. Hu and P. C. Loizou, "Evaluation of Objective Quality Measures for Speech Enhancement, IEEE Transactions on Audio, Speech, and Language Processing, vol. 16, no. 1, pp. 229-238, Jan. 2008.

3. S. Abramov, V. Abramova, V. Lukin, K. Egiazarian, Prediction of Signal Denoising Efficiency for DCT-Based Filter, Telecommunications and Radio Engineering, Vol. 78, No 13, 2019, pp. 1129-1142.

МЕТОДИ ШВИДКОЇ ТА ДОСТОВІРНОЇ ОБРОБКИ ІНФОРМАЦІЇ ПРИ РОЗРОБЦІ ІГОР

Коль Є.В., Сітніков В.І.
Харківський національний університет радіоелектроніки, Харків, Україна

Швидка та надійна обробка даних є важливою для забезпечення хорошого досвіду для гравців. Тому тема дослідження методів обробки інформації є важливою проблемою. До цих методів входять в першу чергу шляхи оптимізації даних, такі як попередня обробка даних, стиснення та рівень деталізації (LOD)[1]. LOD – це метод, який використовується в комп'ютерній графіці для оптимізації візуалізації 3D-моделей [2]. Також не менш важливим аспектом є оптимізація коду, тобто використання ефективних структур даних, виконання процесу профілювання, тобто збору та аналізу інформації про роботу програмного забезпечення з метою його оптимізації. Із завданням підвищення продуктивності пов'язана необхідність дослідження існуючих підходів, тобто патернів, їх аналізу та створення своїх методів що підходять під конкретну задачу розробника. Ігрові патерни – це типові рішення поширених проблем у розробці ігор, що використовуються для покращення дизайну ігрового процесу, зменшення часу розробки та покращення читабельності коду [3].

Метою доповіді є огляд існуючих шаблонів розробки ігор, визначення їх ключових аспектів що дозволяють підвищити швидкість та достовірність обробки інформації при розробці ігор.

В доповіді наводяться приклади найпоширеніших ігрових патернів. Наприклад Singleton – цей патерн гарантує, що існує лише один екземпляр певного класу, Observer – цей патерн дозволяє об'єктам отримувати сповіщення про події, State – використовується для зміни поведінки об'єкта залежно від його внутрішнього стану та Decorator – він використовується для динамічного додавання нових функціональних можливостей до об'єктів. Наведені приклади патернів дозволяють покращити дизайн ігрового процесу, зменшити час розробки та найголовніше підвищити продуктивність. Але також дослідження підтверджує що не існує універсального патерну що підходить до всіх випадків та надмірне їх використання може зробити код складним і незрозумілим.

Список літератури

1. Berezovskyi O. How to Optimize a Game: Video Game Optimization Best Practices for Console [Електронний ресурс] / Oleksandr Berezovskyi // Pingle Studio. – 2022. – Режим доступу до ресурсу: https://pinglestudio.com/blog/porting/video-game-optimization-best-practices-for-console.

2. Boeykens S. What Is LOD, or Level of Detail? [Електронний ресурс] / Stefan Boeykens // WTWH Media. – 2022. – Режим доступу до ресурсу: https://www.engineering.com/story/what-is-lod-or-level-of-detail.

3. Nystrom R. Game Programming Patterns / Robert Nystrom., 2014. – 354 с.

РОЗРОБКА ТА ОПТИМІЗАЦІЯ АЛГОРИТМІВ ПАРАЛЕЛЬНОЇ ОБРОБКИ ДАНИХ НА ГРАФІЧНИХ ПРОЦЕСОРАХ

Дерев'янко К.А., Гук А.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Зі зростанням обсягів даних і вимог до їх обробки виникає потреба у вдосконаленні алгоритмів паралельної обробки даних на графічних процесорах (GPU).

Використання GPU для обробки даних стає все більш актуальним, оскільки ці пристрої мають значні обчислювальні потужності та можуть ефективно виконувати паралельні обчислення [1]/

Адаптація традиційних алгоритмів обробки даних до потреб паралельної обробки на GPU вимагає специфічних підходів та технік. Важливо розглянути методи оптимізації використання ресурсів GPU для досягнення максимальної продуктивності та ефективності.

Ефективне управління пам'яттю на графічних процесорах є вирішальним для забезпечення необхідної швидкості обробки даних та уникнення перевантаження.

Паралельне програмування стає ключовим аспектом при розробці алгоритмів обробки даних на GPU і вимагає володіння специфічними навичками та підходами.

Важливо розглянути приклади застосування паралельної обробки даних на GPU в різних галузях.

Обробка графічної інформації у відеоігровій індустрії, наукові дослідження, такі як обробка зображень у медичній діагностиці, а також фінансові аналітичні додатки для аналізу великих обсягів фінансових даних - це лише кілька прикладів застосування паралельної обробки даних на графічних процесорах [2].

Метою доповіді є висвітлення важливості розробки та оптимізації алгоритмів паралельної обробки даних на графічних процесорах і їх застосування в різних галузях, а також для висвітлення ключових аспектів цього процесу та прикладів його застосування.

Список літератури

1. Симонюк О. В. Алгоритми Паралельної Обробки Даних / Олег Вікторович Симонюк. – Київ: Видавничій дім, 2010. – С. 131-154 – (Сучасні технології).

2. Марченко С. О. Алгоритми: Концепція та види / Сергій Олександрович Марченко. – Київ: Видавничій дім, 2003. – С. 482-489 – (Техніка).

РОЗРОБКА ВЕБ-СИСТЕМИ АВТОМАТИЧНОГО АНАЛІЗУ ТА ВИПРАВЛЕННЯ ПРОГРАМНОГО КОДУ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Зіарманд Д.Н., Гаврашенко А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасному світі спостерігається великий перехід від традиційних десктоп-додатків до веб-додатків. Цей тренд викликаний не лише зручністю та доступністю веб-технологій, а й їхньою динамічністю та можливістю постійного розвитку. Веб-додатки стають все складнішими, використовуючи нові технології та функціонал для задоволення потреб користувачів.

Проте, разом з цим розвитком, зростає і кількість помилок у програмному коді [1]. Це може бути викликано як недоліками в процесі написання коду, так і простими помилками, які важко виявити на етапі розробки. Крім того, постійні зміни в коді можуть призводити до збоїв та неправильної роботи веб-додатків.

Метою доповіді є розробка веб-системи, яка автоматично аналізує та пропонує виправлення програмного коду з використанням штучного інтелекту. Основним завданням цього проекту є зменшення часу, витраченого на виявлення та виправлення помилок у веб-додатках, що дозволить розробнику зосередитися більше на написанні логіки веб-додатку.

Одним з можливих рішень цієї проблеми є розробка веб-системи автоматичного аналізу та виправлення програмного коду з використанням штучного інтелекту [2]. Така система зможе автоматично аналізувати код на предмет помилок та пропонувати варіанти їх виправлення. Це зробить процес розробки продуктивнішим, покращить якість коду, зробивши його більш стабільним та надійним.

Для створення веб-додатку пропонується використати JavaScript та бібліотеку React.js [3], Material UI для стилізації, та react-highlight для відображення коду. Аналіз та виправлення коду буде здійснюватися за допомогою моделі gpt-3.5-turbo від OpenAI, з комунікацією через REST запити [4] до OpenAI API.

Список літератури

1. Flanagan D. JavaScript: The Definitive Guide. 7th ed. O'Reilly Media, 2020. 706 p.
2. Mitchell M. Artificial Intelligence: A Guide for Thinking Humans. Picador, 2020. 336 p.
3. Wieruch R. The Road to React: Your journey to master plain yet pragmatic React.js. Independently published, 2018. 226 p.
4. Richardson L., Ruby S., Amundsen M. RESTful Web APIs: Services for a Changing World. O'Reilly Media, 2013. 406 p.

ОПТИМІЗАЦІЯ АЛГОРИТМІВ ПОШУКУ НАЙКОРОТШОГО ШЛЯХУ ТА ІНШИХ АЛГОРИТМІВ НА ГРАФАХ

Маслов В.С., Гаврашенко А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

В наш час при постійному розвитку телекомунікаційних технологій в усіх галузях стрімко набувають популярності машинне навчання, комп'ютерний зір та інші напрямки комп'ютерних наук, в яких так чи інакше необхідне ефективне оброблення даних. Для цього використовують різні структури даних як способи представлення даних у зручному режимі для обробки різними алгоритмами, що дозволяють ефективно знайти рішення конкретно взятої задачі. У число таких структур даних входять і графи різних класів, які часто застосовуються на практиці та мають критично важливе значення для представлення та ефективного вирішення багатьох прикладних завдань.

Метою роботи є дослідження методів оптимізації алгоритмів для пошуку найкоротших шляхів та інших алгоритмів на графах.

Існує багато алгоритмів для роботи з графами, зокрема такі техніки, як пошук компонентів сильної зв'язності [1], пошук найкоротших шляхів від обраної вершини до всіх інших алгоритмом Дейкстри, пошук найкоротших шляхів між усіма вершинами алгоритмом Флойда-Уоршелла та ін. Відповідно, є декілька кроків для оптимізації алгоритмів для роботи з графами: безпосередній аналіз сучасних методів оптимізації алгоритмів пошуку найкоротших шляхів, дослідження, як структура графа впливає на ефективність алгоритмів пошуку найкоротших шляхів, зокрема проведення порівняльного аналізу кількості використаної пам'яті та асимптотики часу виконання алгоритмів, якими може бути ефективно розв'язано окремо взяту задачу як-от знаходження найкоротшого шляху при маршрутизації в мережах різних класів, пропозиції щодо нових методологій, які можуть покращити швидкість та точність алгоритмів пошуку найкоротших шляхів, обговорення можливості застосування машинного навчання для прогнозування оптимальних шляхів у графах [2], та приклади практичного застосування оптимізованих алгоритмів пошуку найкоротших шляхів у реальних системах транспорту та логістики.

Запропоновано ефективні методи оптимізації алгоритмів пошуку найкоротших шляхів на графах та приклади практичного застосування даних методів.

Список літератури

1. Кубайчук, О. О., Теренчук, С. А., & Єременко, Б. М. (2008). Оптимізація управління методом виділення сильно зв'язних компонентів на графах.

2. Thomas H. Cormen and others Introduction To Algorithms 4th Edition — Massachusetts: "The MIT Press", 2022. — 1312 с.

МЕТОД ЗМЕНШЕННЯ ЧАСУ ПЕРЕДАЧІ ДАНИХ У БЕЗПРОВІДНИХХ МЕРЕЖАХ

Можаєв О.О.
Харківський національний університет внутрішніх справ, Харків, Україна
Кучук Г.А., Лисиця Д.О.
Національний технічний університет «Харківський політехнічний інститут», Харків, Україна

Питання передачі інформації нині є актуальною проблемою. Людям завжди був потрібен швидкий та надійний канал передачі даних. З розвитком інформаційних технологій на зміну дротовим методам передачі інформації прийшли бездротові методи.

Бездротові мережі передачі даних (БМПД) повинні забезпечувати передачу даних з характеристиками, що дозволяють забезпечити вимоги користувачів, зокрема, забезпечити потенційну можливість доступу до ресурсів за прийнятний час. Серед факторів, що впливають на зміну часу передачі пакету даних на критичній ділянці, можна виділити такі: інтенсивність трафіку, час комутації пакета (залежить від типу маршрутизатора та його характеристик), пропускна здатність каналу передачі даних; обсяг пакета даних; довжина черги пакетів даних до каналу; коефіцієнт завантаження каналу службовою інформацією [1].

Метою доповіді є розробка методу зменшення часу передачі даних у безпровідній мережі за рахунок раціональної маршрутизації пакетів та зменшення обсягу службової інформації.

В доповіді наводяться результати дослідження залежності зміни часу передачі даних в БМПД від середньої затримки пакета даних, порівняння запропонованого методу зменшення часу передачі даних в БМПД за рахунок раціональної маршрутизації з методом маршрутизації, що застосовується в протоколі EIGRP. Суть запропонованого методу зменшення завантаження буферної пам'яті маршрутизатора полягає в реалізації механізму розвантаження службової мережевої інформації з буферної пам'яті маршрутизатора в інтервали часу, які йдуть за інтервалами максимального завантаження, коли частково вивільняються ресурси маршрутизатора в результаті зменшення інтенсивності вхідного трафіку.

Список літератури

1. Кучук Г. А. Метод перераспределения пропускной способности для уменьшения времени передачи данных в беспроводной сети / Г.А. Кучук, А.С. Мохаммад, А.А. Коваленко // Збірник наукових праць Харківського національного університету Повітряних Сил. – 2011. – № 3(29). – С. 140-145.

2. Янко А.С., Філь І.В. Забезпечення відмовостійкості комп'ютерних систем на основі коригувальних властивостей непозиційних кодових структур. *Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління*: тези доповідей тринадцятої міжнародної наук.-техн. конф. 26 – 27 квітня 2023 р. Т. 2. С. 51. DOI: https://doi.org/10.32620/ICT.23.t2

МЕТОД ПІДВИЩЕННЯ ПРОПУСКНОЇ ЗДАТНОСТІ БЕЗПРОВІДНИХ МЕРЕЖ

Серков О.А., Касілов О.В., Арутюнян Д.А.
Національний технічний університет «Харківський політехнічний інститут», Харків, Україна

Мета роботи – розробка методу підвищення пропускної здатності безпровідних мереж з мінімізацією семантичних похибок при прийомі інформації. На відміну від традиційних методів пропонується здійснювати відновлення речень, а не бітових чи символьних похибок.

Виявлено, що між семантичними сигналами декількох користувачів є значна кількість загальної інформації, яку пропонується використовувати для зменшення витрати смуги пропускання [1]. Вилучення загальної інформації пропонується здійснювати шляхом порівняння дисперсії кожного з вимірів двох семантичних векторів на ґрунті встановленого відсотку порогового рівня.

Семантичні ознаки, які вилучено з інформації джерела за допомогою моделі штучного інтелекту дозволяють визначати особисті характеристики користувача, що забезпечує базу знань для диференціації багатокористувальної семантичної інформації.

За рахунок окремого вилучення загальної та персоналізованої семантичної інформації різних користувачів формується модель інформаційного простору, який є простором семантичної моделі. Причому, загальна семантична інформація передається у межах одного й того ж частотне-часового ресурсу, а персоналізована змістова інформація передається окремо.

Виграш у використанні ресурсу виникає за рахунок повторного використання загальної інформації серед різних користувачів у інформаційному просторі моделі. В умовах низького співвідношення сигнал / шум (SNR) розпізнавання речової семантичної інформації здійснюють за допомогою механізму навчання нейронної мережі.

Таким чином побудова семантичної системи зв’язку на фізичному рівні розширяє рівень теоретичного уявлення Шеннона [2], а модель штучного інтелекту стає важливою складовою при реалізації семантичної комунікації на основі моделі інформаційного простору.

Список літератури

1. P Zhang. Model division multiple access for semantic communications / Front Inform Technol Electron Eng 24, 801-812 (2023). https://doi.org/10.1631/FITEE.2300196. Download citation. Received: 21 March 2023.

2. Shannon CE, 1948. A mathematical theory of communication. *Bell Syst Tech J*, 27(3):379-423. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x

МНОЖИННИЙ ДОСТУП У БЕЗПРОВІДНИХ МЕРЕЖАХ НАДШИРОКОСМУГОВОГО ЗВ'ЯЗКУ

Серков О.А., Лазуренко Б.О.
Національний технічний університет «Харківський політехнічний інститут», Харків, Україна

Використання надширокосмугових сигналів (НШС) у безпровідних мережах дозволяє передавати інформацію на швидкостях, які значно перевищують швидкість передачі традиційних засобів зв'язку з високим рівнем завадозахищеності [1].

Однак широкосмужність інформаційних сигналів накладає суттєві обмеження на ефективність використання радіочастотного спектру, особливо при організації множинного доступу (МД). Технологія МД прагне використовувати загальну інформацію користувачів для усунення втрат смуги пропускання за рахунок надлишкових передач. Окреме вилучення і передача загальної та персоналізованої семантичної інформації здійснюють на ґрунті технології штучного інтелекту (ШІ), який використовують для створення бази знань як в приймачі, так і передавачі [2, 3].

Здійснюючи запит на з'єднання, спочатку передають загальну інформацію – опорну послідовність чипів у вигляді моделі, яку порівнюють з наявними моделями у базі даних базової станції.

При відсутності її у базі даних – додають до бази та вилучають при наступних сеансах зв'язку. Продовжуючи сеанс зв'язку, користувачі відправляють на базову станцію тільки синхросигнал та персональну семантичну інформацію.

Отримавши їх, базова станція відновляє первинні семантичні сигнали кожного користувача шляхом кореляції прийнятого та опорного сигналів, який вилучають з бази знань базової станції.

Таким чином майже удвічі зменшують навантаження на безпровідний канал зв'язку при організації множинного доступу.

Список літератури

1. Серков О.А., Лазуренко, Б.О., Пєвнєв В.Я., Ткаченко В.А., Харченко В.С. Спосіб передачі інформації надширокосмуговими імпульсними сигналами // Патент України на винахід № 123519 U МПК H04B 1/69, H04B 7/00, Опубл. 14.04.2021, Бюл. № 15.

2. Zhang P, Peng MG, Cui SG, et al., 2022b. Theory and techniques for "intellicise" wireless networks. Front Inform Technol Electron Eng, 23(1):1-4. https://doi.org/10.1631/FITEE.2210000

3. Zhang P, Xu XD, Dong C, et al., 2022c. Intellicise communication system: model-driven semantic communications. J China Univ Posts Telecommun, 29(1):2-12. https://doi.org/10.19682/j.cnki.1005-8885.2022.2002

СЕКЦІЯ 4
БЕЗПЕКА ФУНКЦІОНУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ

Керівник секції: д.т.н., проф. О. А. Смірнов, ЦНТУ, Кропивницький
Секретар секції: к.т.н., доц. О. В. Сєвєрінов, ХНУРЕ, Харків

ENHANCING COMPUTER NETWORK SECURITY THROUGH INFORMATION FLOW ANALYSIS

Tanriverdiyev E.E.
National Defense University, Baku, Azerbaijan

Cybersecurity threats, ranging from malware and phishing attacks to advanced persistent threats and distributed denial-of-service (DDoS) attacks, have evolved in complexity and scale. These threats not only aim to steal sensitive information but also seek to disrupt the normal functioning of network systems, posing a grave risk to the integrity and availability of critical information and services. The stakes are higher than ever, with potential impacts including financial losses, damage to reputation, and even threats to national security [1].

Given this context, there is a pressing need for innovative approaches to enhance the security and resilience of computer networks. Traditional methods, while necessary, are no longer sufficient to address the dynamic and complex nature of modern cyber threats. This thesis argues for a paradigm shift towards a more analytical and predictive approach to network security, leveraging mathematical models to deeply understand and monitor the flow of information within networks. By applying principles of graph theory, statistical analysis, and computational algorithms, this approach seeks to identify patterns, anomalies, and potential vulnerabilities in information flow, enabling proactive identification and mitigation of security threats.

This mathematical approach to information flow analysis offers a novel perspective on network monitoring and security control methodologies. It emphasizes the need to go beyond surface-level defenses and delve into the fundamental dynamics of data transmission and interaction within networks. Through rigorous analysis and modeling, it is possible to uncover insights that are not apparent through traditional security measures alone. This thesis aims to explore these methodologies, demonstrating how they can be applied to enhance the detection and prevention of security breaches in complex network environments.

Information flow in computer networks refers to the transmission of data across network components such as routers, switches, servers, and end-user devices. This flow is governed by various protocols that ensure data is sent and received accurately and efficiently. Understanding these dynamics is crucial for network design, management, and security. Characteristics of information flow: volume; velocity; variability; veracity. To quantitatively analyze information flow, mathematical

models are employed. One foundational concept is the graph theory, where a network is modeled as a graph G= (V, E) with nodes V representing network devices and edges E representing the connections between them. Data flow can then be analyzed in terms of paths, connectivity, and flow capacities [2].

Entropy, H(X), is used to quantify the uncertainty or randomness in the information flow, providing insights into the network's behavior. A higher entropy value can indicate unpredictable traffic patterns, possibly hinting at anomalies or security breaches.

$$H(X) = -\sum_{i=1}^{n} P(x_i) \log P(x_i)$$

Where P (x_i) is the probability of occurrence of a specific flow pattern x_i in the network. The summation runs over all possible flow patterns, quantifying the overall unpredictability of network traffic. This measure is particularly useful for detecting changes in network behavior, such as the emergence of security threats like DDoS attacks, malware propagation, or unauthorized data exfiltration activities. Higher entropy values might indicate a more complex and less predictable network state, potentially requiring further investigation. By applying graph theory and entropy measures, network analysts and security professionals can gain valuable insights into the structure, performance, and security posture of computer networks [3-4]. This approach enables: The identification of critical nodes and links, aiding in the optimization of network infrastructure, Enhanced monitoring and anomaly detection capabilities, facilitating the early detection of security incidents and network performance issues, Informed decision-making regarding network design, security strategies, and resource allocation. These mathematical tools and concepts are pivotal in managing the complexity of modern computer networks, ensuring they remain robust, efficient, and secure against an ever-evolving landscape of cyber threats and operational challenges. The application of mathematical models has demonstrated significant potential in enhancing network security. Through entropy measurement, anomalies in data traffic were effectively identified, indicating potential security breaches. In summary, the analysis of information flow in computer networks encompasses understanding the dynamics of data transmission, employing mathematical models to represent and quantify these flows, and using this knowledge to enhance network security and efficiency.

References

1. J. Doe and A. B. Smith, "Advanced Analytics for Network Flow Detection in Cybersecurity," in J. Network Security, vol. 15, no. 2, pp. 112-130, Apr. 2021.

2. H. Li, Y. Zhang, and R. Kumar, "Graph Theoretical Approaches in Network Security: A Comprehensive Study," Computers Networks, vol. 88, pp. 50-75, May 2022.

3. S. Patel and F. Wang, "Entropy-Based Anomaly Detection in Distributed Networks," IEEE Trans. Networks Sci. Eng., vol. 10, no. 3, pp. 204-219, June 2023.

4. Hasanov A. H., Hashimov E. G. Analysis of the effectivness of communication and automated management systems //Modern directions of development of information and communication technologies and management tools, Abstracts of reports of the 12th Int. Scientific and Technical Conf. – 2022. – T. 1. – p. 1-4.

MITIGATING THE IMPACT OF DESTABILIZING INFORMATION IN COMPUTER NETWORKS: A MATHEMATICAL APPROACH

Tanriverdiyev E.E.
National Defense University, Baku, Azerbaijan

Signature-based detection systems, firewalls, and antivirus software play crucial roles in defending networks against known threats. However, the dynamic and evolving nature of destabilizing information, characterized by its ability to mutate, adapt, and circumvent conventional security protocols, necessitates more advanced and anticipatory approaches to network security [1].

To effectively limit the flow of destabilizing information through computer networks, it is imperative to develop mathematical models that encapsulate the nuances of how such information spreads. These models need to account for various factors, including network topology, node vulnerability, and the inherent characteristics of the information itself. By utilizing differential equations, we can construct a dynamic framework that describes the rate of information spread and identifies potential control mechanisms to mitigate this process.

The structure of a network significantly influences the propagation of destabilizing information. Network topology refers to the arrangement of nodes (computers, devices) and edges (connections) in a network. Different topologies (e.g., star, mesh, and tree) exhibit unique vulnerabilities to information spread. For instance, in highly centralized networks, the compromise of a central node can lead to rapid dissemination of harmful information across the entire network.

Node vulnerability is a measure of a node's susceptibility to destabilizing information, influenced by factors such as security measures in place, software version, and the node's role within the network. To mathematically model these aspects, let N be the set of nodes in the network, with each node $i \in \mathrm{N}$ having a vulnerability score V_i , which can range from 0 (completely secure) to 1 (completely vulnerable).

We consider the flow of destabilizing information through a network as a dynamic process that can be described by a system of differential equations. Let $I(t)$ represent the fraction of nodes affected by destabilizing information at time t. The rate of change of $I(t)$ over time can be influenced by various factors, such as the average node vulnerability and the rate of information spread through network connections [2-4].

A basic model for the spread of information in a network can be represented by the equation:

$$\frac{dI}{dt} = \beta * I(t) * \big(1 - I(t)\big) * V,$$

where: $\frac{dI}{dt}$ - is the rate of change of the fraction of nodes affected by the information over time; β - is the transmission rate of the information, representing how quickly it spreads from an affected node to a susceptible node through a network connection; V - is the average vulnerability of the network, calculated as

$$V = \frac{1}{|N|}\sum_{i\in \mathrm{N}} v_i.$$

This equation is a simplified model that assumes homogeneous mixing of nodes, meaning that any node can potentially interact with any other node in the network. However, real-world networks often exhibit more complex patterns of interaction, necessitating more sophisticated models that incorporate network topology explicitly [5].

For networks with well-defined topology, the model can be extended to incorporate the adjacency matrix *A*, where $A_{ij}=1$ if there is a direct connection between nodes *i* and *j*, and $A_{ij}=0$ otherwise. The model then becomes:

$$\frac{dI_i}{dt} = \beta * \sum_{j\in \mathrm{N}} A_{ij} \ * \ I_j\,(t) * \left(1 - I_j\,(t)\right) * v_i\,,$$

where $\frac{dI_i}{dt}$ represents the rate of change of the fraction of node *i* being affected by the destabilizing information.

The characteristics of the destabilizing information itself, such as its ability to evade detection or exploit specific vulnerabilities, can also be integrated into the model. For example, the transmission rate β can be adjusted based on the sophistication level of the malware or the credibility of the misinformation.

Through these mathematical models, it becomes possible to simulate the spread of destabilizing information across networks and evaluate the effectiveness of various intervention strategies. By adjusting parameters such as network topology, node vulnerability, and information characteristics, these models offer valuable insights into the dynamics of information flow and provide a foundation for developing robust cybersecurity measures.

References

1. T. Johnson and L. M. O'Connor, "Differential Equation Models for Cyber Threat Propagation in Network Systems," IEEE Trans. Information Forensics Security, vol. 19, no. 4, pp. 789-805, Mar. 2024.

2. A. Gupta, B. Singh, and C. Patel, "Mitigating Information Spread in Social Networks: A Machine Learning Approach," Journal of Computational Social Science, vol. 6, no. 1, pp. 123-142, Jan. 2021.

3. Hasanov A. H., Hashimov E. G. Analysis of the effectivness of communication and automated management systems //Modern directions of development of information and communication technologies and management tools, Abstracts of reports of the 12th Int. Scientific and Technical Conf. – 2022. – T. 1. – p. 1-4.

4. İbrahimov, B.G., Hashimov, E.G. Research quality of functioning of the efficiency optical telecommunication systems using spectral technologies // Problems of informatization. Proceedings of 11-th International Scientific and Technical Conference. Vol. 1. - Baku – Kharkiv – Bielsko-Biala: november 16 – 17**,** -2023, -p.29-30. doi: https://doi.org/10.32620/PI.23.t1

5. K. Zhang, M. Qiu, and N. Zhao, "Evaluating the Resilience of Complex Networks Against Cyber Attacks: A Graph-Theoretic Approach," Computers & Security, vol. 103, pp. 101925, Feb. 2022.

EFFECTIVENESS OF INFORMATION PROTECTION MANAGEMENT IN CRITICAL INFORMATION INFRASTRUCTURES

Mammadov I.A., Sadigov U.K.
Azerbaijan Technical University, Baku, Azerbaijan

Currently, the rapid development digital technologies leads to the emergence of new threats and vulnerabilities in telecommunication systems in various areas society, the exploitation which increases the likelihood of a successful attack by an attacker. In this regard, there is a need to explore methods for increasing the security telecommunication networks in the face various attacks in critical information infrastructures (CII). Critical information infrastructure – objects critical information infrastructure, as well as telecommunication networks used to organize the interaction such objects [1-3].

The analysis showed [4-6] that critical information infrastructure objects are complex telecommunication systems. In this case, the task arises - to study the effectiveness of the information security system, which depends on the quality of its management processes.

The main purpose of CII information security management processes is the timely development and implementation of control actions on the managed object. An indicator effectiveness is the probability timely adoption and implementation of the correct decision:

$$E(t,\lambda_i) = W[P_{cbn}(t,\lambda_i), A_{np}(t,\lambda_i)], \quad i = \overline{1,k}. \tag{1}$$

The resulting analytical expression (1) describes the essence of the proposed new approach for creating methods for calculating performance indicators for information security management in CII. In addition, expression (1) allows you to get a fairly complete picture of the reaction of the protection system to various situations in telecommunication communication systems and clearly demonstrates its operation.

Based on a new approach for creating calculation methods, we select information security efficiency indicators, which will proceed from the fact that the efficiency information security management in CII is assessed using the communication network management efficiency indicator.

Let's consider the procedure for assessing the effectiveness information security management in critical information infrastructures:

1. The probability of correct decision making is expressed as follows:

$$A_{np}(t,\lambda_i) = \frac{1}{N_s}\sum_{j=1}^{N_s}(1/L_j)\cdot M_{np.j} \quad , \quad j = 1, 2, 3, ..., N_s, \tag{2}$$

where N_s – number of situations considered; L_j – number decision makers (DM) involved in work for the *j-th* situation; $M_{np.j}$ – the number ocorrectly made decisions for the j-th situation.

2. The probability of timely and correct decision making is defined as:

$$P_{cbn}(t,\lambda_i)=\sum_{j=1}^{N_S}(1/M_{np.j})\cdot R_j\ ,\ \ j=1,2,3,...,N_S\ , \tag{3}$$

where R_j – the number of decisions made timely and correctly for the *j-th* situation is found as follows:

$$R_j=\sum_{i=1}^{L}R_{i\,j}\ ,\ \ j=1,2,3,...,N_S\ , \tag{4}$$

From expression (5) the following inequalities can be obtained:

$$R_{i\,j}=1,\ \text{if}\ \ t_{i\,j}\le t_{all.},\qquad R_{i\,j}=0,\ \text{if}\ \ t_{i\,j}\ge t_{all.}. \tag{5}$$

where $t_{i\,j}$ – the current value of the time spent on making a decision by the i-th decision maker in the j-th situation; $t_{all.}$ – acceptable time to make a decision.

As a result of the study, analytical expressions (2),…,(5) were obtained, which help to create the opportunity to evaluate the performance indicators of information security management with the help of which the following important results can be obtained.

References

1. Hasanov A. H., Hashimov E. G. Analysis of the effectivness of communication and automated management systems //Modern directions of development of information and communication technologies and management tools, Abstracts of reports of the 12th Int. Scientific and Technical Conf. – 2022. – T. 1. – C. 1-4.

2. Мамедов И.А., Садыгов У.К. Анализ процессов установления соединений в системах связи объектов критической информационной инфраструктуры// Материалы XXVII-Международная научно-техническая конференция по «Современные средства связи», БГАС, Минск 2022.- С.199-202.

3. İbrahimov B. et al. Research and analysis indicators fiber-optic communication lines using spectral technologies //Advanced information systems. – 2022. – T. 6. – №. 1. – C. 61-64.

4. Старикова А.А., Макарова Д.Г. Оценка эффективности управления системой защиты информации в государственных информационных системах//Интерэкспо Гео-Сибирь. 2017. Т. 8.188 с.

5. Ibrahimov, B.G., Hashimov, E.G., Hasanov, A.H., Mammadov, T.H. Research throughput multiservice telecommunication networks // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. Матеріали 10-і міжнародної науково-технічної конференції, 9-10 квітня 2020. Том1. Баку-Харків-Жиліна, 2020, с.30.

6. İbrahimov, B.G., Hashimov, E.G. Research and analysis of fiber-optic communication lines based on wave multiplexing technology // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. Тези доповідей тринадцятої міжнародної науково-технічної конференції, - Харків: - 26 – 27 квітня, - 2023, Том 2: - pp.4-5.

INVESTIGATION OF CTS TESTS FAILS, RELATED TO WIFI NETWORK SSID, DURING ANDROID FIRMWARE CERTIFICATION

Hlavchev D., Popello M.
National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine
Lishuk Yu.
Lviv Polytechnic National University, Lviv, Ukraine

The Android Open Source Project (AOSP) [1] is an open-source operating system (OS) supported by Google. Its feature is that it allows manufacturers of various devices to modify it and use it according to their own needs, equipment features, etc [2]. But AOSP is not Android, although it is quite similar to it, there are quite a few differences between these OS. The thing is that although AOSP contains all the necessary components and libraries that can ensure the operation of a particular device and the operating system as a whole, AOSP is not integrated into the Google ecosystem. Only Android has official Google Services, official support for Google Play, Google Maps, and more. Therefore, AOSP is often used by hardware developers, enthusiasts, and open-source projects who want to create their own customized version of the OS that will not depend on Google and its services. Instead, Android with Google services is usually used on devices sold to consumers in the global market, as they provide a more enriched user experience with access to a wide range of services and applications.

The main feature is access to millions of apps through the Google Play Store. In such devices, when the operating system is loaded, you can see the inscription "Powered by Android". In order for AOSP to become Android, it is necessary to pass certification from Google, using sets of special tests [3]. If the tests are passed, the firmware is certified.

The purpose of the report is to analyze the practical experience of the Android-based firmware certification process, potential errors that may occur in the process of performing CTS tests [4], and ways to solve them. In particular, attention will be focused on errors related to WiFi network testing, which were successfully reproduced using a Nokia 7 smartphone with the Android 9 operating system and the *android-cts-9.0_r20* test suite.

The report analyzes issues related to CTS tests as a component of the Android firmware certification process, as well as approaches to solving errors that arise during the testing process and lead to test failures.

The Android certification procedure includes several key tests, each of which has its own specifics and purpose. The most important are the CTS and GTS tests. Let's consider them in more detail. CTS (Compatibility Test Suite) – checks whether the device meets the Android compatibility specifications, ensuring the ability to run applications from Google Play without problems. GTS (Google Test Suite) – focuses on testing Google-specific functions and services, including Google applications and access to the Google Play Store [3, 4]. There are other types of tests, but in this case, we will not focus on them. Together, these tests ensure that an Android device is not only compatible with a wide range of applications and services available on the

market but also meets high-security standards, providing users safe and reliable experience with the device using.

The largest of these test packages is a set of CTS tests that test the main functions of the device and operating system components. The advantage of this package is that its source code is open source and is contained in the cts folder in the AOSP root directory. Therefore, in some cases, if there is not enough information, you can add additional logging, and check more details of the test execution, or simply see how this or that test works.

One of the areas of CTS testing is tests related to WiFi networks. Practical experiments and analysis of test code have shown that it is possible to accidentally get tests fail even when everything is fine. In particular, for the **CtsDevicePolicyManagerTestCases** module, when performing tests from the **MeteredDataRestrictionTest.java** file, you may receive an error that the name of the WiFi point (SSID) to which the device under test is connected, contains spaces. After all, the following call is executed in the **setWifiMeteredStatus** method using the **executeCmd** command: *cmd netpolicy set metered-network <**WIFI_SSID**> true/false*. Thus, if the name of our WiFi point contains spaces, this command will be broken into several parts, losing its structure, and will not be executed correctly. As a result of the test failure, there will be an error: Timeout waiting for network reconnection. Therefore, in some cases, there may be problems related to this, and if the WiFi access point is renamed correctly (without spaces), the tests will start to pass successfully.

As a conclusion, we can say that certification from Google is a complex and painstaking process, so sometimes errors may occur in CTS tests, the reason of which is difficult to understand. Therefore, an important step will be to add additional logging or analyze the test code in order to identify the cause of the error. In this case, it was clearly demonstrated the need to use WiFi points that do not contain gaps when testing the device. On the other hand, in the process of writing tests, it is necessary to take into account such types of errors, and not insert variables into the "raw" command, without additional checking for possible problems if the variable has unexpected values.

References

1. Android OS Core Topics. AOSP. URL: https://source.android.com/core
2. Главчев Д. М. Розширення області застосування AOSP для використання в бортових комп'ютерних системах на залізничному транспорті / Д. М. Главчев // Сучасні напрями розвитку інформаційно-комунікаційних техн. та засобів управління : тези доп. 13-ї міжнар. наук.-техн. конф., 26-27 квітня 2023 р., Баку–Харків–Жиліна : [у 2 т.]. Т. 1 : секція 1, 3, 4 / Нац. ун-т оборони Азербайджанської Республіки [та ін.]. – Харків : Impress, 2023. – С. 41-42.
3. Tests overview. URL: https://source.android.com/docs/core/tests
4. CTS Tests. URL: https://source.android.com/docs/compatibility/cts

ANALYSIS OF BUILT-IN KEY STORAGE MECHANISMS IN THE ANDROID OPERATING SYSTEM

Balagura D.S, Sydorenko Z.M.
Kharkiv National University of Radioelectronics, Kharkiv, Ukraine

The Android operating system is one of the most prevalent operating systems worldwide. Based on open sources, as of 2023, over 3 billion devices globally were operating under this operating system. It is evident that Android-powered devices are utilized across various domains, ranging from mobile communication and IoT systems to the management of technological processes within device groups. Naturally, a substantial portion of these devices may store and process information that requires protection against unauthorized access or modification through the use of cryptographic algorithms. A crucial aspect of employing cryptographic algorithms is the storage of private keys [1-3]. Android provides various mechanisms for secure key storage in the operating system itself or on the device. Developers may choose an approach based on their specific use case. **The work provides** some analysis of general methods for secure private key storage in Android OS which uses OS mechanisms and/or hardware platform capabilities.

Android Keystore System is a system-provided cryptographic API that allows developers to store and retrieve cryptographic keys securely. It provides developers with a secure container (keystore) for key storage. All keys stored in the keystore are protected against extraction. Android Keystore offers hardware-backed security, if available on the device. While no system can be considered completely invulnerable, the Android Keystore is designed to provide a high level of security for cryptographic key storage on devices developed for Android OS.

Secure Elements or Trusted Execution Environments (TEE): Some devices support secure elements or TEEs to store cryptographic keys securely. These environments are designed to be isolated from the main parts of operating system and resistant to attacks. If you need to store small pieces of sensitive information like keys, using of Secure Shared Preferences with encryption is one of the options as well Secure Shared Preferences is an approach in Android application development to enhance the security of storing sensitive information such as user preferences, authentication tokens, or encryption keys. The standard Shared Preferences in Android allows developers to store and retrieve key-value pairs, but it doesn't provide inherent encryption, making the stored data susceptible to unauthorized access. Secure Shared Preferences aims to address this limitation by introducing encryption mechanisms to protect the stored data.

References

1. "Android Cookbook: Problems and Solutions for Android Developers 2nd Edition, O'Reilly, Ian F. Darwin, 2017

2. "Android Security Internals ", No Starch Press, Inc, Nikolay Elenkov, 2015

3. Trusted Execution Environment a Complete Guide, The Art of Service, 2021

CAUSES OF ENERGY CONSUMPTION IN MOBILE DEVICES AND SUGGESTED SOLUTIONS

Mustafayeva N.A.
Mingachevir State University, Mingachevir, Azerbaijan

Nowadays, smart phones have become an integral part of our lives. Their use is increasing and almost everyone uses it. As everyone knows, these smart phones operate with a specific energy source. Currently, one of the biggest problems is that the energy storage capacity of smart phones is decreasing day by day. Sometimes, due to a lack of energy at a very important moment, our work is interrupted or not completed at all.

The aim of the paper is to talk about the reasons for energy consumption on Android devices and how to eliminate them.

1. One of the reasons for energy consumption in mobile devices is that the screen is too bright. A screen that is too bright increases energy consumption. So, keep the screen brightness in auto mode. Thus, your device will automatically adjust the brightness of the screen according to the light.

2. A second reason for energy consumption is that account synchronization is left on. Turning off account synchronization causes a significant reduction in device power consumption. Account sync is triggered each time mobile data is enabled and runs as a background process on the device. It continues as long as the Internet is active. This causes serious energy depletion. If you turn off this feature, you will have to check email or other programs manually. Also, apps like WhatsApp will not automatically copy chats. But in return, the energy consumption of your device will decrease and you will be able to use the device comfortably for up to 1 full day.

3. Another reason for energy consumption in mobile applications is that functions such as Wi-Fi, Bluetooth and GPS remain open. Functions such as Wi-F and Bluetooth are always active when they are on, so they consume a lot of energy. Therefore, keep these functions off when not in use, keeping them off when not in use will increase battery life.

The GPS system is the main source of energy consumption in smart devices. Because currently, almost most programs can work with the GPS program on the phone. At this time, the number of processes in the background increases, location search through GPS is always provided. Therefore, too much energy is spent on this process. Therefore, if you are not using map applications, it is recommended that you keep the GPS settings turned off.

4. If you don't close the programs after you are done using them, the program will always run in the background. This increases energy consumption. When you close the programs after you are done, those processes stop. Only the processes of system programs remain behind, which leads to less energy consumption than before. Therefore, it is recommended that you close the programs running in the background.

In addition to what we have listed above, you can save energy in your device in other ways. One of them is to set the number of processes running in the background from the "Developer Options" section on the device. As you know, background processes are constantly consuming energy. The smaller their number,

the more energy savings you can achieve. But it is worth noting that if you reduce the number of background processes, the program will not be active after exiting many programs. All you have to do is log in and see again to verify your accounts.

Use power saving modes if available on your device. This will help drastically reduce the power consumption of your device. These features automatically close background processes when enabled and prevent them from restarting until you touch the device. With these functions, the duration of the daily energy capacity of the battery is also increased. In addition to all this, you can use additional programs. You can close background processes with programs like Task Killer. Thus, only the processes of system programs remain on the device. You can search and download them from the market. It is very convenient to use. And finally, let's note that another reason for energy consumption in smartphones is that we don't completely exit from other programs that we use very often, such as Facebook, Instagram, Twitter and WhatsApp, when we close them, they work in the background and consume the device's energy. Instead of closing these programs one by one, we recommend using a program that automatically exits such programs running in the background.

References

1. Vasile C. V., Pattinson C., and Kor A. L. Mobile phones and energy consumption. *Green IT Engineering: Social, Business and Industrial Applications, Springer*: – 2029. p. 243-271. DOI: https://doi.org/10.1007/978-3-030-00253-4_11

2. El Outmani, A., Jaara, E. M., & Azizi, M. Literature Review of Energy Consumption Modeling for Mobile Devices. In International Conference on Advanced Intelligent Systems for Sustainable Development. *Cham: Springer Nature Switzerland*: – 2022. pp. 99-112.

ОСОБЛИВОСТІ ВИКОРИСТАННЯ VIVADO HLS В КОНТЕКСТІ ПОБУДОВИ АЛГОРИТМІВ ОБРОБКИ ЗОБРАЖЕНЬ

Філіппенко І.В., Корнієнко В.Р.
Харківський національний університет радіоелектроніки, Харків, Україна

Питання скорочення часу проектування користувацьких IP ядер з метою реалізації блоків апаратного прискорення та прототипування нових алгоритмів є актуальною проблемою з науковою та інженерною складовою Однією з найважливіших складових є вибір частини алгоритму що буде реалізовуватись та особливостей паралелізації імплементації, що у випадку обробки зображень є доцільним шляхом прискорення[1]. Зокрема, слід визначити що побудова оптимального шляху обробки з метою запобігання пропуску кадрів і забезпечення низької затримки між вхідним та вихідним кадром є одними з головних критеріїв оцінки в подібних рішеннях.

Метою доповіді є дослідження можливостей Vitis HSL для побудови системи обробки зображень з підтримкою декількох різновидів алгоритмів.

В доповіді наводяться результати вимірювань latency для використання передачі даних між блоками, розподілу трафіку з використанням DMA та AXI-FIFO буферів для пересилання даних між апаратною та програмною частиною.

Зокрема проведено дослідження ефективності використання AXI STREAM та AXI-SUBSET блоків з метою підвищення швидкості передачі між блоками та апаратного виділення фрагментів трафіку. Наведені результати показують перспективність та доцільність використання HLS для розробки алгоритмів обробки зображень на технологічній платформі SoC. Наступні етапи дослідження включають до себе особливості використання часткової реконфігурації FPGA частини та побудови рішень з використанням контейнеризації додатків на PS частині FPGA зокрема для аудіо та відео складових.

Список літератури

1. Kortli Y., Gabsi S., Jridi M., Alfalou A., Atri M. Hw/Sw Co-Design technique for 2D fast fourier transform algorithm on Zynq SoC. Integration. 2021. Vol. 82. P. 78–88. DOI: 10.1016/j.vlsi.2021.09.005

ВИКОРИСТАННЯ АРХІТЕКТУРИ ONION ARCHITECTURE У ВЕБ-ДОДАТКАХ ДЛЯ СПРОЩЕННЯ ТЕСТУВАННЯ

Золотайко Є.І., Холєв В.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Сьогодні до тестування програмного забезпечення ставляться комплексно: існує багато різновидів тестів, створюються технології для полегшення побудови тестів. Але тестуванню також має сприяти сама архітектура додатку, бо без достатнього його розбиття на окремі модулі процес написання тестів може дуже сильно вповільнитися, а самі тести будуть менш ефективними. Є декілька архітектур, що спрощують тестування додатку, серед них у веб-розробці популярною є Onion Architecture, бо, вона надає компроміс між складністю у вивчанні й імплементації та можливістю підтримувати й масштабувати додаток [1].

Основна ідея Onion Architecture полягає в тому, що код додатку розбивається на шари, впаковані один в інший так, що бізнес-логіка розташована в центрі, як ядро (core), а інші шари вибудовуються навколо нього. Це сприяє високій гнучкості, оскільки зміни в одному з шарів не впливають безпосередньо на інші [2]. Шари в Onion Architecture включають:

- Domain Layer (Доменний шар). Містить основну бізнес-логіку та доменні об'єкти, повинен бути чистими від залежностей від інших частин системи;
- Application Layer (Шар застосунків). Відповідає за координацію дій та виконання бізнес-логіки, обробляє запити та викликає методи з Domain Layer;
- Infrastructure Layer (Інфраструктурний шар). Містить зовнішні та технічні аспекти, забезпечує доступ до даних та зовнішніх ресурсів для Application Layer;
- Presentation Layer (Шар представлення). Отримує дані від Application Layer та відображає їх для користувача [2].

У висновку, Onion Architecture є архітектурою програмного забезпечення, чиє використання дозволяє досягти більш простого тестування. Це досягається цього шляхом розбиття коду додатку на декілька чітко виділених шарів, що не мають тісних залежностей між собою.

Список літератури

1. Süleyman A. Comparing clean architecture, onion architecture, and traditional architectural approaches in CQRS context. Medium. URL: https://topuzas.medium.com/comparing-clean-architecture-onion-architecture-and-traditional-architectural-approaches-in-cqrs-2820119de1e1

2. Traversi A. Understanding onion architecture: an example folder structure. Medium. URL: https://medium.com/@alessandro.traversi/understanding-onion-architecture-an-example-folder-structure-9c62208cc97d

РОЗРОБКА ТА ФУНКЦІОНУВАННЯ КОРПОРАТИВНОЇ КОМПЮТЕРНОХ МЕРЕЖІ ПРОВАЙДЕРА

Севостьянова О.М., Гусаров Є.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Сьогодні провайдери грають критичну роль у глобальному зв'язку, забезпечуючи мільйонам користувачів доступ до інформації та послуг через Інтернет. їхні мережі постійно розвиваються, адаптуючись до нових технологій та вимог користувачів, що дозволяє забезпечити ефективність та надійність зв'язку у сучасному цифровому світі[1].

Метою доповіді є побудова корпоративної комп’ютерної мережі провайдера для подальшої діяльності та підбір і налаштування обладнання .

В доповіді наводяться результати побудови корпоративної мережі для провайдера Union.com. Мережева інфраструктура, яка забезпечує надійний і швидкий зв'язок між клієнтами та послугами провайдера, забезпечуючи при цьому високий рівень безпеки та продуктивності. Проектування мережевої архітектури: першим кроком у побудові корпоративної мережі є ретельне проектування архітектури. Це включає в себе розгляд різних компонентів, таких як комутатори, маршрутизатори, сервери, брандмауери та інші пристрої, а також створення оптимізованого плану їх розташування та взаємодії [2].

Надання мережевих послуг: Після того, як архітектура мережі розроблена, наступним кроком є надання мережевих послуг. Сюди входить встановлення та налаштування програмного забезпечення, моніторинг та управління мережею, а також надання рішень для забезпечення безпеки.

Моніторинг та підтримка: Однак побудова мережі - це не кінцевий пункт, а безперервний процес. Ми пропонуємо постійний моніторинг мережі та її компонентів, а також швидке реагування на проблеми або збої в роботі.

Список літератури

1. Лунтовський А. Проектування та дослідження комп\'ютерних мереж / А. Лунтовський, І. Мельник. – Київ: Університет "Україна", 2010. – 362 с.

2. Karumanchi N. Elements of Computer Networking [Електронний ресурс] / Narasimha Karumanchi // CareerMonk Publications. – 2014. – Режим доступу до ресурсу: https://books.google.com.ua/books/about/Elements_of_Computer_Networking.html?id=qs_voAEACAAJ&redir_esc=y.

ТЕХНОЛОГІЇ БЛОКЧЕЙН В МІЖОПЕРАТОРСЬКИХ РОЗРАХУНКАХ В СФЕРІ ТЕЛЕКОМУНІКАЦІЙ

Смідович Л.С., Кулик Ю.О.
Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна

Одним із напрямків діяльності оператора телекомунікацій є міжоператорський обмін трафіком. При цьому виникають задачі узгодження тарифів, взаєморозрахунків, та узгодження обсягу трафіку.

Взаєморозрахунки зазвичай проводяться у кінці розрахункового періоду (тиждень, місяць) і при наявності значних розходжень їх узгодження може тривати довго.

Помилки тарифікації, фрод тощо, якщо їх виявлено несвоєчасно, можуть призводити до значних фінансових втрат. Тому актуальною є задача автоматизації та прискорення узгодження між операторами обсягу голосового трафіку та його вартості.

Метою доповіді є розгляд можливостей використання технологій блокчейн для автоматизації узгодження міжоператорського та роумінгового трафіку, що прискорить взаєморозрахунки та зменшить фінансові втрати за рахунок запобігання фроду та вирішення конфліктів.

Кожний голосовий виклик можна розглядати як окрему транзакцію. Міжнародні виклики зазвичай проходять через декількох транзитних операторів, і послуга вважається наданою, коли виклик доставлено кінцевому абоненту. Фродом в такому випадку є FAS (False Answer Supervision), коли транзитний оператор імітує відповідь абонента з використанням автовідповідача. Застосування не вірних або не узгоджених тарифів також може бути причиною фінансових втрат.

Блокчейн, завдяки таким своїм властивостям як децентралізація зберігання даних, прозорість та недоступність для втручання може стати ефективним інструментом для вирішення цих проблем [1].

Пропонується використовувати технологію smart contract для публікації, підтвердження та застосування тарифних планів, відповідних умов SLA тощо.

Виклик (CDR, який йому відповідає) узгоджується як окрема транзакція між двома операторами та може зберігатися у розподіленому реєстрі. Умовою реалізації такого підходу є наявність блокчейн платформи, яка надає відповідний функціонал та API, що використовується декількома операторами.

Список літератури

1. TM Forum. TR279 CSP Use Cases Utilizing Blockchain v4.0.0 [Електронний ресурс] – Режим доступу: https://www.tmforum.org/resources/technical-specification/tr279-csp-use-cases-utilizing-blockchain-v4-0-0/

КРИПТОАНАЛІЗ СТАНДАРТНИХ ФУНКЦІЙ ГЕШУВАННЯ

Щербакова Ю.А.
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут», Харків, Україна

Безпека в ІТ-сфері є надважливим процесом, а геш-функції є складовою цього процесу [1, 2]. Якісний ріст в останні роки можливостей сучасних комп'ютерних систем вимагає ретельної перевірки криптостійкості, в тому числі і функцій гешування.

Метою доповіді є доведення результатів криптоаналізу найбільш поширених на цей час геш-функцій, а саме «Купина» (ДСТУ 7564:2014), «Стриборг» (ГОСТ 34.11-2018), MD5 та SHA (модифікацій 256 та 512). Для дослідження колізійних властивостей розглянутих функцій гешування спочатку були розроблені зменшені версії цих функцій, а далі згідно методики проводилось оцінювання даних алгоритмів. Тестування було проведено на коротших повідомленнях, а дані було екстрапольовано. Атаки проводилися в декілька раундів, за результатами яких виводилось середнє значення.

Вимоги до геш-функції:

1) фіксована довжина вихідного значення геш: h(m)=const;

2) швидкодія у напрямі $m \rightarrow h(m)$;

3) неможливість у реальному часі зворотнього розв'язку $h(m) \rightarrow m$;

4) унеможливлення колізій (коли $m' \neq m \Rightarrow h(m') = h(m)$;

5) аваланшний ефект;

Аналіз зазначених функцій було проведено по напрямах: швидкодія; пошук колізій за методом, що заснований на парадоксі днів народження; аваланшний ефект.

Наведені дані демонструють, що:

– «Купина» в обох своїх версіях (на 256 та 512 біт) є чудовим вибором для роботи і у системах, де потрібна швидкодія та висока надійність, навіть не дивлячись на те, що вона програє у швидкості MD5 та SHA256;

– «Купина-512» виявилась більш стійкою і за кількістю спроб теж;

– «Стрибог-256» на початковому етапі показав себе гірше, аніж «Купина-256», MD5 та SHA256, але зі збільшенням розміру повідомлень до 256 біт він показав себе краще, аніж SHA256;

– «Стрибог-512» виявився найбільш стійким до колізій серед усіх пропонованих функцій як на початкових етапах тестування, так і на більших повідомленнях.

Список літератури

1. ДСТУ ISO 7564:2014 Інформаційні технології. Криптографічний захист інформації. Функція хешування. Київ, 2015. 39 с.

2. Євсеєв С. П., Йохов О. Ю., Король О. Г. Хешування даних в інформаційних системах: монографія – Х.: Вид. ХНЕУ, – 312 с.

РИЗИКИ ТА ЗАХОДИ ЗАХИСТУ ДЛЯ БЛОКЧЕЙНУ SOLANA

Черкасов Д.К., Сітніков В.І.
Харківський національний університет радіоелектроніки, Харків, Україна

Безпека комп'ютерних систем та мереж є одним з найважливіших питань у сучасному інформаційному суспільстві. Зростаюча кількість і складність кібератак робить це питання все більш актуальним.

Мережа Solana - одна з найпопулярніших блокчейн-платформ. Її використовують для розробки децентралізованих додатків, смарт-контрактів, ігор та інших проектів. Вона має ряд механізмів, які роблять її безпечною платформою для розробки та використання децентралізованих додатків.

Проте, важливо пам’ятати, що жодна система не є абсолютно безпечною. Тому користувачам Solana слід вживати заходів для захисту своїх даних та коштів [1].

Метою доповіді є аналіз та висвітлювання стратегії та методів, які використовує мережа Solana для забезпечення безпеки своєї інфраструктури та захисту від кібератак.

У доповіді розглядаються питання безпеки мережі Solana. А саме стійкість до DDoS-атак за рахунок Proof-of-Stake, що робить її більш стійкою до DDoS-атак, ніж мережі, що використовують Proof-of-Work, так як POS не вимагає ресурсоємного майнінгу, що робить атаки більш складними і дорогими.

Solana також використовує інші методи захисту, такі як:

– фільтрація трафіку і балансування навантаження [2],

– захист смарт-контрактів за допомогою формальних інструменти верифікації, які можуть математично довести, що смарт-контракти не є вразливими;

– алгоритм цифрового підпису, який використовується для гарантування автентичності та цілісності даних; він заснований на еліптичній кривій Едвардса і використовує криптографічну хеш-функцію SHA-512 для захисту приватних ключів. [3]

Список літератури

1. Exploring Solana: A Comprehensive Guide to Accounts, Tokens, Transactions, and Ensuring Asset Security [Електронний ресурс]. – 2024. – Режим доступу до ресурсу: https://slowmist.medium.com/exploring-solana-a-comprehensive-guide-to-accounts-tokens-transactions-and-ensuring-asset-cf910837ccb3.

2. DDoS Attacks on Solana [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: https://cryptopotato.com/solana-network-suffers-another-reported-ddos-attack/.

3. Ed25519: high-speed high-security signatures [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://ed25519.cr.yp.to/.

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Дорофєєва К.І., Євгеньєв А.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Інформаційна безпека відіграє важливу роль у забезпеченні інтересів будь-якої держави. Створення розвиненого й захищеного інформаційного середовища є неодмінною умовою розвитку суспільства та держави.

Метою доповіді є визначення заходів забезпечення інформаційної безпеки держави.

Останнім часом в багатьох країнах все більше уваги приділяється проблемам захисту інформації та пошуків шляхів її вирішення. Разом з цим посилюється небезпека несанкціонованого втручання в роботу інформаційних систем, і вагомість наслідків такого втручання дуже сильно зросла. Як наслідок, в багатьох країнах все більше уваги приділяється проблемам захисту інформації та пошуків шляхів її вирішення [1]. Згідно з [2] під інформаційною безпекою розуміється: здатність держави, суспільства, соціальної групи забезпечити з визначеною імовірністю достатні й захищені інформаційні ресурси, надійність функціонування інформаційно-комунікативних систем в інтересах стійкого розвитку суспільства; протистояти інформаційним небезпекам і загрозам, негативним інформаційним впливам на суспільну й індивідуальну свідомість, психіку людей, а також на інформаційні структури; виробляти особистісні й групові навички і вміння безпечного поводження; підтримувати постійну готовність до адекватних мір в інформаційному протиборстві.

Інформаційна безпека має три основні складові. Конфіденційність належить до захисту чутливої інформації від несанкціонованого доступу. Цілісність означає захист точності і повноти інформації та програмного забезпечення. Доступність – це забезпечення доступності інформації і основних послуг для користувачів потрібний для нього час [3].

Система інформаційної безпеки сьогодні є низкою підсистем. Вивчення науково-теоретичних та практичних проблем інформаційної безпеки дозволить визначити та розв'язати завдання щодо створення системи інформаційної безпеки, яка б функціонувала ефективно.

Список літератури

1. Степко О.М. Аналіз головних складових інформаційної безпеки держави // Науковий вісник Інституту міжнародних відносин НАУ.–Сер.: Економіка, право, політологія, туризм.–2011.–Вип.1(3). – С.90-99.

2. Yevseiev Serhii et al. "Development of a concept for building a critical infrastructure facilities security system." Eastern-European Journal of Enterprise Technologies 3.9 (2021): 111.

3. Косогов О.М., Сірик А.О. Сучасна політика безпеки кіберпростору в умовах його мілітаризації // Сучасні інформаційні технології у сфері безпеки та оборони, 2015. – №3(24). – С. 181-186.

ЕФЕКТИВНІСТЬ ТА МАЙБУТНІЙ РОЗВИТОК СИСТЕМ ЗБОРУ МЕРЕЖЕВИХ АРТЕФАКТІВ

Малахова А.А., Євгеньєв А.М.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасному цифровому світі ефективні системи збору мережевих артефактів відіграють важливу роль у виявленні та протидії кіберзагрозам.

Метою доповіді є розгляд майбутніх перспектив розвитку таких систем і ключові інновації, які можуть забезпечити їх ефективність та надійність [1, 2].

Сучасні системи збору мережевих артефактів базуються на різноманітних технологіях, включаючи сенсори, журнали подій, системи моніторингу мережевого трафіку тощо.

Ефективність систем збору мережевих артефактів є ключовим аспектом в забезпеченні кібербезпеки та виявленні потенційних загроз.

Ці системи відіграють важливу роль у зборі, аналізі та моніторингу мережевої активності, дозволяючи виявляти аномальні зміни та підозрілу поведінку [3].

Майбутні перспективи розвитку систем збору мережевих артефактів досить передбачувані і можуть характеризуватись такими аспектами як автоматизація та інтелектуалізація, розширення області застосування, безпека та конфіденційність.

Якщо говорити за інновації у розвитку збору мережевих артефактів, то розвиток нових алгоритмів аналізу даних – це необхідні міри для забезпечення цілісності та автентифікації даних. [3, 4].

Майбутній розвиток систем збору мережевих артефактів відкриває перед нами широкі перспективи для підвищення безпеки та ефективності цифрових мереж. Для досягнення цілей необхідно продовжувати інвестувати в дослідження та розробки в цих напрямках, що дозволить забезпечити нам безпеку та стабільність у цифровому середовищі [3, 5].

Список літератури

1. Arvidsson V., Mønsted T. Generating innovation potential: How digital entrepreneurs conceal and propagate new technology. The Journal of Strategic Information Systems. 2018. Vol. 27, no. 4. P. 369–383. (дата звернення: 05.03.2024).

2. Martovytskyi V., Ruban I., Kovalenko A., Sievierinov O. (2022, June). Method for Detecting FDI Attacks on Intelligent Power Networks. In International Scientific-Practical Conference" Information Technology for Education, Science and Technics", Springer Nature Switzerland (pp. 715-731).

3. Martovytskyi Vitalii, et al. Devising an approach to the identification of system users by their behavior using machine learning methods." Eastern-European Journal of Enterprise Technologies 117.3 (2022).

4. Local Network Security. Cybersecurity. Indianapolis, Indiana, 2018. P. 423–447.

5. Cybersecurity and Network Security / A. Guha et al. Wiley & Sons, Limited, John, 2022.

АНАЛІЗ ВИКОРИСТАННЯ ДНК-ПЕРЕТВОРЕНЬ В КРИПТОГРАФІЇ ТА СТЕГАНОГРАФІЇ

Скибенко М.С.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасному цифровому світі, де обмін інформацією став неодмінною складовою повсякденного життя, безпека та конфіденційність цієї інформації стають особливо важливими.

З кожним днем зростає кількість цифрових даних, які обробляються, зберігаються та передаються, тому виникає потреба у захисті цих даних від несанкціонованого доступу, змін та витоку.

Метою доповіді є аналіз застосування ДНК-перетворень в сфері зберігання даних, криптографії та стеганографії.

Стеганографія ДНК: стеганографія - це техніка приховування інформації в медіафайлах. В контексті ДНК-перетворень, стеганографія включає вбудовування секретних повідомлень в ДНК-секвенції, так що вони є непомітними без спеціального декодування.

ДНК-криптографія: цей принцип використовує властивості ДНК для створення нових методів шифрування. Наприклад, можна використати ДНК-секвенції як ключі для шифрування та дешифрування повідомлень. Також можна використати ДНК для створення біометричних систем безпеки, які використовують унікальні ДНК-характеристики особи для перевірки її ідентичності [1].

Генерація якісної випадкової послідовності – найбільш складна частина багатьох криптографічних операцій.

В [2] показано, що для забезпечення стійкості шифрування необхідно забезпечити надійний ключ, а це в свою чергу, досягається шляхом використання криптографічно якісних генераторів випадкових послідовностей.

Для вирішення цієї задачі пропонується використовувати властивості ДНК.

Висновок: за результатами аналізу, проведеного авторами, пропонується використовувати ДНК-перетворення для вирішення актуальних криптографічних та стеганографічних задач.

Список літератури

1. Yevheniev A.M., Skybenko M.S., Dorofieieva K., Savchenko I., Botvinchuk V. DNA-cryptography // Yevheniev A.M., Skybenko M.S., Dorofieieva K., Savchenko I., Botvinchuk V. Trends in the development of modern scientific: між. конф., 2021. с. 471-476.

2. Sievierinov O., Evheniev A. (2018). DNA Cryptosystem Using a Simple Replacement. «Інформаційні системи та технології» ICT-2018, 389.

3. Cohen A., Wigderson A. Dispersers, deterministic amplification, and weak random sources // In Proceedings of the 30th IEEE Symposium on Foundations of Computer Science. –1989. – P. 14–19.

ПОРІВНЯЛЬНИЙ АНАЛІЗ СУЧАСНИХ КВАНТОВО-СТІЙКИХ КРИПТОСИСТЕМ

Хівренко Г.О.
Харківський національний університет радіоелектроніки, Харків, Україна

З розвитком квантових обчислень з'являється потреба в модернізації криптографії. Алгоритми розкладання цілих чисел і дискретних логарифмів, які використовуються в RSA та Elliptic Curve Cryptography (ECC), стають вразливими до квантових атак.

Спірос Магліверас дослідив логарифмічні підписи, які лягли в основу криптосистем MST1 та MST2. MST3 - нова криптосистема, що поєднує MST1 та MST2, ґрунтується на логарифмічних підписах і випадкових покриттях неабелевих груп. Вона використовує Судзукі 2-групи для реалізації. MST3 - квантово-стійка криптосистема, що використовується для створення цифрових підписів.

Серед переваг можна виділити: стійкість до квантових атак, відносно невеликий розмір ключів, можливість використання на мобільних пристроях.

Метою доповіді є розгляд та порівняння пост-квантових алгоритмів, що перемогли у конкурсі NIST у 2022 році.

Переможцями конкурсу є: CRYSTALS-Dilithium - криптосистема на основі ґраток Falcon - криптосистема на основі ґраток, SPHINCS+ - криптосистема на основі хеш-функцій. MST3 не брала участі в конкурсі NIST, але вона має схожі характеристики з CRYSTALS-Dilithium і Falcon, хоч і побудована на логарифмічних підписах.

Актуальним є створення і розвиток нових алгоримів стійких до квантових атак, зниження складності обчислень та розміру ключів, оптимізація для швидшої роботи, розробка планів та методів переходу з доквантових криптосистем на постквантові, створення тестових векторів та інструментів для оцінки стійкості алгоритмів.

Також одним з найактуальніших питань є розробка та прийняття міжнародних стандартів для постквантових криптосистем.

Виконано попередній порівняльний аналіз алгоритмів переможців конкурсу NIST та криптосистеми MST3, який показує що на поточний момент алгоритми CRYSTALS-Dilithium та MST3 лідирують з огляду на розмір ключа, швидкість підпису та швидкість перевірки, у порівнянні з іншими алгоритмами які вибрав за переможців NIST.

Список літератури

1. Hong, Haibo & Li, Jing & Wang, Licheng & Yang, Yixian & Niu, Xinxin. (2014). A Digital Signature Scheme Based on MST3 Cryptosystems. Mathematical Problems in Engineering. 2014. 10.1155/2014/630421.

2. Svaba, Pavol. (2011). Covers and Logarithmic Signatures of Finite Groups in Cryptography.

3. NIST. (2022). First Four Quantum-Resistant Cryptographic Algorithms.

ФРАКТАЛЬНЕ ШИФРУВАННЯ КЛІЄНТ-СЕРВЕРНИХ ЗАСТОСУНКІВ

Сєвєрінов О.В., Лєвтєров О.А., Балагура Д.С.
Харківський національний університет радіоелектроніки, Харків, Україна

При сучасному цифровому розвитку у всіх галузях господарства усе більше залежність від використання технологій, смартфонів, комп'ютерів і Інтернету. Однак, зі збільшенням кількості інформації, яка обробляється й передається через мережі, зростає й ризик несанкціонованого доступу до неї з боку зловмисників [1]. Одним з таких видів передавання інформації є архітектура "Клієнт-Сервер" ("мережа Клієнт-Сервер"). Щоб захистити цифрові данні, що передаються в мережі від злочинців повинно використовувати шифрування.

Одним з альтернативних сучасних методів шифрування є метод фрактального шифрування, який використовує як кодуючу функцію фрактальну послідовність [2]. **Метою доповіді** є розгляд принципів фрактального шифрування клієнт-серверних застосунків.

Фрактальну послідовність одержують за допомогою ітераційної функції, яка у свою чергу є однобічною функцією, у таких функцій визначення аргументів за значенням самої функцій не може бути зроблене більш ефективно, ніж перебором по безлічі значень початкових параметрів [3]. Для опису ітераційної функції, досить указати набір дійсних чисел, які задають початкові умови ітераційного процесу побудови фрактальної послідовності. Це дає досить простий метод шифрування, він є варіантом гамірования - процесу "накладення" гама-послідовності на відкриті дані [4], де в якості гама-послідовності (послідовності псевдовипадкових елементів) використовується фрактальна послідовність, що генерується за допомогою ітераційної функції за початковими параметрами [5].

Таким чином, використання фрактальних послідовностей як ключа для шифрування достатньо просте й ефективне. Для їх побудови необхідна невелика кількість параметрів, при цьому на виході формуються об’єкти зі складними хаотичними межами.

Список літератури

1. Голубничий Д.Ю., Сєвєрінов О.В., Коломійцев О.В., Місюра О.М., Третяк В.Ф., Власов А.В., Крук Б.М. (2021). Аналіз сучасних загроз в інформаційних системах за складовими загроз: кібербезпеки, інформаційної безпеки та безпеки інформації.

2. Mandelbrot, B. The Fractal Geometry of Nature. USA: Echo Point Books & Media, LLC. 2021. 500 p. DOI: https://doi.org/10.1119/1.13295.

3. Soumitro Banerjee. Fractal Image Compression. Available at: https://youtu.be/Lte3xpmH2_g (accessed 23.03.2023).

4. Xian Y., Wang X. Fractal sorting matrix and its application on chaotic image encryption //Information Sciences. – 2021. – Т. 547. – С. 1154-1169.

5. Chen G., Ueta T. Yet another chaotic attractor //International Journal of Bifurcation and chaos. – 1999. – Т. 9. – №. 07. – С. 1465–1466.

ВИКОРИСТАННЯ ТРИФАКТОРНОЇ АВТЕНТИФІКАЦІЇ ДЛЯ ЗБІЛЬШЕННЯ НАДІЙНОСТІ ЗАХИСТУ ІНФОРМАЦІЇ

Куштим М.О., Сєвєрінов О.В.
Харківський національний університет радіоелектроніки, Харків, Україна

В останні роки можна побачити тенденцію все більш широкого використання двофакторної автентифікації, що обумовлюється збільшенням інтересів злочинців щодо пошуку нових способів її зламу та підриву довіри до неї. Незважаючи на свою більшу простоту та зручність, двофакторна автентифікація має власний ряд недоліків.

У системах з 2FA користувач надає лише дві форми ідентифікації для доступу до системи, що може залишити систему вразливою у разі компрометації одного з факторів, що робить її менш надійною. Крім того два фактори можуть виявитися вразливими для атак зловмисників через соціальну інженерію або інші методи шахрайства [1].

Використання факторів автентифікації по окремості дає змогу злочинцям зосередитися на них для обходу захисту, що зменшує кінцеву надійність 2FA як такої, але технічно застосування цих факторів разом забезпечує кращий захист облікових записів користувачів в Інтернеті від несанкціонованого доступу порівняно з одно- або двофакторними методами [2]. Навіть якщо облікові дані користувача будуть скомпрометовані, зловмисники не зможуть отримати доступ до облікового запису, якщо вони не мають додаткових факторів автентифікації.

Метою доповіді є реалізація трифакторної автентифікації у власному створеному додатку та спроба її обходу з метою доказу прояву більшої надійності захисту облікових записів від несанкціонованого доступу порівняно з двофакторною автентифікацією.

В такому випадку зламування MFA потребує спільного злому всіх трьох факторів, що ускладнює завдання зловмисників. Це суттєво підвищує вартість та складність атаки, роблячи систему більш захищеною [3]. Крім того, деякі методи трифакторної автентифікації, такі як біометричні сканери, можуть бути зручнішими для користувачів, ніж введення пароля або використання додаткових пристроїв.

Список літератури

1. Кліпоносова В.С., Сєвєрінов О.В. Сучасні методи біометричної ідентифікації та автентифікації користувачів. ВА ЗС АР; НТУ" ХПІ"; НАУ, ДП" ПДПРОНДІАВІАПРОМ"; УмЖ, 2021.

2. Analyzing 2FA Phishing Attacks and Their Prevention Techniques – Режим доступу: https://ieeexplore.ieee.org/document/9945766.

3. Russell, Steve (2023-02-22). "Bypassing Multi-Factor Authentication". ITNOW. 65: 42–45. doi:10.1093/combul/bwad023. ISSN 1746-5702. – Режим доступу: https://academic.oup.com/itnow/article-abstract/65/1/42/7051213.

АНАЛІЗ ВИКОРИСТАННЯ SIEM СИСТЕМ У СУЧАСНИХ УМОВАХ

Мартиненко Я.А., Сєвєрінов О.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Атаки на інформаційні системи стають все більш розповсюджені на сьогоднішній день, і як наслідок це приносить великі збитки для компаній. Щоб обмежити їх, однією з найважливіших стратегій безпеки для запобігання та протидії атакам є виявлення та реагування на інциденти безпеки в режимі реального часу [1].

Згідно зі звітом NIST [2], рішення з кібербезпеки в промислових системах управління повинні забезпечувати виявлення поведінкових аномалій в режимі реального часу, швидке управління інцидентами та інтелектуальну візуалізацію мережі та всіх її взаємопов'язаних вузлів. Ці питання можуть забезпечити SIEM системи (Security information and event management). Тож SIEM системи розглядають вищезгадані можливості як вбудовані функції.

У сучасному комерційному світі рішення для забезпечення безпеки повинні бути сумісними з хмарними технологіями. Тому імплементація SIEM систем у хмарне середовище забезпечить більшу ефективність виявлення загроз безпеці інформації в організаціях, а також зможе підвищити швидкість реагування на інциденти, що в свою чергу сприятиме зменшенню ризику для бізнесу і забезпечить збереження даних та інфраструктури в безпеці.

Метою доповіді є аналіз використання SIEM систем для виявлення інциденти безпеки у сучасних умовах.

В доповіді розглядаються результати досліджень найзатребуваних SIEM систем [3]. Описується система Splunk [4], її переваги та недоліки в порівнянні з іншими SIEM системами.

Розробка концепції розгортання SIEM систем у хмарному середовищі з вибором моделі хмарних обчислень для забезпечення має надзвичайно велике значення для захисту даних в компаніях.

Така імплементація може забезпечити ряд переваг: гнучкість, еластичність, економію ресурсів.

Список літератури

1. Ушатов В., Сєвєрінов О. В. "Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки." (2019).
2. NIST Recommendations For IoT & ICS Security. Malware Analysis, News and Indicators. URL: https://malware.news/t/nist-recommendations-for-iot-ics-security/32231 (дата звернення:31.03.2024).
3. Овчаренко М.Ю, Сєвєрінов О.В. Аналіз сучасних систем управління інформаційною безпекою та інцидентами безпеки // Проблеми інформатизації: сьома міжнародна науково-технічна конференція: Міжнар. науково-техн. конф. Харків. С. 12.
4. Splunk | The Key to Enterprise Resilience. URL: https://www.splunk.com/en_us/pdfs/resources/e-book/the-siem-buyers-guide-2023.pdf.

АНАЛІЗ МЕТОДІВ ДЕТЕКТУВАННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Сєвєрінов О.В., Федоров І.А., Власов А.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Шкідливе програмне забезпечення (ПЗ) постійно розвивається та стає все більш вдосконалим, адаптуючись до сучасних методів детектування. Шкідливе ПЗ перешкоджає нормальному використанню кінцевих пристроїв. Коли пристрій заражений шкідливим програмним забезпеченням, можна зіткнутися з несанкціонованим доступом, компрометацією даних або блокуванням і вимогою заплатити викуп [1].

Виявлення зловмисного ПЗ передбачає використання методів і інструментів для виявлення, блокування, попередження та реагування на загрози. Основні методи виявлення зловмисного програмного забезпечують ідентифікацію та обмеження відомих загроз та включають виявлення на основі сигнатур, контрольних сум та білого списку програм [2]. До методів виявлення можна віднести використання репутаційної системи, яка містить інформацію про загрози в реальному середовищі.

Метою роботи є аналіз методів детектування шкідливого програмного забезпечення.

В роботі розглядаються основні методів детектування шкідливого ПЗ. Показано, що передовим є метод виявлення за допомогою штучного інтелекту. При цьому детектування та захист від шкідливого ПЗ вимагає комплексного підходу та використання декількох різноманітних методів.

Розглянуті методи ухилення від детектування шкідливого ПЗ. Щоб ухилитися від детектування, зловмисники використовують техніки обфускації коду, шифрування, виконання коду в пам'яті та інші методи, щоб уникнути виявлення антивірусними програмами та системами виявлення вторгнень.

Приводяться сучасні методи захисту від шкідливого програмного забезпечення.

Для успішного захисту важливо мати в організації команду SOC аналітиків [3], які будуть вчасно реагувати на загрози, оновлювати та патчити програмне забезпечення, використовувати стабільні версії оновлень, втілювати план реагування на інциденти інформаційної безпеки.

Список літератури

1. Сєвєрінов О.В., Хрєнов А.Г., Поляков А.О. Аналіз сучасних методів атак на автоматизовані системи управління військами та інформаційні мережі // Системи обробки інформації, 9 (2015): 101-104.

2. Martovytskyi Vitalii et al. Method for Detecting FDI Attacks on Intelligent Power Networks // International Scientific-Practical Conference "Information Technology for Education, Science and Technics". Cham: Springer Nature Switzerland, 2022, pp. 715-731.

3. Sievierinov O., Ovcharenko M., Vlasov A. Enterprise Security Operations Center // Computer and information systems and technologies (2021).

АКТИВНИЙ ЗАХИСТ ВІД ЛАЗЕРНИХ ЗАСОБІВ АКУСТИЧНОЇ РОЗВІДКИ

Довгаль В.С., Заболотний В.І.
Харківський національний університет радіоелектроніки, Харків, Україна

Існує актуальний технічний канал витоку інформації (ТКВІ), що утворюється шляхом дистанційного зняття лазерними засобами акустичної розвідки (ЛЗАР) вібраційних коливань поверхонь у виділених приміщеннях, інженерних або будівельних комунікацій, предметів інтер'єру, що спричинені акустичним полем (небезпечного мовного сигналу).

Віддзеркалений промінь лазеру модулюється вібраційними коливаннями і може переносити інформацію, що озвучується у виділеному приміщенні далеко за межі контрольованої зони.

Застосування ЛЗАР є складною технічною задачею. Що обумовлено їх складністю, як оптико-електронного пристрою [1], якій потрібно ретельно налаштовувати при його використанні.

Тим не менше, ЛЗАР є небезпечним пристроєм розвідки, що створює небезпечний ТКВІ.

Запобігання витоку інформації для ЛЗАР може досягатися такими способами [2]:

- використання вакуумних та інших захищених вікон;
- матування в вікнах зовнішньої поверхні скла;
- створення на шибках вікон та інших предметів відзеркалення вібраційного зашумлення, що маскує небезпечні сигнали;
- використання зовнішніх ролетів, ставень на вікнах.

З прийнятих на тепер способів захисту від ЛЗАР витікає, наряду з їх достоїнствами, і деякі недоліки, що дає підґрунтя на їх подальше покращання.

Метою доповіді обґрунтуванням можливостей захисту за рахунок застосування активних перешкод для проміня лазеру в діапазоні його робочої хвилі.

В доповіді наводяться обґрунтування особливих умов та обмежень на застосування запропонованого способу захисту від ЛЗАР.

Наведені дані визначають особливість запропонованого способу створення активних перешкод у створення перевипромінювання бокових пелюсток лазерного проміня в зворотному напрямку за рахунок використання оптичних відбивачів променя лазеру та режиму їх використання.

Список літератури

1. Сєлюков О.В., Хлапонін Ю.І. Принципи побудови датчика лазерного опромінювання. Київський національний університет будівництва і архітектури, Київ Телекомунікаційні та інформаційні технології. 2020. № 1 (66). С. 197 – 204.

2. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник / Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. - К.: ІСЗЗІ НТУУ «КПІ», 2016. - 104 с.

ЗАСОБИ ВТІЛЕННЯ ПРИВАТНИХ БЛОКЧЕЙН-РОЛАПІВ ДЛЯ ФІНАНСОВИХ ОРГАНІЗАЦІЙ

Гаража Р.Ю., Мельникова О.А.
Харківський національний університет радіоелектроніки, Харків, Україна

Децентралізовані облікові системи на базі блокчейну стали потужним засобом забезпечення таких факторів інформаційної безпеки як цілісність та доступність.

З іншого боку, публічність даних і відсутність можливостей щодо регулювання дій користувачів у цих системах є перешкодою на шляху повсюдного їх застосування, зокрема у банківській сфері.

Метою доповіді є ідентифікація та аналіз засобів, здатних забезпечити в обліковій системі на базі блокчейну приватність та регуляторні можливості. **В доповіді** наводяться описи таких засобів та пропозиції щодо їх застосування.

На сьогоднішній день вже знайшла своє активне застосування технологія блокчейн-ролапів, що являють собою надбудову над системами першого рівня [1]. Метою ролапів є масштабування цих систем та зменшення комісій за транзакції. Для перевірки коректності обчислень, проведених в ролапах, використовуються докази із нульовим розголошенням, заради ще більшої оптимізації обчислень. Дані, що передаються у складі доказу, залишаються приватними.

Доказ повинен доводити, що обчислення в ролапі виконувалися згідно певних правил, визначених за допомогою контуру (англ. circuit). Контури описуються за допомогою спеціалізованих мов програмування, таких як Circom [2]. Зазвичай контур дублює правила першого рівня, але можливо визначити додаткові правила щодо допустимих дій користувачів у системі другого рівня (білий список користувачів, обмеження на розмір переказів, тощо). Оптимізувати доказ входження до списку можна за допомогою дерев Меркла, що є зручною для доказів із нульовим розголошенням структурою даних [3]. Крім того, саму систему можна зробити такою, що вимагає підтвердження особистості для доступу, як і звичайні банківські послуги.

Таким чином, стає можливим додати до переліку послуг безпеки децентралізованих облікових систем приватність користувацьких даних, а також регулювання дій користувача, важливе для фінансових організацій.

Список літератури

1. Rollup. URL: https://www.techopedia.com/definition/rollup (дата звернення: 29.03.2024).

2. Circom. URL: https://docs.circom.io/ (дата звернення: 29.03.2024).

3. Мельникова О. А., Гаража Р. Ю. Докази із нульовими знаннями на базі дерев Меркла [Текст] // Тринадцята міжнародна науково-технічна конференція «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління»: Зб. матеріалів конференції. Т.1: секції 1, 3, 4. — Харків: ХНУРЕ, НТУ “ХПІ”, НАУ “ХАІ”, УмЖ, НУО АР, 2023. — С. 66.

АНАЛІЗ ОБЧИСЛЮВАЛЬНОЇ СКЛАДНОСТІ ВАРІАНТІВ ПЕРЕДПІДПИСІВ ЗА СТАНДАРТАМИ ЦП В ГРУПАХ ТОЧОК ЕК

Мельникова О.А., Польовий О.А.
Харківський національний університет радіоелектроніки, Харків, Україна

Алгоритми ЦП (цифрового підпису) мають функціонувати в режимі реального часу. Передпідписи зменшують обчислювальну складність формування ЦП. Наразі велика кількість діючих КСЗІ (криптографічних систем захисту інформації) використовує стандарти ЦП в групах точок еліптичних кривих (ЕК) [1, 2], що модифікуються із урахуванням сучасних викликів. Так, до оновленого стандарту [1] додано ЕК Едвардса, що передбачалося досить давно [3].

Метою доповіді є аналіз можливостей зменшення обчислювальної складності формування ЦП за рахунок передпідписів із урахуванням особливостей різних стандартів. **В доповіді** також розглянуто зменшення обчислювальної складності формування передпідписів при надвеликому їх обсязі за рахунок методів скалярного множення, які одноразово формують великі таблиці передобчислень при використанні незмінної (базової) точки. Наприклад [4], методів Брікела, варіантів comb-методів із різною кількістю таблиць (методи Ліма-Лі), тощо. Порівняння формування ЦП за стандартами [1, 2] показує, що варіант [1] дозволяє розширити попередні обчислення. Пропонується розширений варіант передпідписів: $\{k_i^{-1} \bmod n, r_i, d \cdot r_i \bmod n\}$ замість рекомендованого в стандарті $\{k_i^{-1} \bmod n, r_i\}$. Нажаль, для [2] можливе використання єдиного варіанту передпідписів: $\{k_i, x_i\}$.

Порівняння оцінок обчислювальної складності етапів передпідпису та швидкого формування ЦП в режимі реального часу показав, що при розширеному варіанті передпідпису обчислювальна складність передобчислень для [1] більша, ніж для [2]. Але етап ЦП для [1] стає швидшим, принаймні на одне множення за модулем елементів поля GF(2^m).

Список літератури

1. National Institute of Standards and Technology (2023) Digital Signature Standard (DSS). (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 186-5. DOI: https://doi.org/10.6028/NIST.FIPS.186-5

2. ДСТУ 4145 – 2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. — Перше видання; Введ. 1.07.2003. — К.: Державний комітет України з питань технічного регулювання та споживчої політики, 2003 р. — 44 с.

3. Мельникова О. А., Джурик О. В., Маслєннікова А. О. Еліптичні криві Едвардса. Порівняння криптографічних бібліотек // Радіотехніка. — 2018. — №. 195. — С. 41 - 45. DOI: https://doi.org/10.30837/rt.2018.4.195.05

4. Hankerson D., López J. H., Menezes A. Software implementation of the NIST elliptic curves over binary fields // Proceedings of CHES 2000, LNCS 1965 (2000), 1–24. DOI: http://dx.doi.org/10.1007/3-540-44499-8_1

АНАЛІЗ ТИПІВ АВТЕНТИФІКАЦІЇ ТА АВТОРИЗАЦІЇ СУЧАСНИХ WEB-ЗАСТОСУНКІВ

Ткачук І.К., Сєвєрінов О.В.
Харківський національний університет радіотехніки, Харків, Україна

Швидкий розвиток інформаційних технологій та поширення web-застосунків у різних сферах життя вимагає підвищувати їх інформаційну безпеку, одним з основних факторів якої є методи автентифікації та авторизації.

Недоліки в системах автентифікації та авторизації можуть призвести до серйозних проблем, включаючи втрату даних, порушення конфіденційності та витрати на відновлення [1]. Щоб забезпечити найвищий рівень безпеки веб-додатків використовуються різні методи захисту, що включають такі як: багаторівнева автентифікація, JWT [2], OAuth [3], TLS/SSL, RBAC [4].

Метою доповіді є аналіз різних типів автентифікації та авторизації веб-застосунків з метою виявлення їхніх переваг, недоліків та відповідності конкретним вимогам безпеки. Аналіз дозволяє визначити, які методи захисту найбільш ефективні для конкретних сценаріїв використання, найважливіші вимоги до безпеки веб-застосунків, а також які ризики пов'язані з різними підходами до автентифікації та авторизації.

Аналіз різних типів автентифікації та авторизації веб-додатків проводився в контексті використання власною реалізацією інформаційної системи. На основі аналізу формулюються рекомендації щодо вибору та впровадження ефективних методів автентифікації та авторизації для забезпечення оптимального рівня безпеки та функціональності веб- застосунків у інформаційній системі.

Також однією з сучасних тенденцій є використання механізмів безпеки, в тому числі і автентифікації, провідних хмарних провайдерів, таких як Amazon, IBM, Google, Microsoft та інших. Використовуються методи багатофакторної автентифікації, що вимагають надання принаймні двох форм облікових даних. Це надає додатковий рівень безпеки. Для розгляду сервісів автентифікації та авторизації було обране рішення від AWS (Amazon Web Servises) EC2 (Elastic Compute Cloud), що є пропонує найширшу обчислювальну платформу з надійними механізмами безпеки.

Список літератури

1. Сєвєрінов О.В., Кліпоносова В.С. Автентифікації користувачів веб-ресурсів. НТУ «ХПІ», 2022.
2. Understanding JWT". Atlassian Connect Documentation. URL: https://web.archive.org/web/20150518082002/https://developer.atlassian.com/static/connect/docs/latest/concepts/understanding-jwt.html
3. Sievierinov O., Kholosha O. Securing Bearer token in OAuth2.0 // COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES, 2021.
4. Jin X., Krishnan R., Sandhu R. S. A unified attribute-based access control model covering DAC, MAC and RBAC // LNCS. − 2012. V. 7371. − P. 41-55.

БАГАТОАЛЬТЕРНАТИВНЕ ВИЯВЛЕННЯ ЗАДАНИХ РАДІОВИПРОМІНЮВАНЬ

Голобородько Ю.М., Наконечний М.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Для підвищення надійності та безпеки, а саме скритності радіозв'язку необхідно здійснювати оперативний радіоконтроль завантаження декаметрового діапазону радіочастот.

З цією метою слід з усієї множини радіовипромінювань (РВ) виділити задані [1, 2].

У декаметровому діапазоні хвиль існує безліч РВ, що відрізняються: частотою; розміщенням джерела в просторі (у ближній зоні - зоні поверхневого поширення електромагнітної хвилі і в дальній - зоні просторового поширення електромагнітної хвилі); видом радіовипромінювання (вид модуляції та маніпуляції, параметри модулюючого сигналу тощо); рівнем сигналу; часом появи; тривалістю.

У ряді випадків радіоконтролю діапазону представляють оперативний інтерес РВ, для яких апріорі відомі: вид радіовипромінювання; зона розміщення джерела радіовипромінювання (ближня); смуги діапазону або номінали частот, на яких задані радіовипромінювання не можуть з'явитися.

За умовами завдання багатоальтернативне виявлення заданих РВ повинно проводитись в умовах підвищеної апріорної невизначеності. Зокрема, статистичні характеристики сигналів апріорі невідомі.

Однак можуть бути отримані навчальні вибірки сигналів для заданих РВ. Для інших (невідомих, тих, які заважають) РВ навчальні вибірки неможливо знайти, або вони є представницькими, тобто недостатніми для синтезу алгоритмів обробки [3, 4].

У доповіді розглядається питання багатоальтернативного виявлення заданих РВ в умовах підвищеної апріорної невизначеності для забезпечення надійності та скритності систем передачі.

Список літератури

1. Lazarov, Lazar. "Perspectives and trends for the development of electronic warfare systems." 2019 International Conference on Creative Business for Smart and Sustainable Growth (CREBUS). IEEE, 2019.

2. Крючкова Л.П., Котенко А.М., Пшоннік В.О. "Оцінка ефективності маскування сигналів в каналах радіозв'язку." Сучасний захист інформації 2 (2018): 93-98.

3. Голобородько Ю.М. Синтез систем пошуку та багатоальтернативного виявлення заданих випадкових сигналів за сукупністю показників якості. Тези доповіді у книзі «Методи подання та обробки випадкових сигналів та полів», Харків, 1989.

4. Балабанов В.В., Безрук В.М., Голобородько Ю.М. Дослідження алгоритмів виявлення нових невідомих радіовипромінювань на тлі стаціонарної перешкоди. Збірник наукових праць ХВУ, випуск 5 (43), 2002.

БЕЗПЕКА ІНФОРМАЦІЇ ПРИ ВИКОРИСТАННІ МОБІЛЬНИХ ПРИСТРОЇВ В КОРПОРАТИВНИХ МЕРЕЖАХ

Сидоренко З.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Останнім часом все більше в інформаційних системах організацій використовується підхід BYOD (Bring your own device), який забезпечує зручність та гнучкість роботи персоналу. На противагу цьому, залежність від персональних пристроїв створює небезпеку для корпоративних даних, особливо під час можливих атак кіберзлочинців [1]. При експлуатації мобільних абонентських пристроїв в корпоративних мережах існує низка особливостей, що істотно впливають на безпеку інформації в цих системах. Це невеликі розміри абонентських пристроїв, мобільність користувачів, мультифункціональність пристроїв, можливість доступу до послуг корпоративної мережі із різними вимогами щодо захищеності. Вказані особливості збільшують ймовірність здійснення загроз інформаційній безпеці та потребують їх врахуванню при побудові системи безпеки [1]. Мобільність користувачів висуває особливі вимоги до контролю за корпоративною мережею з боку служби безпеки – контролювати потрібно не лише інфраструктуру, а й бездротові клієнтські пристрої.

Однією з завдань, що впливають на безпеку інформації, а також здійснення аудиту безпеки в корпоративних мережах є оцінка ефективності захисту інформації при експлуатації мобільних пристроїв. Існують різні методики оцінки ефективності інформаційної безпеки, в ході яких проводиться збір інформації та розрахунок показників TCO, BCP та ROI організації. Аналіз зібраних показників дозволяє оцінити та порівняти стан захищеності інформаційної системи організації з типовим профілем захисту. Але дані методики як правило не враховують особливості експлуатації мобільних абонентських пристроїв в корпоративних мережах.

Метою доповіді є аналіз факторів, що впливають на безпеку інформації при використанні мобільних пристроїв в корпоративних мережах, розгляд існуючих методів оцінки ефективності захисту інформації та пропозиції по розробці методики оцінки ефективності захисту при експлуатації мобільних пристроїв, що враховує їх особливості та забезпечить комплексний захист корпоративних даних від найскладніших загроз, навіть у випадку втрати пристрою [2,3].

Список літератури

1. Нечволод К.В., Сєвєрінов О.В., Власов А.В. Аналіз безпеки даних в ЕММ системах / Системи управління, навігації та зв'язку. 3.55 (2019): 131-134.

2. Сердюков Д.В., Сєвєрінов О.В., Сидоренко З.М. Безпечне підключення мобільних пристроїв до корпоративної мережі з використанням тунелю VPN. Сучасні напрями розвитку інф.-ком. технологій та засобів управління. – Том 1, 70 (2023).

3. Serdiukov D., Sievierinov O., Sydorenko Z. Особливості розгортання застосунку ESET MDM/MDC для забезпечення безпеки мобільних пристроїв // Системи управління, навігації та зв'язку. Збірник наукових праць 4.74 (2023): 102-105.

ТЕСТУВАННЯ ГЕНЕРАТОРІВ ВИПАДКОВИХ ТА ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

Гріненко Т.О., Волобуєв К.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Генератори випадкових та псевдовипадкових послідовностей (ГВП (ГПВП)) мають широкий спектр застосування, в тому числі і в криптології. Від якості генератора залежить якість криптографічної системи в цілому. Для всебічного та об'єктивного дослідження якості ГВП (ГПВП) необхідно застосовувати відразу безліч різних тестів [1, 2]. Визначення необхідного та достатнього набору тестів представляє поки що невирішене завдання і є актуальним.

Метою доповіді є аналіз існуючих підходів до визначення випадковості послідовності; порівняльний аналіз та обґрунтування наборів тестів та методик тестування генераторів випадкових та псевдовипадкових послідовностей.

Так чи інакше, всі методики тестування базуються на порівнянні властивостей генерованих послідовностей з властивостями істинно еталонної випадкової послідовності. За характером оцінювання та подання тести, що використовуються для дослідження властивостей послідовностей, можна розділити на два основні типи: статистичні тести та графічні тести.

Найбільш поширеними на сьогодні є такі методики тестування: серія стандартів FIPS-140, що спрямовані на розв'язання задачі статистичного контролю використовуваних у криптографічних модулях ВП (ПВП); AIS 20; AIS 31; набір статистичних тестів DIEHARD; набір тестів та методика проведення статистичного тестування ГВП (ГПВП) NIST STS [1]; DIEHARDER, що включає в себе оновлені та стилізовані тести DIEHARD, тести NIST STS та нові тести, що розроблені Робертом Г. Браун [3].

В умовах постійної появи нових та вдосконалення існуючих засобів тестування ВП (ПВП) необхідно обґрунтувати та розробити базовий варіант методики перевірки якості послідовностей, надійний, швидкий, доступний та загальноприйнятий. Слід також зауважити, що будь-які окремі тести можуть давати помилкові результати для конкретного генератора, але в добре підібраному наборі тести доповнюють один одного і взаємно компенсують властиві їм недоліки.

Список літератури

1. Гріненко Т.О., Горбенко І.Д. Методики та засоби тестування послідовностей випадкових чисел та особливості їх застосування. Прикладна радіоелектроніка. Науково-техн. журнал. Харків. 2006. Том 5, №1. С. 115-126.

2. Євєрінов О.В. Аналіз методів побудови генераторів псевдовипадкових послідовностей / Системи обробки інформації, 8 (2013): 198-201.

3. Robert G. Brown. DieHarder: A Gnu Public License Random Number Tester. Duke University Physics Department, Durham, NC 27708-0305. Mode of access: https://rurban.github.io/dieharder/manual/dieharder.pdf (date of access: 30.03.2024).

БЕЗПЕКА ПРОТОКОЛІВ VPN

Гріненко Т.О., Бельмаз Б.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Протоколи VPN – це спеціальні правила, що визначають порядок роботи віртуальної приватної мережі VPN. Вони відповідають за процеси автентифікації пристроїв, способи передачі даних, безпеку алгоритмів, що використовуються, і приватність з'єднання. VPN-протокол складається з тунелювання та шифрування.

Протокол тунелювання створює з'єднання між пристроєм користувача і VPN-сервером, а протокол шифрування забезпечує конфіденційність [1, 2].

Метою доповіді є аналіз та обґрунтування методів побудови VPN-з'єднання, що дозволять покращити безпеку інформації, яка передається через локальну мережу. В доповіді наведені результати порівняльного аналізу протоколів VPN, надані та обґрунтовані рекомендації щодо використання протоколів канального, мережевого та сеансового рівнів для побудови захищених віртуальних каналів зв'язку.

Для незалежності від прикладних протоколів та додатків захищені віртуальні мережі формуються на одному з нижчих рівнів моделі OSI – канальному, мережевому чи сеансовому. Канальному (другому) рівню відповідають такі протоколи реалізації VPN, як PPTP, L2F, L2TP; мережевому (третьому) рівню – IPSec, SKIP; сеансовому (п'ятому) рівню – SSL/TLS та SOCKS [1, 3].

Чим нижчий рівень еталонної моделі, на якому реалізується захист, тим він є прозорішим для додатків і непомітнішим для користувача. Але при зниженні цього рівня зменшується набір послуг безпеки, що реалізуються, і стає складніше організація управління. Чим вище рівень захисту, тим ширше набір послуг безпеки, надійніший контроль доступу і простіше конфігурування системи захисту, але в цьому випадку посилюється залежність від протоколів обміну та додатків, що використовуються. Протокол сеансового рівня SSL/TLS створює захищений тунель між кінцевими точками віртуальної мережі, забезпечуючи взаємну автентифікацію абонентів, а також конфіденційність, справжність та цілісність даних, що циркулюють по тунелю. На відміну від віртуальних мереж, захищених на сеансовому рівні, віртуальні мережі на канальному або мережевому рівнях зазвичай просто відкривають або закривають канал для всього трафіку, що передається автентифікованим тунелем.

Список літератури

1. Jeff Tyson, Chris Pollette, Stephanie Crawford. How a VPN (Virtual Private Network) Works. Mode of access: https://computer.howstuffworks.com/vpn.htm (date of access: 25.03.2024).

2. Сердюков Д.В., Сєвєрінов О.В., Сидоренко З.М. Безпечне підключення мобільних пристроїв до корпоративної мережі з використанням тунелю VPN, 2023.

3. Комп'ютерні мережі: [навчальний посібник] / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. – Львів: «Магнолія 2006», 2013. – 256 с.

КЛАСИФІКАЦІЯ МЕХАНІЗМІВ ЗАХИСТУ ВІД АТАК ТИПУ DDOS

Топіха Т.Б., В'юхін Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

В сучасних умовах організації все більше використовують розподілені інформаційні мережі. Проведений аналіз показав, що в таких мережах одними з найбільш опасних для безпеки інформації є DDoS атаки [1, 2].

Метою доповіді є розгляд системи класифікації механізмів захисту від DDoS атак відповідно до різних критеріїв. Система класифікує механізми захисту від DDoS залежно від розгорнутої активності. Запобігання вторгненням. Найкращою стратегією захисту від будь-якої атаки є та, за якої вона атака ніколи не відбудеться. Існує безліч механізмів захисту від DDoS механізмів, які намагаються вберегти системи від атак зловмисників [3]:

– використання глобально узгоджених фільтрів;

– вимкнення невикористовуваних служб. Якщо мережеві служби не використовуються, їх слід вимкнути для запобігання атакам;

– застосування виправлень безпеки. Хост-комп'ютери повинні оновлюватися останніми виправленнями безпеки для усунення наявних помилок і використовувати останні доступні методи щоб мінімізувати ефект від DDoS-атак;

– зміна IP-адреси. Рішення, практичне тільки для локальних DDoS-атак, називається "захист від рухомої цілі", за якого ми анулюємо IP-адресу комп'ютера-жертви, змінивши її на нову. Щойно адресу IP буде змінено, прикордонні маршрутизатори відкидають атакуючі пакети;

– вимкнення IP-трансляцій хост-комп'ютери більше не можуть використовуватися як підсилювачі в ICMP Flood і Smurf-атаках;

– створення "вузьких місць" для клієнтів. Ці засоби намагаються створити вузькі місця на комп'ютерах Zombie і обмежити їхню здатність до атаки. Алгоритм RSA "Загадки клієнта" і тест Тюрінга вимагають від клієнта додаткових обчислень перед встановленням з'єднання [4].

Виявлення та захист від DDoS-атак є ключовими аспектами забезпечення безпеки мережевої інфраструктури.. Негайна реакція після виявлення атаки, включаючи визначення джерела та блокування трафіку, є критичною.

Список літератури

1. Сєвєрінов О.В., Хрєнов А.Г., Поляков А.О. Аналіз сучасних методів атак на автоматизовані системи управління військами та інформаційні мережі // Системи обробки інформації 9 (2015): 101-104.

2. Сєвєрінов О.В., Шевцов В.О., Сокол-Кутиловська А.С. Аналіз сучасних методів атак на електронні ресурси органів управління // Системи озброєння і військова техніка 1 (2017): 65-68.

3. Implementing Pushback: Router-Based Defense Against DDoS Attacks. Department of Computer Science, Columbia University. URL: https://www.cs.columbia.edu/~smb/papers/pushback-impl.pdf (date of access: 24.02.2024).

4. S. M. Bellavin. ICMP traceback messages. Internet Draft, 2001

СТВОРЕННЯ БЕЗПЕЧНИХ ЛОКАЛЬНИХ МЕРЕЖ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

Тяптя А.В., В'юхін Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Аналіз сучасних загроз в локальних інформаційних системах показав, що їх кількість постійно зростає [1]. Тому виникає необхідність розгляду основних методів безпеки інформації в даних мережах.

Метою доповіді є розробка рекомендації щодо створення безпечної локальної мережі організації.

Локальна мережа (LAN) - це група комп'ютерів, принтерів та інших пристроїв, які з'єднані між собою в одному місці, наприклад, вдома або в офісі. Створення безпечної локальної мережі - це важливий крок для захисту ваших даних та пристроїв від кіберзагроз. Використання нижчеописаних технологій кібербезпеки допоможе вам створити безпечну локальну мережу, яка буде захищена від несанкціонованого доступу, атак та збоїв [2].

Технології кібербезпеки для локальних мереж:

1. Брандмауер - це перша лінія захисту локальної мережі [2]. Він блокує несанкціонований доступ ззовні та контролює трафік, який проходить через мережу.

2. Віртуальна приватна мережа (VPN) - шифрує дані, які передаються між пристроями в локальній мережі, роблячи їх нечитаними для сторонніх осіб.

3. Антивірусне програмне забезпечення: Антивірусне програмне забезпечення захищає комп'ютери в локальній мережі від вірусів, шпигунських програм та інших шкідливих програм [2].

4. Контроль доступу - дозволяє адміністратору мережі управляти тим, хто має доступ до певних ресурсів в локальній мережі.

Рекомендації щодо створення безпечної локальної мережі:

1. Використовуйте стійкий пароль для вашого маршрутизатора (бажано від 14 символів).

2. Увімкніть брандмауер на вашому маршрутизаторі та налаштувати його на вашій ОС (якщо вона це передбачає).

3. Використовуйте VPN для шифрування даних, які передаються між пристроями в локальній мережі.

4. Встановіть антивірусне програмне забезпечення на всі комп'ютери в локальній мережі.

Список літератури

1. Голубничий Д.Ю. et al. Аналіз сучасних загроз в інформаційних системах за складовими загроз: кібербезпеки, інформаційної безпеки та безпеки інформації,.2021.

2. Хорхе Гранхал, Едмундо Монтейру, Хорхе Са Сілва. Безпека для Інтернет речей: огляд існуючих протоколів і відкритих досліджень. Кібербезпека. Липень 2015. № 1. С. 1294–1312.

ПОКРАЩЕННЯ РЕАЛІЗАЦІЇ СТАНДАРТУ БЕЗПЕКИ WPA3

Хая А.О., В'юхін Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні бездротові Wi-Fi мережі стали невід'ємною частиною повсякденного життя. При цьому захист даних, які передаються через Wi-Fi, є надзвичайно важливим, оскільки існує загроза злому з будь-якого місця, де має місце з'єднання [1, 2]. Стандарт WPA3 Wi-Fi пропонує нові функції та покращені механізми шифрування, що робить вторгнення у мережі складнішими для зловмисників. Він є важливим кроком у забезпеченні безпеки Wi-Fi і відображає постійний розвиток стандартів безпеки.

Метою доповіді є аналіз основних покращень безпеки у WPA3 [3]:

1. Індивідуальне шифрування. Використовується протокол Simultaneous Authentication of Equals (SAE), що дозволяє кожному пристрою в мережі створювати унікальний ключ шифрування під час підключення.

2. Захист від атак "перехоплення пакетів". Протокол безпеки для бездротових мереж включає механізми, що запобігають атакам, спрямованим на перехоплення та декодування передаваних даних.

3. Покращена конфіденційність. WPA3 використовує захищені канали для забезпечення конфіденційності даних, які передаються між пристроями у мережі, що робить його більш надійним для використання в чутливих сферах.

4. Захист від перебору паролів. Протокол має механізми, що ускладнюють атаки на перебір паролів, що робить його більш ефективним у запобіганні несанкціонованому доступу до мережі.

5. Сумісність з попередніми версіями та масове впровадження.

Реалізація стандарту на рівні програмного забезпечення є критичною для безпеки мережі, оскільки саме програмне забезпечення визначає конкретні параметри і функції, які використовуються в процесі автентифікації, шифрування та управління ключами. Якщо ці реалізації не досягають високого рівня безпеки, то мережа стає вразливою перед різноманітними атаками, як перехоплення трафіку, атаки на паролі або впровадження шкідливого коду. Аналіз потенційних вразливостей, які можуть виникнути через недоліки у реалізації WPA3, виявляє різноманітні загрози. Провідні компанії в галузі мережевих технологій можуть створювати ініціативи з тестування безпеки та сертифікації пристроїв, що використовують стандарт WPA3. Це дозволить споживачам мати більшу впевненість у безпеці та надійності обладнання, яке вони використовують у своїх мережах.

Список літератури

1. Єфремов Н.С. Дослідження засобів безпеки безпроводових мереж. Н. С. Єфремов; М-во освіти і науки України, ХНУРЕ. – Харків, 2024. – 75 с.

2. Северинов А.В., Черныш В.И. Анализ угроз и рисков безопасности информации в беспроводных сетях // Системи управління, навігації та зв'язку. – Вип 1: 229-232.

3. TheFastCode. Що таке WPA3 і коли я отримаю його на своєму Wi-Fi? 2023. URL: https://www.thefastcode.com/uk-uah/article/what-is-wpa3-and-when-will-i-get-it-on-my-wi-fi.

МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЙНИХ ДАНИХ КОРИСТУВАЧІВ В СФЕРІ VOICE OVER IP

Черкашинов Т.К., В'юхін Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Voice over IP (VoIP) - це технологія, яка дозволяє здійснювати телефонні дзвінки через Інтернет. VoIP може бути більш економічно вигідним та зручним, порівняно з традиційними телефонними лініями, але також може бути більш вразливим до атак [1].

Метою доповіді є аналіз методів захисту інформаційних даних користувачів при використанні технології VoIP.

Методи захисту інформаційних даних користувачів в VoIP:

1. Шифрування даних робить їх нечитаними для зловмисників, які можуть перехопити їх.

2. Автентифікація та авторизація дозволяють перевірити, чи є користувачами ті, ким вони себе видають, і чи мають вони доступ до певних ресурсів.

3. Контроль доступу дозволяє адміністраторам VoIP-системи control who can access what resources on the network.

4. DoS-атаки можуть перешкодити роботі VoIP-системи. Існують різні методи захисту від DoS-атак, такі як брандмауери та системи виявлення вторгнень.

Фізична безпека VoIP-обладнання також є важливою для захисту даних користувачів [2].

В роботі запропоновані рекомендації щодо захисту інформаційних даних користувачів в VoIP:

– використання надійних паролів та зберігання їх у таємниці;

– заборона використання загальнодоступних Wi-Fi мереж для підключення до VoIP-системи;

– встановлення на особисті пристрої антивірусного програмного забезпечення та програмного забезпечення брандмауера;.

– оновлення програмного забезпечення VoIP-системи до останньої версії;

– необхідність звертання уваги на підозрілу активність.

Захист інформаційних даних користувачів в сфері VoIP - це важливе завдання, яке потребує комплексного підходу. Використання вищезазначених методів допоможе вам захистити ваші дані від атак.

Список літератури

1. Saburova, S.A.; Gmati Abdulbari; Kadatskaja, O.I. Methods Of Control Quality Of Services *VoIP* Over LTE. 2021

2. S.M. Bellavin. ICMP traceback messages. Internet Draft, 2001.

ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ БЕЗПЕКИ ЗВ'ЯЗКУ 5G

Чибізов І.О., В'юхін Д.О.
Харківський Національний університет радіоелектроніки, Харків, Україна

5G - це п'яте покоління мобільного зв'язку, яке пропонує значно більшу швидкість, пропускну здатність та надійність, порівняно з 4G. Зростаюче використання 5G у різних галузях, таких як Інтернет речей (IoT), автономні транспортні засоби та телемедицина, робить питання безпеки зв'язку 5G надзвичайно важливим [1].

Метою доповіді є аналіз особливості функціонування безпеки мобільного зв'язку 5G.

Основні характеристики безпеки 5G визначаються рядом факторів:

1. Автентифікація та авторизація: 5G використовує більш досконалі протоколи автентифікації та авторизації, такі як EAP-TLS та 5G AKA, щоб гарантувати, що лише авторизовані користувачі та пристрої мають доступ до мережі [2].
2. Ізоляція мережі: 5G використовує віртуалізацію мережі та програмно-визначені мережі (SDN) для створення віртуальних сегментів мережі, що ізолюють один від одного [3]. Це допомагає запобігти поширенню атак та мінімізувати їх вплив.
3. Захист від DDoS-атак: 5G використовує вдосконалені методи захисту від DDoS-атак, такі як фільтрація трафіку та динамічне масштабування мережі.
4. Конфіденційність абонентів: 5G включає в себе функції, які захищають конфіденційність абонентів, такі як анонімні ідентифікатори та контроль доступу до даних [1].

5G пропонує значні переваги в порівнянні з 4G, але також має нові виклики безпеки.

Завдяки вдосконаленим методам захисту 5G може забезпечити безпечний зв'язок для мобільних пристроїв, критичної інфраструктури та інших сфер.

Проте важливо постійно вдосконалювати методи захисту та співпрацювати на міжнародному рівні, щоб гарантувати безпеку 5G.

Список літератури

1. 5G NR: технологія бездротового доступу нового покоління. Ерік Дальман, Стефан Парквалл, Йохан Скольд. Академ. вид.: 2020 р.. 548 с.
2. Sievierinov Oleksandr and Lesia Bilan. Analysis of Variations in Biometric Authentication Methods in Mobile Devices // COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES (2021).
3. Тимошенко, Д. В. Публікація: Вплив розвитку 5G технологій на майбутнє телекомунікаційного сектору 2023 р.

СЕКЦІЯ 5
СУЧАСНІ ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНІ СИСТЕМИ

Керівник секції: д.т.н., проф. О. О. Можаєв, ХНУВС, Харків
Секретар секції: PhD І. Ю. Петровська, НТУ «ХПІ», Харків

SOME ASPECTS OF THE APPLICATION OF THE GEOGRAPHIC ANALYSIS SYSTEM IN THE MILITARY FIELD

Hashimov E.G.
National Defense University; Azerbaijan Technical University, Baku, Azerbaijan

The analysis of modern wars, including the Second Karabakh War and the ongoing Russia-Ukraine war, shows that military operations mainly take place in dynamically changing conditions. Thus, the influence of geography on the implementation of military operations is very large. Therefore, in the stage of preparation for the operation, it is one of the most important issues to study the geography and relief conditions of the area (region) where the operation will be carried out and to analyze it in a timely manner. Geographical analysis of the area is needed for the most suitable placement of the offensive units, artillery and missile troops, material and technical support units and forces that will be felt in the area, as well as to study the future directions of movement. Detailed information about the territory, maps and other descriptions of the territory, organization and planning of military operations, calculation of coordinates, etc. very important for military affairs. Therefore, geospatial information always occupies an important place in military affairs [1-6]. The analysis of the geographical factors affecting the military operation is carried out by a close study and evaluation of the territory. A close study of the terrain and a correct assessment gives the commanders the opportunity to foresee all possible movements of the enemy.

In order to organize the battle and effectively manage the available forces and resources in its course, each commander must know where the enemy is, what he is doing and what he is preparing to do, as well as the characteristics of the terrain in the area of the upcoming combat operations. Observational data must be obtained in a timely manner and delivered to the commander in a timely manner. Anticipating these requirements is especially important in modern, highly maneuverable warfare.

Geospatial technologies, especially map and geographic information systems (GIS), are used in the military as well in Azerbaijan. Its fields of application, methods of use and technologies are known to many military specialists. Geospatial technologies is a generalized term that includes technologies of geodesy, cartography, photogrammetry, geographic information systems, and remote space exploration of the Earth [1,7-10].

The report discusses the application and benefits of the Geographical Analysis System (GAS) developed on the basis of Geographical Information Systems and successfully used in the Turkish Armed Forces.

The GAS software platform is a desktop 3D "Virtual Sphere" application running on a server-client architecture. GAS can be used online (server-connected) or offline (server-independent) and works on laptops, tablets, mobile phones as well as desktop computers. Thanks to the GAS Algorithm, GAS displays data very quickly and ensures immediate data exchange between all users. The GAS software platform allows users to perform various queries and analyses, and to create new data and modify existing data. Buffer zone analysis, profiling, determination of visible and dead zones, and threat area analysis are examples of the simplest geographic analyses. Users can perform accurate 2D and 3D distance, area and perimeter calculations on the site.

The GAS software platform has a modular structure and can be constantly improved since the source code is completely nationally developed. The intensive use of the software platform is of great importance in terms of ensuring the security of the defense and security forces and the data they use.

It is advisable to widely use the GAS software platform in creating a visual image of the operational field in units and formations, determining the depth of enemy defenses, obtaining an idea of the terrain shape, and studying the operational field in parts or in its entirety using satellite images and aerial photographs.

References

1. Geographic information systems for military purposes. Textbook./ Utekalko V.K. and others. Ed. G.P.Kobeleva. Minsk: VA RB, 2009, 244 p.

2. Hashimov, E.G. Application of relief digital model for combat operation planning / E.G. Hashimov, A.A. Bayramov, Y.A. Nasibov, R.R. Amanov // Baku: Military Knowledge, – 2015. № 4, – p. 63–69.

3. Bayramov, A. A. The detection of invisible objects on the terrain on the basis of GIS technology // A.A.Bayramov, E.G.Hashimov, R.R.Amanov/ -Baku:Geography and nature sources. – 2016, № 1. – p. 124-126.

4. Bayramov, A.A. Seismic location station for detection of unobserved moving military machineries // A.A. Bayramov, E.G .Hashimov / Journal of Management and Information Science, Turkey, 2016, vol.4, № 2, p. 61-66. DOI: https://doi.org/10.17858/jmisci.82365

5. Bayramov, A.A. Assessment of invisible areas and military objects in mountainous terrain // A.A.Bayramov, E.G.Hashimov / Defence Science Journal, 2018, vol. 68, №4, pp. 343 – 346. DOI: https://doi.org/10.14429/dsj.68.11623

6. Hashimov, E. G. Detection unobserved moving armored vehicles by seismic method // E.G.Hashimov, A.A.Bayramov / - Baku:National Security and Military Sciences. – 2015. – T. 1. – №. 1. – C. 128-132.

7. Hashimov, E. G. Terrain orthophotoplanes making for military objects revealing // E.G.Hashimov, A.A.Bayramov, B. M. Khalilov / -Baku:National security and military sciences. – 2016, vol. 2, №. 4. – p. 14-20.

8. Modelling of the rationally deployment of observing systems // Y.A.Nasibov, A.A.Bayramov, E.N.Sabziev, E.G.Hashimov / Kharkov: Advanced Information Sistems. Vol. 3, №2, 2019, p.10-13. doi: https://doi.org/10.20998/2522-9052.2019.2.02

9. Piriyev, G. K. Modelling of the battle operations. Monograph // H.K.Piriyev, E.G.Hashimov, A.A.Bayramov / -Baku: Herbi Nashriat. – 2017. -256 p.

10. Geographic Information Systems (GIS): [Electronic resource] / URL: https://www.earthdata.nasa.gov/learn/backgrounders/gis

A METHOD OF DETECTING MOVING MACHINERY

Hasanov A.H., Talibov A.M., Hashimov E.G.
National Defense University; Azerbaijan Technical University, Baku, Azerbaijan

When military operations are conducted or troops are concentrated in combat posts located in mountainous areas or forest massifs, it becomes difficult to directly observe the movement of the enemy's heavy armored vehicles - tanks, armored personnel carriers, infantry fighting vehicles, cannon tractors and other heavy vehicles. As a result, the probability of the enemy's sudden artillery attack on the positions of our troops increases [1,2]. Therefore, it is very important to quickly detect the movement trajectory of the enemy's invisible and distant heavy equipment in the conditions of the mountain landscape [3-5].

The device for detecting moving objects is divided into two groups according to the working principle: active and passive devices.

The article looks at passive detection devices. This option is determined by the fact that in combat conditions, the electromagnetic field generated by the active detection device can be detected by the enemy's radar device and subjected to artillery attack. In the article, a method of detecting the movement of the enemy's invisible heavy equipment hidden behind a forest massif, a high hill or a mountain range at a distance of 3-5 km using the three-coordinate detection 3D device of the seismic location is proposed. This type of 3D devices allows you to accurately determine the position of target objects in space. By applying the new plasma technology developed by us as a seismic accelerometer, the use of highly sensitive sensors made of PVDF+BaTiO3+PZT polymer hybrid piezoelectric composites based on nanoscale BaTiO3, SiO2 and microscale piezoelectric materials was proposed. Polyvinylidenfluoride (PVDF) was used as a matrix additive.

References

1. Piriyev G. K. et al. Modelling of the battle operations //Monografiya, Herbi Nashriat", Baku. – 2017.
2. Bayramov, A.A., Hashimov, E.G.: Assessment of Invisible areas and military objects in Mountainous Terrain // Defense Sciense Journal, **68**(4), 343–346 (2018). https://doi.org/10.14429/dsj.68.11623
3. Bayramov A. A. et al. The detection of invisible objects on the terrain on the basis of GIS technology //Geography and nature sources. – 2016. – C. 124-126.
4. Bayramov A.A., Hashimov E.G. Seismic Location Station for Detection of Unobserved Moving Military Machineries // Journal of Management and Information Science, 2016, Vol.4, № 2, p. 61-66. DOI: https://doi.org/10.17858/jmisci.8236513-cw
5. Hashimov E. G., Bayramov A. A. Detection unobserved moving armored vehicles by seismic method //National Security and Military Sciences. – 2015. – vol. 1. – №. 1. – C. 128-132.
6. Hashimov E. G. et al. Determination of the bearing angle of unobserved ground targets by use of seismic location cells //2017 International Conference on Military Technologies (ICMT). – IEEE, 2017. – p. 185-188.

DEVELOPMENT OF ATMOSPHERIC WEAPONS

Ganjiyev A.Sh., Khalilov Y.M.
Military Institute named after Heydar Aliyev, Baku, Azerbaijan

It is well known that humans have developed various weapons of destruction. It is possible to create a disaster in a certain area with atmospheric weapons, which are considered global weapons. The operation of atmospheric weapons is based on the microscopic instability of the particles that make up clouds and are free in the atmosphere. With a decameter range dipole antenna system, electromagnetic energy heats the ionosphere above the ozone layer and creates an artificial ion cloud. It is used to reflect intermediate frequency waves and create a plasma of beams focused at a given geographical point.

It takes a lot of energy to heat the air mass. Also, this system should have a good efficiency. The second important problem is the accurate initiation effect of forecasting the dynamics of geospheric processes, which requires a significant scientific base.

Active phased antenna arrays are proposed as emitters in atmospheric weapon systems. Controlling the air mass heated by the space waves of the dipole antenna system is difficult and requires initiation. In the proposed active phased antenna arrays system in the decameter wave range, the radiation direction and orientation are adjusted by changing the shape of the diagram, the amplitude-phase distribution of the currents, or by individually changing the excitation field of each active radiating element. The location of the active phased antenna arrays system in the area and the number of radio transmitter modules, conventionally divided into sections, are selected according to the required radiation power.

Active phased antenna arrays with electric coning has wider possibilities. They ensure the creation of different phase shifts in the entire opening of the antenna and a large rate of change of these shifts with relatively small power losses. The way the beam swings in space is possible with a pre-given program or with the application of artificial intelligence. The phase values of the sections are adjusted from the common point. By adjusting the phases in different sections, the movement of the heated mass can be controlled. So there is no need for initiation. This will ensure the effective operation of atmospheric weapons.

References

1. Jerry, E. Smith. The ultimate weapon of the conspiracy / Jerry E. Smith. Published by Adventures Unlimited Press One Adventure Place, – Kempton, Illinois, USA, 2002 – P. 24–27.
2. Piriyev G. K., Hashimov E. G., Bayramov A. A. Modelling of the battle operations //Monografiya, Herbi Nashriat", Baku. – 2017.
3. Ganjiyev, A.S. Theoretical basis of radiolocation. Textbook./ A.S. Ganciyev, E.Y. Karimov – Bakı: – HN, – 2020. – 511 p.
4. Ganjiyev, A.S. Phased antenna arrays // – Baku: Collection of scientific works of the Military Institute named after Heydar Aliyev, – 2016. №2 (27), – p. 35-40.

THE ROLE OF GEOINFORMATION TECHNOLOGIES IN THE PROTECTION OF NATIONAL SECURITY – IN THE EXAMPLE OF THE PROTECTION OF STATE BORDERS

Nasibov Y.A.
National Defense University, Baku, Azerbaijan

Protection of state borders is the basis of the country's national security and is one of the main stages of defense against foreign threats. The developed countries of the world use geographic information systems based on spatial data to protect their borders [1]. Different types of technical surveillance devices are used during border protection. The correct determination of the positions of technical surveillance devices in the area is considered one of the main issues [2-4].

In the article, a study was conducted on the issue of correct location of observation points in the area. Various digital terrain models were developed using GIS technology and digital elevation data for the purpose of conducting the research.

After the restoration of state independence of the Republic of Azerbaijan, the strengthening of national sovereignty, the organization of reliable protection of the state border and the determination of state borders with neighboring countries have become one of the main priority areas of state policy. The national border strategy established the conceptual foundations of the border policy and defined the tasks ahead for the protection of the state border. Border security is an essential part of a country's defense and is of vital importance to government agencies around the world [5]. Organizations responsible for border protection use advanced technologies to effectively and reliably protect their borders against threats such as illegal migration and terrorism [6]. Examples of these technologies include surveillance and radar systems. Border security is a rather complex and serious problem. Various factors influence the solution of this problem: the level of development of the state from the socio-economic and military point of view, the geographical situation of the country, the length of the borders, the approach of the bordering state or states to this issue, the scale and structure of cross-border threats, the professionalism of the armed structures responsible for border security [7]. The sensitive geographical situation of the Republic of Azerbaijan confronts it with a number of cross-border threats such as international terrorism, illegal migration, transnational organized crime, human trafficking, drug smuggling, and proliferation of weapons of mass destruction [8]. Ensuring the security of the borders of each country is a necessary condition for its continuous development and successful international cooperation.

It is no coincidence that in our modern world, national states attach special importance to all components of strengthening their national security, including the security of their borders, and actively work towards the optimal organization of border services [8]. An area bordering the Russian Federation was selected as the research area. ASTER GDEM (Global Digital Elevation Model) elevation data of the area selected for the study was provided from an open source. Esri's ArcGIS Desktop and Global Mapper software were used as software. Observation conditions were studied from each observation post in the study area. A complex method based on GIS was applied in the

study of observation conditions. The correct selection of the positions of the border observation points allows to use a minimum number of observation devices. This can be considered favorable from the economic point of view. The use of Geographic Information Systems (GIS) allows effective exchange of digital spatial data collected and analyzed at border points with headquarters, neighboring and higher units.

References

1. Bayramov A. A., Hashimov E. G., Amanov R. R. The detection of invisible objects on the terrain on the basis of GIS technology //Geography and nature sources. – 2016. – p.124-126.
2. Hashimov E. G., Bayramov A. A. Seismic Location Station for Detection of Unobserved Moving Military Machineries //Journal of Military and Information Science. – 2016. – T. 4. – №. 2. – p. 61-66.
3. Hashimov, E. G., Bayramov, A. A., Nasibov, Y. A., & Amanov, R. R. (2015). Application of relief digital model for combat operation planning. *Military Knowledge*, (4), 63-69.
4. Nasibov Y. A. et al. MODELLİNG OF THE RATİONALLY DEPLOYMENT OF OBSERVİNG SYSTEMS //Advanced Information Systems. – 2019. –T. 3. – №2.-p. 10-13.
5. Cantens, T. Potential uses of geodata for border management: [Electronic resource] // WCO News – Brussels, – 2019. URL: https://mag.wcoomd.org/magazine/wco-news-89/potential-uses-of-geodata-for-border-management/
6. Malikli, G. Border security issues // Baku: Military Knowledge, 2019. №3, p. 59–63.
7. Concept of National Security of the Republic of Azerbaijan: [Electronic resource] // Presidential Decree - 2007. URL: https://e-ganun.az/framework/13373
8. Malikli, G. The problem of military and border security in the national development system of the Republic of Azerbaijan //- Nakhchivan: Nakhchivan State University. Scientific Works. Social sciences series, – 2020. No. 6(107), – p. 50–54.

ANALYSIS OF THE EFFECTIVENESS OF RAISING THE ANTENNA TO A HIGH ALTITUDE

Zulfugarov B.S.
National Defense University, Baku, Azerbaijan

The range of ultrahigh frequencies communications strongly depends on the height of the antenna. The antenna can be raised to great heights using, for example, an air balloon. But this causes signal loss in the feeder [1-4]. Consequently, there is a problem of choosing the optimal antenna height at which the signal at the receiver input will be maximum. Choosing the optimal antenna height is a pressing problem in the field of ultrahigh frequencies communication systems. Communication efficiency directly depends on this parameter, and optimizing it will significantly improve system performance [3, 5]. Solving this problem has the potential to improve a wide range of telecommunication technologies, such as ultrahigh frequencies communication systems, unmanned aircraft and remote sensing of the Earth [2, 6]. The study aims to conduct a comprehensive analysis to determine the optimal height for raising an ultrahigh frequencies radio communication antenna. The research methodology includes determining target communication parameters, creating mathematical models of the system, analyzing the effect of antenna height on communication performance,

optimizing parameters and verifying results through simulation. This will allow us to study the influence of various factors on the efficiency of antenna elevation and optimize its height to achieve maximum communication performance. Sampling parameters include types of antennas and drop feeders, and communication frequency. These parameters will ensure the representativeness of the research results and will allow the methodology to be adapted to the specific conditions of use of ultrahigh frequencies communication systems.

The main results of the study will include determining the optimal antenna height to maximize communication efficiency while minimizing signal loss in the feeder. The study should also identify the impact of antenna and feeder types on communication quality. It is likely that these results will provide important practical recommendations for optimizing the antenna height selection and improving the performance of ultrahigh frequencies communication systems. The findings of the study will indicate the optimal antenna height to maximize communication efficiency while minimizing signal loss in the feeder. The recommendations will also address the importance of considering the characteristics of antennas and reduction feeders to optimize the performance of ultrahigh frequencies communications systems. Optimal placement of the antenna at the correct height allows you to achieve maximum communication and data transmission efficiency with minimal signal loss. Antenna and feeder selection recommendations can significantly improve the performance of communications systems in a variety of applications.

The study provides the opportunity to optimize the height of antenna placement to improve the quality of ultrahigh frequencies communications. This will improve the performance and reliability of communications in various fields such as telecommunications, unmanned aircraft and remote sensing.

References

1. Shawel, B. S., Woldegebreal, D. H., Pollin, S. A Deep-Learning Approach to a Volumetric Radio Environment Map Construction for UAV-Assisted Networks // *International Journal of Antennas and Propagation*, – 2024, Volume 2024, – p. 2023-2038

2. Xing, J. Chapter 9 - 5G radio-frequency design / J. Xing, Z. Zhang, Q. Liu [et al.] // *5G NR and Enhancements*, – 2022, From R15 to R16, – p. 507-556

3. Akpado, K. A. Investigating the Impacts of Base Station Antenna Height, Tilt and Transmitter Power on Network Coverage / K. A. Akpado, O. S. Oguejiofor, C. O. Ezeagwu [et al.] // *International Journal of Engineering Science Invention*, – 2013, Vol. 2, Issue 7, – p. 32-38

4. Abdallah, N. Investigation of the Effect Different Antenna parameters (Height, Tilt, and Power) on Network Coverage and System Capacity / N. Abdallah, H. Alyasiri, M. H. Ali [et al.] // *American Scientific Research Journal for Engineering, Technology, and Sciences*, – 2019, Volume 56, Number 1, – p. 74-85

5. Ibrahim, E., Ismael, F. E., Saeid, E. Investigation of the Effect of Receiving Antenna Height on Cell Coverage Area // *International Journal of Wireless Communication and Simulation*, – 2017, Volume 9, Number 1, – p. 15-22

6. Hashimov E. G., Huseynov B. S. Some aspects of the combat capabilities and application of modern UAVs //Baku:"National Security and military knowledges. – 2021. – №. 3. – С. 7.

SOME PROPERTIES OF SEMICONDUCTORS USED IN MODERN COMMUNICATION TECHNOLOGIES

Nasirov E.V., Nasirov V.I., Huseynov A.Q., Mabudov Q.F.
Military Institute named after Heydar Aliyev, Baku, Azerbaijan

Modern technology materials are an integral part of the electronic devices that surround us [1-5]. Semiconductor materials, such as telluride-based compounds, play an important role in various technological applications, especially in electronics and optoelectronics [6-8]. The construction phase in the crystal structure of $Cu_{1.55}Zn_{0.35}Te$ refers to the arrangement of atoms or ions within the crystal lattice during its formation. $Cu_{1.55}Zn_{0.35}Te$ is a compound semiconductor composed of copper (Cu), zinc (Zn), and tellurium (Te). Understanding the characteristics of its transformations during construction provides insights into its properties and potential applications. In the article, the study of structural transformations in $Cu_{1.55}Zn_{0.35}Te$ crystal by X-ray diffractometric method is explained. Since copper atoms can be in two different valence states (Cu1+, Cu2+) in the crystals of compounds of the Cu-Te system, there are a number of non-stoichiometric compounds between the stoichiometric compounds Cu2Te and CuTe. The study of structural transformations in non-stoichiometric combinations of the Cu-Te system is of particular importance.

It was determined that the studied sample is two-phase, undergoes structural transformation from room temperature to melting temperature T ≥973 K and T temperature. For the crystal lattice parameters of the rhombic phase at room temperature, α=7.353Å, b=21.991Å, c=36.407Å, and for the hexagonal lattice parameters, α=7.350Å, c=22.495Å, and for the UMK lattice parameter of the high-temperature phase, a=6.124 Å were obtained. It was determined that the lattice parameters in the studied crystal grow linearly depending on the temperature, and only the parameter c of the rhombic phase decreases in the temperature range (290-473)K, and increases linearly starting from 473K. With a wide range of military applications, this substance can be used in thermogenerators, infrared detectors, night vision and thermal vision devices, optical military communications devices, and electronic warfare systems for detecting heat signatures or other infrared emissions associated with enemy targets.

References

1. Гашимов Э. Г., Байрамов А. А. Пьезоэлектрических композиты для разработки на их основе приемно-передающих акустических антенн //Евразийский Союз Ученых. – 2015. – №. 5-3 (14). – С. 38-40.

2. Hashimov E. G., Bayramov A. A. Detection unobserved moving armored vehicles by seismic method //National Security and Military Sciences. – 2015. – Т. 1. – №. 1. – С. 128-132.

3. Hashimov E. G. et al. Development of the multirotor unmanned aerial vehicle //National security and military sciences. – 2017. – Т. 3. – №. 4. – С. 21-31.

4. Hasanov A. H., Hashimov E. G. Analysis of the effectivness of communication and automated management systems //Modern directions of development of information and

communication technologies and management tools, Abstracts of reports of the 12th Int. Scientific and Technical Conf. – 2022. – T. 1. – C. 1-4.

5. Gasanov A. G., Bayramov A. A., Hashimov E. G. Mathematical modeling of the electron structure of SiO2 nanoparticle //Fizika. – 2017. – T. 23. – №. 1. – C. 34-39.

6. Asadov, Yu.G. "Structural transformations in crystals of Cu1.79 Zn0.05 Te" / Yu.G.Asadov, K.M.Dzhafarov, A.G.Babaev [etc.] // Baku: ANAS News, Physics, - 1995. T. 1, No. 3, – p. 41.

7. Blachnik, R., Lasocka, M., Walbercht, U. Structal transfotuction in system of Cu-Te. // Journal of Solid State Chemistry, 1983. 48, – p.431-438.

8. Nasirov V.I. "Structural phase transformations in $Cu_{1.55}$ $Zn_{0.20}$ Te crystal"/ Nasirov V.İ., Nasirov E.V., Rzayeva A.B.// -Baku: Proceedings of Science of the Military Institute named after Heydar Aliyev, Volume 21, № 2, 2023 / 62-67.

EFFECTIVE APPLICATION OF TELEMETRY SYSTEMS IN UNMANNED AERIAL VEHICLES

Rustamov A.R., Gasanov A.G.
Military Scientific Research Institute, Baku, Azerbaijan
Azizullayev M.G.
National Aerospace Agency, Baku, Azerbaijan

Currently, various types of unmanned aerial vehicles (UAVs) are widely used on the battlefield and in operations as both intelligence and strike tools, and are viewed as highly effective tools that can solve combat tasks. The conduct and outcome of military operations, the degree of combat readiness of the army, and the ability to perform the assigned task depend significantly on the use of UAVs. The analysis of modern wars shows that the widespread use of UAVs makes it possible to significantly reduce the loss of manpower of units, as well as to have an advantage over the enemy both in terms of strength and morale-psychological condition. It is known that the characteristic feature of the military operations that began in Karabakh on September 27, 2020 was the effective use of various types of UAVs by the Azerbaijani Army. The Armenian army defends the occupied territories with S-300PS, S-125, 2K2 Kub, 2K11 Krug, Buk-M2, Tor-M2, OSA-AKM Air Defense and Autobaza-M, Repellent1, Groza -S, Mortira, Manushak, Pole -21 was organized in several echelons with Radio Electronic Combat systems [1-4]. From UAVs in military operations it was used in echeloning, swarming and interaction with other types of weapons. Its use for military, civilian and professional purposes is increasing rapidly, and it is interesting to study the telemetry systems used in UAVs.

Telemetry is the technology used to receive, record and transmit various data collected by UAVs during flight, collecting basic information such as its flight status, position, speed, altitude and battery level. It can also provide information such as interior and exterior conditions, engine temperature, engine speed, and GPS location. This information is essential to monitor in real-time how the UAV is operating and under what conditions, to optimize flight parameters, ensure safety and intervene when necessary. Telemetry systems provide operators with detailed

information to ensure safe UAV flight, as well as collect data for analysis or further review. It processes data received from various sensors and can transmit them to a control station, an operator or a ground station. The UAV operator can receive information about its condition during flight and intervene if necessary. It is essential to ensure safe and efficient operation.

The data provided by the telemetry systems have a great impact on the UAV's flight quality, safety and ability to successfully perform its tasks. Telemetry systems may include: flight control systems; positioning GPS/GNSS systems; sensors that monitor altitude and other flight parameters; cameras and sensors to monitor battery level, power consumption and power status. RFD-900X, 3DR radio and RFD-868x telemetry modules are currently used. In order to investigate the effective application of these telemetry tools, using the methodology given in [5-9], the RFD 900X for a distance of 10 km, the RFD 868x for a distance of 40 km, it is appropriate to use telemetry system [10-11].

References

1. Hashimov E. G., Huseynov B. S. Some aspects of the combat capabilities and application of modern UAVs //Baku:"National Security and military knowledges.–2021.– №. 3. – P. 14-24.

2. Hashimov E. G. et al. Development of the multirotor unmanned aerial vehicle //National security and military sciences. – 2017. – T. 3. – №. 4. – C. 21-31

3. Hashimov E. G., Bayramov A. A. The flight dynamics of drones //National security and military sciences. – 2016. – T. 2. – №. 3. – C. 11-16.

4. Huseynov, B.S., Hashimov, E.G. Characteristics of UAVs application during the Second Karabakh War // Problems of informatization. Proceedings of 11-th International Scientific and Technical Conference. Vol. 3. - Baku – Kharkiv – Bielsko-Biala: november 16 – 17**,** -2023, -p.10-11. doi: https://doi.org/10.32620/PI.23.t3

5. Gasanov, A.Q. Solving problems of mathematical modeling of military systems. Textbook. -Baku: Military Publishing House, -2018, -120 p.

6. Piriyev, H.K., Hashimov, E.G., Bayramov, A.A. Modelling of battle operations. Monograph. Baku: Military publishing house, 2016. 250 p.

7. Hashimov, E.G., Talibov, A.M., Gasanov, A.Q. Mathematical modeling of military systems. Textbook. -Baku: Military publishing house, -2018. -266 p.

8. Abramov, S.K., Abramova, V.V., Abramov, K.D., Lukin, V.V., Bondar, V.V., Kaluzhinov, I.V. Methodology for determining the detection field of unmanned aerial vehicles by a ground observer // Kharkov, Radioelectronics and computers systems, – 2020, No. 3(95). - With. 35 - 42.

9. Makarenko, S.I. Analysis of means and methods of countering unmanned aerial vehicles. Functional damage by microwave and laser radiation // – St. Petersburg: Control, Communication and Security Systems, – 2020. No. 3, – p. 122-157.

10. Genç, Y. M. Erciyes, E. İnsansız Hava Araçları. Tehditleri ve Guvenlik Yönetimi. // Türkiye İnsansız Hava Araçları Dergisi, – 2020. No. 2(2), – s. 36-42.

11. Filin, E.D., Kirichek, R.V. Methods for detecting small unmanned aerial vehicles based on electromagnetic spectrum analysis. // Information technologies and telecommunications, – 2018. vol.6. No. 2, – p. 87-93.

WORKFLOW FROM GEOID TO MAP IN THE PROCESS OF MAPPING THE TERRITORY OF AZERBAIJAN

Musayev I.F.
Ministry of Digital Development and Transport, Space Agency
of the Republic of Azerbaijan (Azercosmos), Baku, Azerbaijan

Geoinformation portals operating on the basis of satellite images provide not only the spatial image of the area or object, but also meta, vector and attributive information about them. In most cases, this information may be sufficient for users. Because going to anywhere, learning information about the area or object and transmitting this information to other users or receiving it from them is enough to ensure daily activities. However, without a topographic map or plan, it is impossible to design and implement large-scale industrial constructions, as well as solve other issues related to the area and requiring accuracy. A topographic map is a precise graphic representation of a geographic area and is a powerful communication and management tool. Maps help individuals and organizations communicate ideas and information more effectively.

Currently, the topographic maps used in the state organizations of the Republic of Azerbaijan are adapted to the map standards of the NATO in terms of their mathematical basis and cartographic design. In addition, it is advisable to integrate the height system of the above-mentioned maps into the NATO height system. Because the height systems used in geographic information (GIS) based open internet portals and GIS systems of most developed countries are related to the NATO height system.

This provides favorable opportunities for international cooperation activities related to territorial elevation issues, development of joint projects, exchange of information and issues of availability to them. The integration of the height system of topographic maps used in the state organizations of Azerbaijan into the NATO height system will provide a significant benefit sustainable development of the country's industry and agriculture in general.

The article discusses possible solutions for integrating the height system of topographic maps used in Azerbaijan into the NATO height system.

References

1. Musayev I., Gojamanov Magsad., 2019: “Establishment the state interactive geo-information center.” Colloquim-journal, warsaw, Poland. 27 (51).
2. Martina Sacher., Gunter Leibsh, 2015 “The European height reference system and its realization.”
3. Musayev, I.F, Hashimov, E.G. Creation of an interactive geoinformation center in Azerbaijan // National security and military sciences, 2020, 2(6), -p.13-18
4. Musayev, I.F., Hashimov, E.G. Establishment of interactive geo-information center in Azerbaijan // National security and military sciences, 2019, №4(5) p.12-17

ANALYSIS OF OPPORTUNITIES TO DETECT UNVISIBLE MILITARY OBJECTS

Huseynov M.A., Piriyev H.K.
National Defense University; Azerbaijan Technical University, Baku, Azerbaijan

In the report, the theoretical and practical issues determining the basics of object detection were reviewed, various methods used to detect invisible objects were analyzed, and additional theoretical and experimental researches enabling the detection of objects were justified. The analysis of the scientific results of some research studies shows that the collection and visualization of digital information about the territory makes it possible to solve the problem of detecting the enemy's surface targets, determining their coordinates and the distance to them [1-6].

Taking into account the results of the analysis, it should be noted that conducting scientific research in the direction of solving the problem of detecting invisible military objects using GIS technology is one of the urgent issues of modern military science [7]. Conducting research in this area will allow the creation of modern devices and systems, including software, to detect enemy targets.

Within the scope of the issue under consideration, the principles of object detection can be used to record the movement of invisible enemy objects located in various areas of modern military operations and to take appropriate action, as well as to collect and visualize the necessary information about the area during the preparation stage of military operations. This will have a positive effect on facilitating the work of the commander in the process of planning military activities, reducing time loss, and harmonizing the work of commanders in the battle process.

References

1. Geographic information systems for military purposes. Textbook./ Utekalko V.K. and others. Ed. G.P.Kobeleva. Minsk: VA RB, 2009, 244 p.
2. Hashimov, E.G. et al. Application of relief digital model for combat operation planning // – Baku: Military Knowledge, – 2015. № 4, – p. 63–69.
3. Bayramov, A.A. Seismic location station for detection of unobserved moving military machineries // Journal of Management and Information Science, Turkey, 2016, vol.4, № 2, p. 61-66. DOI: https://doi.org/10.17858/jmisci.82365
4. Bayramov, A.A. Assessment of invisible areas and military objects in mountainous terrain // A.A.Bayramov, E.G.Hashimov / Defence Science Journal, 2018, vol. 68, №4, pp. 343 – 346. DOI: https://doi.org/10.14429/dsj.68.11623
5. Hashimov, E. G. Detection unobserved moving armored vehicles by seismic method // E.G.Hashimov, A.A.Bayramov / - Baku:National Security and Military Sciences. – 2015. – T. 1. – №. 1. – C. 128-132.
6. Hashimov, E. G. Terrain orthophotoplanes making for military objects revealing // E.G.Hashimov, A.A.Bayramov, B. M. Khalilov / -Baku:National security and military sciences. – 2016, vol. 2, №. 4. – p. 14-20.
7. Bayramov, A. A. The detection of invisible objects on the terrain on the basis of GIS technology // A.A.Bayramov, E.G.Hashimov, R.R.Amanov/ -Baku:Geography and nature sources. – 2016, № 1. – p. 124-126.

DEVELOPMENT OF A 3D MODEL OF THE SELECTED AREA USING THE PHOTOGRAMMETRY

Piriyev H.K., Bayramov A.A., Khalilov B.M.
National Defense University, Baku, Azerbaijan

For the successful conduct of military operations and military staff exercises, the use of 3D terrain modeling methods to identify hidden enemy positions plays an important role [1-7].

The paper presents the results of work on creating a 3D model of a selected area with a certain area.

The survey was carried out using a UAV. A digital camera with a focal length of 15 mm was used for photography. The shooting was carried out from a height of 125 meters, resulting in 800 photographs with a spatial resolution of 3-5 cm.

The resolution of orthomosaics (photos) is 1 cm, the accuracy of the created 3D models is 1000 points/m2.

Photographing was carried out in fully automatic mode.

The "ILCE-7R v.2.00" program was used to process the images. The photo dimensions are 7360x4912 pixels, the volume is 13÷16 MB, the vertical and horizontal resolution is 350 dpi, the shooting exposure is 1/3200 sec.

Photogrammetric processing of the resulting photographs and creation of a 3D terrain model was carried out using the Bentley ContextCapture program. The resulting final photorealistic model was saved in the ".3mx" and ".obj" file formats. In addition, the orthophotomap of the area was saved in the ".tiff" (GeoTİFF) format. The report provides a reconstructed 3D image of the study area.

References

1. Hashimov E. G., Bayramov A. A., Khalilov B. M. Terrain orthophotomap making and combat control //Proceeding of Internatonal Conf."Modern Call of Security and Defence". I-st. – 2016. – T. 19. – C. 68-71.
2. Nasibov Y. A. et al. Modelling of the rationally deployment of observing systems //Сучасні інформаційні системи. – 2019. – №. 3,№ 2. – С. 10-13.
3. Bayramov A. A. et al. The detection of invisible objects on the terrain on the basis of GIS technology //Geography and nature sources. – 2016. – С. 124-126.
4. Bayramov A. A., Hashimov E. G. Assessment of invisible areas and military objects in mountainous terrain //Defence Science Journal. – 2018. – Т. 68. – №. 4. – С. 343.
5. Hashimov E. G. et al. Terrain orthophotoplanes making for military objects revealing //National security and military sciences. – 2016. – Т. 2. – №. 4. – С. 14-20.
6. Hashimov E. et al. GIS technology and terrain orthophotomap making for military application //Journal of Defense Resources Management. – 2017. – Т. 8. – №. 2. – С. 81-90.
7. Hashimov E.G., Bayramov A.A. Application of GIS and seismology methods for detection of invisible military objects. Monograph//- Baku: Military publishing house, 2017, 246 p.

DETECTION OF UAVs WITH ELECTRO-OPTICAL SYSTEM

Maharramov R.R.
Military Scientific Research Institute, Baku, Azerbaijan
Hashimov E.G.
Azerbaijan Technical University, Baku, Azerbaijan

The experience of local wars and military conflicts around the world shows that in order to minimize the loss of manpower in wars and to make operations more effective, operations conducted without the participation of manpower will be more preferred in future wars. Thus, the wide use of reconnaissance UAVs and blow UAVs in conducting combat operations has shown their effectiveness [1-3].

One of the main problems for air defense systems is the development of UAVs. Timely detection of small-sized, relatively silent and low-altitude UAVs by Air Defense Systems becomes difficult. Special colors and protective layers are used in the development of UAVs, which make them difficult to detect by visual observation posts or radiolocation stations [4]. There are various methods for detecting UAVs. Each method differs from each other in its advantages, disadvantages, application conditions, accuracy and other parameters. One of the main methods of detecting UAVs is detection by radiolocation stations. Radiolocation stations are an active means of monitoring the airspace. Airspace surveillance and air target detection using radiolocation stations within a unified air defense system is a fairly common traditional method. During the Patriotic War, the role of radiolocation stations in controlling the airspace of Azerbaijan was great. Thus, RLSs have duly fulfilled the problems of transmitting information to anti-aircraft missile complexes or other types of troops for the detection, identification, and destruction of UAVs that have entered our airspace [3]. In order to combat UAVs more effectively, it is important to detect them quickly at a long distance also as well as in the dead canyon. The field of vision of radiolocation stations is determined by the design of the RLS antenna and its operating characteristics (wavelength, transmission power and other parameters) [5, 6]. Taking into account the relatively short detection ranges of small-sized UAVs, in order to fight with them in a dead zone, it is considered appropriate to equip the designated units and the units guarding critical objects with small-sized (specialized) RLS, and the VOPs with an electro-optical system.

The use of existing and promising electro-optical systems in the direction of the likely flight of the enemy, in VOPs, allows timely detection of UAVs in the dead zone, recognition of their class, type and current nature of their movements.

In the future, the mentioned electro-optical systems can be replaced by more improved models. Thus, examples of electro-optical systems have already been developed, which can detect small UAVs in time.

In order to effectively detect UAVs in a dead zone, when creating a radiolocation area, it is necessary to pay attention to the battle position of radiolocation stations and the number and placement of visual observation posts equipped with an electro-optical system in the area. To reduce the risk of a drone attack on a radiolocation station, control of its dead zone using an electro-optical system can be organized in various

options. These options differ from each other mainly depending on where the electro-optical control devices are placed in the area relative to the radiolocation station, how the electro-optical device is directed and its viewing angle.

In the paper is investigated the problem of detecting of the enemy's unmanned aerial vehicles flying in a dead ravine in the direction probable flight by means of an electro-optical system placed on a visual observation post.

References

1. Hashimov E. G., Huseynov B. S. Some aspects of the combat capabilities and application of modern UAVs //Baku:"National Security and military knowledges. – 2021. – №. 3. – p. 14-24. https://mod.gov.az//images/pdf/7440712d93276d13d09990c7a1e203ea.pdf

2. Hashimov E. G. et al. Development of the multirotor unmanned aerial vehicle //National security and military sciences. – 2017. – Т. 3. – №. 4. – С. 21-31

3. Hashimov E. G., Bayramov A. A. The flight dynamics of drones //National security and military sciences. – 2016. – Т. 2. – №. 3. – С. 11-16.

4. Hashimov E., Khudeynatov E. METHODOLOGY FOR ASSESSING THE EFFECTIVENESS OF THE AIR DEFENSE SYSTEM //Системи управління, навігації та зв'язку. Збірник наукових праць. – 2024. – Т. 1. – №. 75. – С. 21-27

5. What is a RLS detection dead zone and methods of it determine? https :// studfile. net/ preview/8961005/page:11/. 21.08.2019.

6. Hashimov E. et al. ASSESSMENT OF DEAD ZONE OF JOINTLY OPERATING RADARS //Системи управління, навігації та зв'язку. Збірник наукових праць. – 2023. – Т. 3. – №. 73. – С. 171-175.

ROLE OF GEOPORTAL IN BORDER SECURITY

Hasanov A.H., Nasibov Y.A., Talıbov A.M.
National Defense University, Baku, Azerbaijan

Border control is important for the territorial integrity of every state. Border posts play a key role in controlling entry and exit, preventing illegal crossings and strengthening security measures. Ensuring border security is a very responsible and complex activity. However, as a result of the application of GIS technology, this activity has become more effective and things have become easier.

The study of Geographic Information Systems technology in developed countries has been aligned with the changing, developing computer technology since the end of the 20th century and has given a great impetus to the transfer of theoretical information to practice in military science [1].

In the modern world, Geographical Information Systems (GIS) technologies are of great importance [2-4]. Geographic Information Systems (GIS) is one of the fastest growing areas of information technology. GIS technologies make it possible to integrate cartographic and thematic information in a harmonized single structure and provide prompt development of multi-level, visual solutions for a wide class of issues [5]. There is a need to create a geoportal for the purpose of real-time analysis of events occurring at the state border. By using the geoportal, events occurring in the border areas are analyzed instantly, the processes of decision-making and

intervention activities have been accelerated. Geoportal is a web portal used for accessing geospatial data and related geoinformation services through web services. The main task of the geoportal is to provide the user with tools and services for storing, publishing and downloading spatial data, searching for metadata, interactive web visualization, direct access to geodata based on cartographic web services [5]. In another source, a geoportal is defined as an information resource that provides search, access and provision of services for national spatial data [6]. In another definition, a geoportal is a gateway to web-based geospatial resources that allows you to find, view, and access geospatial data and services provided by the organizations that provide them [7]. In recent years, the products of the Esri company have been widely used in the creation of geoportals.

In the article, the reasons for the creation of the geoportal in ensuring the security of the borders are explained and the initial design of the geoportal is presented. It is important to create a geoportal in order to increase the effectiveness of border security. Geoportals are special mapping and spatial data exchange platforms, being a component of Geographical Information System (GIS). Geoportal has customized interfaces, search and analysis tools for different users. In the context of border protection, the geoportal facilitates control through wide spatial data. The Geoportal provides critical data for real-time monitoring and border surveillance and ensures immediate detection of activities such as border violations and illegal crossings by security forces. Drones and other aerial devices are being used for deeper monitoring of areas crossed by state border lines. These are important activities for both security purposes and search and rescue operations. In addition, live video surveillance is provided through security cameras installed along the border areas, potential threats and illegal activities are immediately detected and appropriate measures are taken. The ability to integrate the Geoportal with the above-mentioned radar, sensor and aerial vehicles provides a wide set of data on the state border. It is possible to exchange information with other power structures through the Geoportal.

References

1. Bayramov A. A., Hashimov E. G., Amanov R. R. The detection of invisible objects on the terrain on the basis of GIS technology //Geography and nature sources. –2016. –p. 124-126.

2. Hashimov E. G. et al. Application of relief digital model for combat operation planning // E.G.Hashimov, A.A.Bayramov, Y.A.Nasibov, R.Amanov//Military Knowledge. – 2015. – №. 4. – p. 63-69.

3. Bayramov A. A., Hashimov E. G. Assessment of invisible areas and military objects in mountainous terrain //Defence Science Journal. – 2018. – Т. 68. – №. 4. – p. 343.

4. Hashimov E., Bayramov A. A., Chalilov B. M. GIS technology and terrain orthophotomap making for military application //Journal of Defense Resources Management. – 2017. – Т. 8. – №. 2. – С. 81-90.

5. Imamverdiyev, Y.N. On actual scientific and theoretical problems of geoinformation systems in the big data environment // - Baku: Information society problems magazine, - 2021. No. 2, - p. 38–51.

6. Rules for the formation and integration of national spatial data: [Electronic source] // – Decree of the President of the Republic of Azerbaijan No. 448 dated December 28, 2018, – 2018. URL: https://e-qanun.az/framework/41110

7. Esri Geoportal Server. ArcGIS for INSPIRE: [Electronic resource] // – Esri, – 2021. URL: https://enterprise.arcgis.com/en/inspire/10.8/get-started/introduction-to-geoportals.htm

SOME FEATURES OF OBTAINING ACOUSTIC INFORMATION BY OPTICAL MEANS

Huseynov A.
Military İnstitute named after Heydar Alıyev, Baku, Azerbaijan

Currently, the relevance of research in the field of obtaining acoustic information by probing laser radiation on glass is undeniable. Allowing the study of the physical and mechanical properties of glass and other materials at the micro level, it finds application in the military sphere, materials science, physics, medicine and industry. This process is of particular importance for the security of the information sphere and in the 21st century has risen from the powers of the intelligence services of government agencies to the level of relations in society. One of the main sources of threats to information security is the activities of foreign intelligence services, competitors, criminal communities, organizations, groups, associations and individuals aimed at collecting valuable (confidential) information that is closed to access by unauthorized persons [1]. It is necessary to find out about the plans of the mock enemy, to harm the intelligence agencies by taking measures against sabotage and terrorist activities, as well as to collect information and organize technical channels for information leakage by the relevant units of the Armed Forces in order to successfully carry out operations.

It is known from theory that the speech signal is a complex acoustic signal in the frequency range from 200-300 Hz to 4-6 kHz. Technical leakage channels of acoustic (speech) information are divided into air, vibroacoustic, acoustoelectric, optoelectronic and parametric channels, depending on the physical nature of the formation of information signals, the propagation medium of acoustic vibrations and methods of capturing them [2]. This article discusses the process of obtaining acoustic information through an optical-electronic technical leakage channel created when probing laser radiation on glass.

References

1. Huseynov, A.G. Portable optical communication system. Dissertation of doctor of philosophy in national security and military sciences / - Baku: Military Scientific Research Institute, 2022.- 191 p.

2. Sokolov, A. I. Technical means of information security: technical channels information leaks: textbook. allowance / A. I. Sokolov, M. Yu. Monakhov;– Vladimir: Vladim. state University, –2006. – 71 p.

3. Hasanov A. H., Hashimov E. G. Analysis of the effectivness of communication and automated management systems //Modern directions of development of information and communication technologies and management tools, Abstracts of reports of the 12th Int. Scientific and Technical Conf. – 2022. – T. 1. – p. 1-4.

DESIGN CHARACTERISTICS OF OPTICAL FIBER COMMUNICATION LINES IN COMMUNICATION SYSTEMS

Adiyev G.M., İmanov E.İ., Isgenderov R.Z.
Hayder Aliyev named after Military Institute, Baku, Azerbaijan

Currently, the search and acquisition of new materials is carried out in a random way. Therefore, to reduce the percentage of errors, new technologies and methods are needed (for example, the method of computer-aided design of the optical structure of the material). Resources such as time and information are of particular importance in the construction of radio technical means.

The development of technological process and science causes people to constantly improve information processing. The invention of the first computers played a key role in this process. That invention made it possible to process huge data sets in a short period of time. In this regard, the issue of efficient use of time resources not only in information processing, but also in its transmission appeared. With the discovery of optical fiber communication lines (OLRX), this problem is successfully solved [1-3].

Optical fiber communication lines are widely used in telecommunications and global and local transmission networks of information signals, medical and security systems. Such communication lines are capable of displacing other types of conductors in perspective [4]. Since the installation of conventional cable lines often requires a lot of money, it is more efficient to lay optical fiber communication lines with long life and high data transmission speed.

As a result, it can be noted that different types of optical fibers made of polymer materials have been analyzed and studied, unlike the more commonly known and used glass plastics. Examples of these include photonic crystal fibers, perovskite fibers, and kevlar fiber. With the help of these fibers, it is possible to control optical properties, control dispersion, increase flexibility, ensure longevity, and provide wave direction.

References

1. Hasanov A. H., Hashimov E. G. Analysis of the effectivness of communication and automated management systems //Modern directions of development of information and communication technologies and management tools, Abstracts of reports of the 12th Int. Scientific and Technical Conf. – 2022. – T. 1. – C. 1-4.

2. Ibrahimov, B.G. et al. Research throughput multiservice telecommunication networks // Сучасні напрями розвитку інформацийно-комунікаційних технологій та засобів управління. Матеріали 10-і міжнародної науково-технічної конференції, 9-10 квитня 2020. Том1. Баку-Харків-Жиліна, 2020, с.30

3. İbrahimov B.G. et al. Research and analysis indicators fiber-optic communication lines using spectral technologies //Advanced information systems. – 2022. – T. 6. – №. 1. – p. 61-64.

4. Mansurov, T.M. Electrical and optical communication lines. / T.M. Mansurov, J.A. Aliyev, G.B. Beybalayev Baku: Science Publishing House, -2006.

АВТОМАТИЗАЦІЯ РОЗРОБКИ ДІАГНОСТИЧНОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНИХ СИСТЕМ

Павлик Г.В., Анікін А.М., Сардардінова І.А.
Національний аерокосмічний університет ім. М.Є. Жуковського «Харківський авіаційний інститут», Харків, Україна

Комп'ютерні системи знаходять широке застосування в різних галузях науки й техніки при побудові систем керування, регулювання, передачі й обробки дискретної інформації.

Для забезпечення необхідного рівня якості їхнього функціонування й надійності застосовуються різні підходи: удосконалення існуючих і організація принципово нових систем, їх апаратних і програмних засобів, створення алгоритмічного, апаратно - програмного, контрольно-діагностичного забезпечення, розробка й застосування методів і засобів функціонального й тестового діагностування на етапах проектування, виготовлення й експлуатації комп'ютерних систем і їхніх компонентів [1].

Розробка засобів контролю й діагностичного забезпечення досить трудомістка. При пошуку оптимальних рішень потрібні великі витрати часу навіть при використанні ЕОМ.

Це пов'язане з тим, що в основі рішення поетапних завдань методів розробки діагностичного забезпечення лежить рішення різних логіко-комбінаторних завдань [2].

Метою доповіді є розгляд актуальної проблеми автоматизації розробки діагностичного забезпечення.

В доповіді розглянуто програмно-апаратні засоби розробки діагностичного забезпечення. Розроблений програмний комплекс [3] вирішує наступні завдання: аналіз і формування діагностичних моделей, аналіз серійних послідовностей і побудови каталогів типових представників, побудови контрольних тестів для різних видів діагностичних моделей. Застосування розробленого програмного забезпечення дозволить скоротити строки розробки діагностичного забезпечення й засобів контролю, підвищити вірогідність і якість одержуваних результатів.

Список літератури

1. Knuppel T. Fault Diagnosis for Electrical Distribution Systems using Structural Analysis / T. Knuppel, M. Blanke, J. Stergaard // International Journal of Robust and Nonlinear Control, 2014. – V. 24. – P. 1446 – 1465.

2. Babak V. P. et al. Principles of construction of systems for diagnosing the energy equipment //Diagnostic Systems for Energy Equipments. – 2020. – С. 1-22.

3. Комп'ютерна програма "TEST"// Павлик Г.В., Сіроклин В.П., Анікін А.М., Доценко М.І. – Свід. про реєстр. автор. права на твір № 118504 – Зареєстр. в ДП "УКРНОІВІ" 26.04.2023.

ІНТЕГРАЦІЯ ХМАРНИХ ТЕХНОЛОГІЙ У ВИМІРЮВАЛЬНІ СИСТЕМИ ДЛЯ ЗАБЕЗПЕЧЕННЯ ГНУЧКОСТІ ТА МАСШТАБОВАНОСТІ

Дерев'янко К.А., Гук А.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Інтеграція хмарних технологій у вимірювальні системи відіграє важливу роль у сучасному технологічному ландшафті, пропонуючи нові можливості для забезпечення гнучкості та масштабованості. Одним із ключових аспектів є можливість розширення обчислювальних ресурсів та зберігання даних за допомогою хмарних платформ. Це дозволяє вимірювальним системам легко адаптуватися до змінних потреб користувачів та об'ємів даних, що обробляються. Крім того, інтеграція хмарних технологій дозволяє забезпечити доступ до даних та функцій системи з будь-якого місця, що сприяє підвищенню доступності та ефективності роботи [1]. Важливою перевагою такого підходу є можливість зосередитися на розробці програмного забезпечення та аналізі даних, поклавши на хмарні сервіси більшість інфраструктурних та обчислювальних завдань. Такий підхід до інтеграції хмарних технологій у вимірювальні системи допомагає підвищити їх ефективність, гнучкість та масштабованість, що є ключовими чинниками у сучасному інформаційному середовищі. Інтеграція хмарних технологій дозволяє розробникам систем зосередитися на розробці програмного забезпечення та аналізі даних, змінюючи спосіб вирішення інфраструктурних завдань.[2]

Метою доповіді є дослідження переваг інтеграції хмарних технологій у вимірювальні системи та показі, як це допомагає підвищити їх гнучкість та масштабованість. Також метою є розгляд практичних прикладів застосування цього підходу та обговорення потенційних викликів та шляхів їх вирішення.

Список літератури

1. Петров О. О. Методи захисту інформації в телекомунікаційних системах. Телекомунікаційні технології / О. О. Петров, В. І. Литвиненко. – 2017. – №2. – С. 49–56.

2. Левченко І. П., Сергієнко А. В. Системи ідентифікації та аутентифікації користувачів в сучасних телекомунікаційних мережах. Безпека інформації. 2019. Т. 7, № 3. С. 33–38.

ZKSYNC ERA ЯК НОВІТНЯ ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНІ СИСТЕМА

Свистельник А.О., Сітніков В.І.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні інформаційно-вимірювальні системи відіграють важливу роль у багатьох сферах життя, включаючи енергетику, промисловість, транспорт і медицину. Ці системи збирають, обробляють і передають великі обсяги даних і тому схильні до проблем з масштабуванням і безпекою. ZkSync Era - це рішення Layer 2, яке розширює блокчейн Ethereum за допомогою технології Zero

Knowledge Rollup.[1] Zk-rollup є перспективним інформаційно-вимірювальною системою, може обробляти тисячі транзакцій в секунду, що робить її ідеальним рішенням. Його децентралізований характер, висока пропускна здатність і низька вартість роблять його ідеальним для систем, які генерують великі обсяги даних.[2]

Метою доповіді є огляд сучасних інформаційно-вимірювальних систем, приділяючи особливу увагу новітнім технологіям і їх можливостям.

У доповіді також наводится оцінка ролі мережі ZkSync Era у підвищенні ефективності та безпеки інформаційно-вимірювальних процесів, особливо з точки зору забезпечення конфіденційності та масштабованості обробки даних. Наведенні данні показують що ZkSync Era може використовуватися в різних сферах. Для моніторингу та управління енергоспоживанням в інтелектуальних мережах. Можливо використовувати для збору або аналізу даних в системах промислової автоматизації, для відстеження і моніторингу вантажів в логістичних системах та для зберігання, обміну медичними даними.[3]

Список літератури

1. Freedom is our mission [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://zksync.io/ethos.

2. Zero-knowledge rollups [Електронний ресурс]. – 2024. – Режим доступу до ресурсу: https://ethereum.org/en/developers/docs/scaling/zk-rollups/.

3. Security Zk-rollups [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://zksync.io/security.

СУЧАСНІ БЛОКЧЕЙН ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНІ РІШЕННЯ

Гуленко С.О., Сітніков В.І.
Харківський національний університет радіоелектроніки, Харків, Україна

Все більш складними та різноманітними стають інформаційно-вимірювальні системи. Використання технології блокчейн та платформи Ethereum може значно покращити такі характеристики, як безпека, прозорість, ефективність та надійність. Записи в блокчейн не можуть бути змінені або видалені без відома інших учасників мережі. Технологія блокчейн забезпечує високий рівень безпеки та прозорості, що важливо для надійності та незалежності данних.[1]

Метою доповіді є висвітлення поточних розробок у сфері інформаційно-вимірювальних систем, з акцентом на потенціал технології блокчейн, зокрема Ethereum. Спрямований на розуміння переваг і можливостей, які пропонує блокчейн, та його впливу на сучасні інформаційно-вимірювальні системи.

У доповіді також наводится сутність використання блокчейну Ethereum у покращені та удосконалення прозорості інформаційно-вимірювальних систем. Однією з її головних переваг є можливість створювати децентралізовані додатки (dApps), які пропонують високий рівень безпеки та прозорості. Записи в блокчейні не можуть бути змінені або видалені без відома інших учасників мережі, що гарантує надійність і незалежність даних. Інформаційні та

вимірювальні системи на основі блокчейну Ethereum можуть принести користь у багатьох сферах, включаючи ланцюжок поставок, фінанси, охорону здоров'я та голосування. Наприклад, вони можуть забезпечити надійність і прозорість у відстеженні походження товарів по всьому ланцюгу поставок і запобігти фальсифікації та підробці. Технологія блокчейн також дозволяє створювати "розумні контракти", які автоматизують і узгоджують транзакції між сторонами без участі третьої сторони. Це спрощує і прискорює процеси управління даними та знижує транзакційні витрати.[2]

Список літератури

1. What is blockchain? [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: https://www.ibm.com/topics/blockchain.

2. Ethereum development documentation [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://ethereum.org/uk/developers/docs/.

ЗБІЛЬШЕННЯ ДАЛЬНОСТІ КОНТРОЛЮ РАДІОЧАСТОТНОГО КАНАЛУ УПРАВЛІННЯ БЕЗПІЛОТНОГО ЛІТАЛЬНОГО АПАРАТУ

Марущенко В.В., Чернявський О.Ю.
Національний технічний університет "ХПІ", Харків, Україна

Для забезпечення надійного управління польотом безпілотного літаль-ного апарату необхідно проводити [1, 2]: контроль спектру характерних звукових частот (особливо для безпілотних літальних апаратів); візуальний контроль визначеного сектору із використанням камер спо-стереження; вимірювання спектру теплового випромінювання (більш ефективний для наземних апаратів, бо більшість безпілотних літальних апаратів виготовлено із спеціального пластику та використовуються електродвигуни, які випромінюють незначну кількість тепла); аналіз радіотехнічних сигналів на частотах управління. При цьому необхідно враховувати дальністю дій систем управління без-пілотними апаратами, яка становить до 5 км [2]. **Метою допов**іді є збільшення дальності контролю радіочастотного ка-налу управління безпілотного літального апарату. У доповіді для збільшення дальності дії інформаційно-вимірювальної системи контролю радіочастотного каналу управління безпілотного літального апарату пропонується ввести додаткове обладнання: декілька ретранслято-рів, які встановлено на повітряних кулях із дальністю дії сигналу управління; радіолокаційну (або оптичну) станцію (для контролю за рухом (польотом) безпілотного апарату). Перевагою запропонованих пропозицій є можливість досягнення максимальної дальності передавання та отримання інформації.

Список літератури

1. Герасимов С. В., Чернявський О. Ю., Нанівський Р. А. и др. Комплектування полігону навчально-тренувальними комплексами для підготовки операторів безпілотних летальних апаратів. Збірник наукових праць Військової академії (м. Одеса). 2023. № 2 (20). С. 63-72. DOI: https://doi.org/10.37129/2313-7509.2023.20.63-72.

2. Герасимов С. В., Марущенко В. В., Чернявський О. Ю. Моделювання роботи навігаційної системи для автономного руху безпілотного летального апарату. Матеріали XVI міжнародної науково-практичної конференції "Інформаційні технології і автоматизація". Одеса. 2023. С. 153-154. https://ontu.edu.ua/download/konfi/2023/ Collection-of-abstracts-of-the-conference-ITIA-2023.pdf.

ОПТИМІЗАЦІЯ ПІДСИСТЕМИ РЕЛЕЙНОГО ЗАХИСТУ СИЛОВИХ ТРАНСФОРМАТОРІВ

Кононов В.Б.
Харківський національний університет Повітряних Сил, Харків, Україна
Петрукович Д.Є.
Харківський національний автомобільно-дорожній університет, Харків, Україна

На сьогоднішній день в Україні гостро стоїть питання зі збереження та відновлення працездатності системи генерації та розподілу електроенергії. Особливо актуальною ця проблема стала через повномасштабну російську військову агресію та регулярні спроби російських загарбників знищити, або нанести максимальну шкоду елементам системи генерації та розподілу електроенергії в країні [1].

Сучасні мікропроцесорні засоби захисту та автоматики мають переваги перед традиційними системами релейного захисту та автоматики, які широко використовуються в Україні та базуються на електромеханічних і мікроелектронних реле, та значно краще інтегруються в технологічні системи керування об'єктами електроенергетики [2].

Метою дослідження є аналіз можливих напрямків оптимізації підсистеми релейного захисту силових трансформаторів шляхом застосування сучасних мікропроцесорних пристроїв і систем автоматики в українській енергосистемі, а також оцінки ефективності запропонованих рішень.

Результати проведеного моделювання показали, що мікропроцесорні пристрої захисту силових трансформаторів мають кращі функціональні можливості, менші втрати потужності та вагу, вищу технологічність їх монтажу, налагодження та технічного обслуговування. Застосування сучасних мікропроцесорних засобів захисту та автоматики у підсистемах релейного захисту силових трансформаторів дозволить зменшити вірогідність втрат силового електрообладнання через стрибки струму і напруги викликаних нанесеною шкодою елементам системи генерації та розподілу електроенергії в країні. Також зменшиться час відновлення, що зумовлено вищою технологічністю більш сучасних елементів автоматики.

Список літератури

1. Кононов В.Б., Науменко А. М. Застосування електричних вимірювань засобами вимірювальної техніки в умовах проведення АТО: навч. посіб. - Х.: ХНУПС, 2018. – 392 с.

2. Полярус О. В., Подорожняк А. О., Коваль А. О. Динамічна нейромережева модель первинного перетворювача. Вісник Нац. техн. ун-ту "ХПІ". Темат. вип.: Інформатика та моделювання, Харків: НТУ "ХПІ", 2014, № 35 (1078), С. 152-160.

ОПТИМАЛЬНИЙ АЛГОРИТМ ОБРОБКИ ВИМІРЮВАЛЬНОЇ ІНФОРМАЦІЇ ПРО ТЕХНІЧНИЙ СТАН КОМПЛЕКСУ

Григоренко І.В., Ольховіков Д.С.
Національний технічний університет "ХПІ", Харків, Україна

Показано, що призначення інформаційно-вимірювальних систем при контролі технічного стану складних комплексів є вироблення в результаті проведення вимірювань параметрів і їх подальшої обробки вектору інформаційних результатів, що використовується у подальшому в системах прийняття рішення про стан комплексів [1, 2]. Вироблення вимірювальної інформації у таких системах основане на алгоритмі «ідеальної роботи», який при безнад-мірній системі датчиків первинної інформації (вимірювачів параметрів про технічний стан комплексу) і в припущенні відсутності похибок цих датчиків забезпечує безпомилкове вироблення рішення про технічний стан [3].

Метою доповіді є розробка оптимального алгоритму обробки вимірю-вальної інформації про технічний стан складного комплексу.

У доповіді обґрунтовано, що реалізація запропонованого алгоритму забезпечує незбуреність систем корисним сигналом, за який виступають дійсні значення параметрів контролю комплексу. Незважаючи на те, що незалежність помилок систем від істинного значення параметрів контролю комплексу з урахуванням мультиплікативних складових похибок, неминучого згладжування високочастотних зміщень реальних значень параметрів контролю комплексу за рахунок інерційності датчиків виконується наближено, алгоритм роботи вимірювальної системи прагне максимально наблизитись до алгоритму «ідеальної роботи».

У доповіді обґрунтований математичний апарат для розробки оптимального алгоритму обробки вимірювальної інформації та оптимальний алгоритм обробки вимірювальної інформації про параметри контролю комплексу для забезпечення заданої достовірності визначення технічного стану комплексу.

Список літератури

1. Herasymov S., Soroka V., Milevskyi S. and etc. Development of a Method for Digital Synthesis of Electrical Signals with a Normalized Harmonic Coefficient. 5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). 2023. Pp. 1-5. DOI: https://doi.org/10.1109/HORA58378.2023.10156678.

2. Shmatko O., Herasymov S., Lysetskyi Y. and etc. Development of the automated decision-making system synthesis method in the management of information security channels. Eastern-European Journal of Enterprise Technologies. 2023. № 6(9) (126). Pp. 39–49. DOI: https://doi.org/10.15587/1729-4061.2023.293511.

3. Herasymov S., Soroka V., Milevskyi S. and etc. Development of a Method for Measuring small Nonlinear Distortions of Periodic Electrical Signals. International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT). 2022. Pp. 49-52. DOI: https://doi.org/10.1109/ISMSIT56059.2022.9932685.

ОПТИМІЗАЦІЯ ПАРАМЕТРІВ КОНТРОЛЮ ПРИ ВИЗНАЧЕННІ ТЕХНІЧНОГО СТАНУ БАГАТОПАРАМЕТРИЧНИХ КОМПЛЕКСІВ

Рощупкін Є.С., Гречка О.В.
Харківський національний університет Повітряних Сил, Харків, Україна

Динамічні системи, для яких призначена апаратура контролю, складається переважно з інерційних блоків з характерними постійними часу у діапазоні [1]. При експлуатації багатопараметрічних комплексів у ряді випадків є апріорна інформація про статистичні характеристики параметрів (середньоквадратичне відхилення, дисперсія, кореляційні зв'язки) [2]. Це дозволяє у окремих випадках проводити прогнозування частину параметрів, без проведення їх безпосередніх вимірювань [3].

В умовах обмеженого об'єму емпіричних даних пропонується виходити з того, що не потрібно відновлювати всю функціональну залежність, яка визначає технічний стан комплексу від параметрів контролю, завданням є визначення значень функції у заданих точках.

Метою доповіді є постановка задачі оптимізації параметрів контролю при визначенні технічного стану багатопараметричного комплексу.

У доповіді розглянуто дві задачі: постановка задачі відновлення інформації про технічний стан комплексу та задача відновлення алгоритму регресії залежності параметрів контролю від технічного стану комплексу.

У загальному випадку задачу контролю технічного стану багатопараметричного комплексу пропонується описувати наступним чином. Кожному вектору параметрів контролю ставиться у відповідність деяке число, яке отримане за допомогою випадкового випробування відповідно до умовної щільності імовірності розкладу справного технічного стану комплексу. Інакше, кожному числу ставиться у відповідність закон, відповідно якому при випадковому випробуванні реалізується вибір справності комплексу. Для розв'язання задачі відновлення алгоритму регресії залежності параметрів контролю від технічного стану комплексу необхідно визначити функціональну залежність між параметрами контролю та справністю комплексу.

Список літератури

1. Herasimov, S., Borysenko, M., Roshchupkin, E. et etc. Spectrum Analyzer Based on a Dynamic Filter. *J Electron Test.* 2021 № 37. Pp. 357–368. DOI: https://doi.org/10.1007/s10836-021-05954-0.

2. Shmatko O., Herasymov S., Lysetskyi Y. and etc. Development of the automated decision-making system synthesis method in the management of information security channels. *Eastern-European Journal of Enterprise Technologies*. 2023. № 6(9) (126). Pp. 39–49. DOI: https://doi.org/10.15587/1729-4061.2023.293511.

3. Herasymov S., Soroka V., Milevskyi S. and etc. Development of a Method for Measuring small Nonlinear Distortions of Periodic Electrical Signals. *International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*. 2022. Pp. 49-52. DOI: https://doi.org/10.1109/ISMSIT56059.2022.9932685.

ПРОПОЗИЦІЇ З ВИКОРИСТАННЯ СИГНАЛІ СПЕЦІАЛЬНОЇ ФОРМИ ПРИ РОЗРОБЦІ ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНИХ СИСТЕМ

Герасимов С.В., Кот В.В.
Національний технічний університет «ХПІ», Харків, Україна

Підвищення оперативність контролю технічного стану технологічних комплексів для збільшення коефіцієнту оперативної готовності можливо за рахунок зменшення часу проведення заходів обслуговування [1].

Вимоги до оперативності та якості проведення контролю технічного стану підвищують-ся при переведенні комплексів на експлуатацію за технічним станом.

Традиційними тестовими сигналами для контролю технічного стану технологічних комплексів є синусоїдні коливання [2, 3]. Однак, використання таких сигналів потребують значної витрати часу на проведення контролю та призводять до зниження оперативності його проведення через необхідність введення інерційних блоків для підвищення завадозахищеності. Уникнути даного недоліку можливо за рахунок використання багаточастотних сигналів з нормованим спектром – складних сигналів [1, 2].

Метою доповіді є обґрунтування пропозицій щодо використання сигналів спеціальної форми при розробці інформаційно-вимірювальних систем.

У доповіді обґрунтовано теоретичні основи щодо синтезу вимірювальних сигналів спеціальної форми для контролю технічного стану технологічних комплексів. Показано, що вимірювальні сигнали складної форми дозволяють удосконалити процес автоматизованого контролю технічного стану комплексів. Розглянуто параметри вимірювальних сигналів складної форми, які дозволяють підвищити завадозахищеність процесу контролю.

Зроблено пропозиції щодо практичного використання синтезованих вимірювальних сигналів при розробці інформаційно-вимірювальних систем для контролю технічного стану технологічних комплексів.

Список літератури

1. Herasymov S., Soroka V., Milevskyi S. and etc. Development of a Method for Digital Synthesis of Electrical Signals with a Normalized Harmonic Coefficient. 5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). 2023. Pp. 1-5. DOI: https://doi.org/10.1109/HORA58378.2023.10156678.

2. Shmatko O., Herasymov S., Lysetskyi Y. and etc. Development of the automated decision-making system synthesis method in the management of information security channels. Eastern-European Journal of Enterprise Technologies. 2023. № 6(9) (126). Pp. 39–49. DOI: https://doi.org/10.15587/1729-4061.2023.293511.

3. Herasymov S., Soroka V., Milevskyi S. and etc. Development of a Method for Measuring small Nonlinear Distortions of Periodic Electrical Signals. International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT). 2022. Pp. 49-52. DOI: https://doi.org/10.1109/ISMSIT56059.2022.9932685.

ПРОПОЗИЦІЇ З ВИКОРИСТАННЯ СИГНАЛІ СПЕЦІАЛЬНОЇ ФОРМИ ПРИ РОЗРОБЦІ ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНИХ СИСТЕМ

Герасимов С.В.
Національний технічний університет «ХПІ», Харків, Україна
Сорока В.В.
Державний університет інфраструктури та технологій, Київ, Україна

Підвищення оперативність контролю технічного стану технологічних комплексів для збільшення коефіцієнту оперативної готовності можливо за рахунок зменшення часу проведення заходів обслуговування [1]. Вимоги до оперативності та якості проведення контролю технічного стану підвищують-ся при переведенні комплексів на експлуатацію за технічним станом.

Традиційними тестовими сигналами для контролю технічного стану технологічних комплексів є синусоїдні коливання [2, 3].

Однак, використання таких сигналів потребують значної витрати часу на проведення контролю та призводять до зниження оперативності його проведення через необхідність введення інерційних блоків для підвищення завадозахищеності. Уникнути даного недоліку можливо за рахунок використання багаточастотних сигналів з нормованим спектром – складних сигналів [1, 2].

Метою доповіді є обґрунтування пропозицій щодо використання сигналів спеціальної форми при розробці інформаційно-вимірювальних систем.

У доповіді обґрунтовано теоретичні основи щодо синтезу вимірювальних сигналів спеціальної форми для контролю технічного стану технологічних комплексів.

Показано, що вимірювальні сигнали складної форми дозво-ляють удосконалити процес автоматизованого контролю технічного стану комплексів. Зроблено пропозиції щодо практичного використання синтезованих вимірювальних сигналів при розробці інформаційно-вимірювальних систем для контролю технічного стану технологічних комплексів.

Список літератури

1. Herasymov S., Soroka V., Milevskyi S. and etc. Development of a Method for Digital Synthesis of Electrical Signals with a Normalized Harmonic Coefficient. 5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). 2023. Pp. 1-5. DOI: https://doi.org/10.1109/HORA58378.2023.10156678.

2. Shmatko O., Herasymov S., Lysetskyi Y. and etc. Development of the automated decision-making system synthesis method in the management of information security channels. Eastern-European Journal of Enterprise Technologies. 2023. № 6(9) (126). Pp. 39–49. DOI: https://doi.org/10.15587/1729-4061.2023.293511.

3. Herasymov S., Soroka V., Milevskyi S. and etc. Development of a Method for Measuring small Nonlinear Distortions of Periodic Electrical Signals. International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT). 2022. Pp. 49-52. DOI: https://doi.org/10.1109/ISMSIT56059.2022.9932685.

ПРОПОЗИЦІЇ З ВИКОРИСТАННЯ СИГНАЛІ СПЕЦІАЛЬНОЇ ФОРМИ ПРИ РОЗРОБЦІ ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНИХ СИСТЕМ

Луценко А.С.
Харківський національний університет Повітряних Сил, Харків, Україна
Грекуляк М.В.
Кіровоградська льотна академія, Кропивницький

В основу навігаційних комплексів сучасних повітряних об’єктів покладено інерціальні навігаційні системи [1, 2]. Це пов'язано з тим, що вони надають повну інформацію про навігаційні параметри польоту – курс, диферент, кути крену; прискорення, швидкість руху та координати розташування об’єкта [3]. При цьому вони повністю автономні, тобто не потребують інфор-мації ззовні. Завдяки можливості визначення кутового положення об’єкта з високою точністю в будь-якому діапазоні кутів і з високою частотою виве-дення інформації інерціальні навігаційні системи не мають альтернативи, особливо за відсутності власної супутникової мережі [2].

Підвищення точності навігації польоту об’єктів пов’язане з удосконаленням як засобів вимірювальної техніки, так і математичного забезпечення розв’язування задач обробки інформації [1, 3].

Метою доповіді є пропозицій з удосконалення вимірювання параметрів інерційних навігаційних систем для підвищення безпеки польоту об’єктів.

У доповіді розглянуто проблемні питання застосування інерційних ме-тодів під впливом аномального гравітаційного поля Землі в перспективних навігаційних системах літальних апаратів. Обґрунтовано моделі для забез-печення вимог адекватності реальному полю, з урахуванням зручності їх використання в задачах обробки інформації. Запропоновано задачу раціоналізації способів використання інерціальних навігаційних систем при польоті.

Доведено, що структура похибок навігаційних систем як функцій часу, унікальність їх реалізацій зумовлені впливом ряду неврахованих факторів, які запропоновано враховувати при використанні розглянутих моделей.

Список літератури

1. Herasimov, S., Borysenko, M., Roshchupkin, E. et etc. Spectrum Analyzer Based on a Dynamic Filter. *J Electron Test*. 2021 № 37. Pp. 357–368. DOI: https://doi.org/10.1007/s10836-021-05954-0.

2. Shmatko O., Herasymov S., Lysetskyi Y. and etc. Development of the automated decision-making system synthesis method in the management of information security channels. *Eastern-European Journal of Enterprise Technologies*. 2023. № 6(9) (126). Pp. 39–49. DOI: https://doi.org/10.15587/1729-4061.2023.293511.

3. Herasymov S., Soroka V., Milevskyi S. and etc. Development of a Method for Measuring small Nonlinear Distortions of Periodic Electrical Signals. *International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*. 2022. Pp. 49-52. DOI: https://doi.org/10.1109/ISMSIT56059.2022.9932685.

СЕКЦІЯ 6
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У ЦИВІЛЬНІЙ БЕЗПЕЦІ

Керівник секції: д.т.н., проф. В. А. Глива, КНУБА, Київ
Секретар секції: PhD Д. М. Главчев, НТУ «ХПІ», Харків

MILITARY CONFLICTS AND ENVIRONMENTAL SAFETY

Akhundov R.G.
Military Scientific Research Institute, Baku, Azerbaijan

Environmental safety is a component of national security, which includes monitoring the state of the environment (natural resources, water, atmosphere, soil, flora and fauna) and the development of measures to prevent the occurrence of environmental crises and catastrophes that threaten the normal functioning of humans and society. Today, environmental disasters are perceived more as emergencies than as catastrophes provoked by violations of the laws of ecogenic and technogenic safety. Society has practically lost its sense of danger regarding the objectively brewing environmental catastrophe [1].

The most important environmental threats caused by the expansion of industrial and military activities of mankind are the depletion of the earth's ozone layer, atmospheric pollution, poisoning of water resources, an increase in the natural radiation background, the burial of waste from environmentally hazardous industries (including nuclear and chemical industries), the consequences of testing weapons of mass destruction (WMD) and weapons based on new physical principles [2].

The end of the twentieth century was characterized, on the one hand, by scientific, technological and information progress, and on the other, by a series of socio-economic crises, wars, and negative anthropogenic impact on the environment. The history of wars are also stories of the destruction of nature. One of the factors in the impact of wars on nature is the movement of significant masses of people, equipment and weapons.

The most significant thing in the development of weapons in the 20th century is that qualitatively new types of weapons appeared - those called weapons of mass destruction and weapons based on new physical principles [3-5].

Today, a number of ways to actively influence the environment for military purposes have already been created. For example, artificial destruction of the ozone layer, dispersion and formation of clouds and fogs, initiation of earthquakes, creation of tidal waves like tsunamis, impact on tropical cyclones, use of atmospheric currents to transport radioactive and other substances, creation of disturbance zones in the ionosphere. Each of them poses a danger both to the parties to the armed conflict and to other states.

Mankind turned out to be very inventive, creating more and more new types of weapons, accumulating an arsenal of means and technologies that can already today destroy the Earth's civilization. The nuclear confrontation may now be replaced by

a less visible but no less effective environmental confrontation. Which is primarily due to the development and emergence of weapons based on new physical principles.

Currently, we can distinguish the following types of weapons based on new physical principles, which, based on the results of their use, can be classified as environmental weapons:

1. Meteorological weapons. It affects atmospheric processes; uses atmospheric currents of radiation, chemical, bacteriological substances; creates zones of disturbances in the ionosphere and stable radiation belts; creates fires and firestorms; destroys the ozone layer; changes the gas composition in local volumes; affects atmospheric electricity;
2. Hydrospheric weapons. It performs the following functions: changing the chemical, physical and electrical properties of the ocean; creation of tidal waves such as tsunamis; pollution of inland waters, destruction of hydraulic structures and the creation of floods; impact on typhoons; initiation of slope processes;
3. Lithospheric weapons capable of triggering earthquakes; stimulate volcanic eruptions;
4. Climate weapons alter climate and temperature patterns in certain areas; destroy the underlying surface (soil and vegetation cover of the earth);
5. Biological weapons, which occupy a special place in the structure of these types of weapons, the use of which makes it possible to influence not only the biosphere, but also the human genotype.

A preliminary analysis comparing the consequences of conventional warfare with the results of modeling the "nuclear winter" effect allows us to conclude that, despite reductions in nuclear weapons, global environmental changes similar to those of the "nuclear winter" may occur in the course of conventional warfare and the use of environmental weapons destructive capabilities.

Maintaining and preserving environmental security in the face of military conflicts is not just an environmental imperative, but an essential component of global human security and well-being. As the international community copes with the challenges of the 21st century, strengthening the symbiotic relationship between peace, security and environmental protection will be of paramount importance. The call to action is clear: it is crucial to align our efforts to achieve peace with the principles of environmental conservation, ensuring a sustainable future for all.

References

1. Ali S. H., Pincus R. The role of the military in environmental peacebuilding //Routledge Handbook of Environmental Conflict and Peacebuilding. – 2018. – p. 306-314.

2. Lawrence M. J. et al. The effects of modern war and military activities on biodiversity and the environment //Environmental Reviews. – 2015, T.23, №. 4. – p. 443-460.

3. Fernandez-Lopez C., Posada-Baquero R., Ortega-Calvo J. J. Nature-based approaches to reducing the environmental risk of organic contaminants resulting from military activities //Science of The Total Environment. – 2022. – T. 843. – C. 157007.

4. Piriyev, H.K., Hashimov, E.G., Bayramov, A.A. Modelling of battle operations. Monograph. Baku: Military publishing house, 2016. 250 p

SOME ASPECTS OF APPLICATION OF COMPOSITE ELECTRET ELEMENTS WITH NANOPIEZOELECTRIC PHASE

Hasanov A.H., Talibov A.M.
National Defense University, Baku, Azerbaijan
Hashimov E.G.
Azerbaijan Technical University, Baku, Azerbaijan

Promptly obtaining coordinates about ground objects is one of the important tasks of Geographic Information Systems for solving various combat tactical tasks. This information can be used in high-precision combat correlation-extreme navigation systems [1]. Information about topographical elements of the area is obtained in various ways, including remotely using unmanned aerial vehicles (UAVs) [2,3]. The efficiency of using a UAV depends to a large extent on the duration of the autonomous flight, which is directly related to the capacity and stability of the UAV's power supply. Therefore, the creation of high-capacity electric batteries is a very urgent task. The paper presents the results of a study of the properties of an electret element based on fluorine-containing polymer matrices and a nanopiezoelectric phase of the lead zirconate-titanate family. Research shows that electrets made from compositions based on fluorine-containing thermoplastic polar polymers and ferropiezoelectrics are not stable. To increase the electret potential difference of these composites, technologies have been developed for producing electret materials with high stability, electret potential difference and dielectric. The essence of this technology is that the electret element with fluorine-containing polymer matrices is pre-crystallized under electric discharge plasma conditions. The results obtained show that the electret potential difference in the case of preliminary plasma crystallization of electret elements for all piezophase structures is noticeably greater than that of electret elements not crystallized by electric discharge plasma.

The conducted studies show that preliminary crystallization of the electret element based on fluorine-containing polymer matrices and the piezoelectric phase of the lead zirconate-titanate-lead family increases the magnitude of the electret potential difference and its stability. This allows it to be considered a promising material for use as a highly efficient and high-capacity energy source for unmanned aerial vehicles and seismic piezoelectric sensors for military purposes [4-7].

References

1. Hashimov E. G. About one method of navigation task solution //AHMC after H. Aliyev. Scientific Review. – 2013. – T. 1. – №. 20. – C. 45-49.

2. Hashimov E. G., Huseynov B. S. Some aspects of the combat capabilities and application of modern UAVs //Baku:"National Security and military knowledges.–2021.– №. 3. – p. 14-24. https://mod.gov.az//images/pdf/7440712d93276d13d09990c7a1e203ea.pdf

3. Bayramov, A.A., Hashimov, E.G.: Assessment of invisible areas and military objects in mountainous terrain // Defense Sciense Journal, **68**(4), 343–346 (2018). https://doi.org/10.14429/dsj.68.11623

INTEGRATION OF NEW TECHNOLOGIES INTO THE TEACHING METHODS OF ENGINEERING EDUCATION IN MILITARY INSTITUTIONS

Dadashov A.S.
Military Institute named after Heydar Aliyev, Baku, Azerbaijan

It is necessary to integrate new technologies into engineering education in military institutions to ensure that graduates are equipped with modern skills and knowledge. By utilizing these technologies, military engineering education offers more immersive and hands-on learning environments, preparing students for the complexities and technological advances of modern warfare. This highlights the importance of adapting teaching methodologies to match the evolving landscape of modern engineering education in military institutions.

Scientific activity in the Azerbaijan Army is a thoughtful, innovative and coordinated process of developing military science and using its results to improve the country's defense capabilities. The purpose of the scientific activity is to conduct research on the actual problems of military science, to organize an effective application of the obtained results to increase the development of the army and strengthen the national defense capability. Renewal of educational methods is aimed at the acquisition of military-scientific knowledge by military personnel and their adequate, scientific context and high level of practical skills for solving problems.The military science and education system plays a crucial role in the development of a strong and modern Armed Forces, which is the main feature of a sovereign state. In the Republic of Azerbaijan, military science and education serve as an important strategic field that ensures national security and defense [1-2]. Education and training in the Armed Forces aims to prepare the army for the performance of its functions, to respond to the specific needs of the military context, and as it is part of the national education system, it is subject to quality management procedures and evaluation [3]. Advances in science and technology are progressing faster every day than the previous day. As a result of these rapid changes in technology, the digitalized world with the concept of Industry 4.0 affects society at the same speed [4]. As digitization increases, it directly or indirectly shows its influence not only in social and industrial fields, but also in other fields. In the military industry, one of these areas, looking at the last 20 years period, it can be said that in the construction of the army, giving importance to digitalization both in the production process and in education is very important [5]. The occurrence of these processes has also had its effects on the military industry. Thus, the management of modern operations with the application of new technologies has already created the need to move to modern education and to integrate new technologies into the teaching methods of engineering education in military institutions, to use modern educational methods.

In conclusion, the integration of new technologies into the teaching methods of engineering education in military institutions is important to meet the demands of

a rapidly developing world. Thus, incorporating new technologies into engineering education in military institutions is critical to stay ahead in the ever-changing landscape of modern warfare.

References

1. Piriyev, H.K., Hashimov, E.G., Talibov, A.M. Some issues of pedagogical staff training for special-purpose higher education institutions // Military knowledge, 2014, No. 4, p. 3-9.

2.Agayev, S.O., Talibov, A.M., Hashimov, E.G. Modern pedagogical technologies in military education. Textbook. Part I. // - Baku: Military Publishing House, 2016, 152 p.

3. Barreiros dos Santos, L. A., Loureiro, N. A. R. S., do Vale Lima, J. M. M., de Sousa Silveira, J. A., & da Silva Grilo, R. J. (2019). Military higher education teaching and learning methodologies: An approach to the introduction of technologies in the classroom. *Security and Defence Quarterly*, *24*(2), 123-154.

4. Çaydere, O.,Akgün, N. (2023). EĞİTİMDE YENİLİKÇİ TEKNOLOJİLERİN KULLANIMI VE ÇAĞDAŞ İÇERİK TASARLAMA. *Stratejik Ve Sosyal Araştırmalar Dergisi*, *7*(2), 439-451.

5. Öztemel, E., (2018). Eğitimde Yeni Yönelimlerin Değerlendirilmesi ve Eğitim 4.0. Üniversite Araştırmaları Dergisi, 1(1), 25-30 https://doi.org/10.32329/uad.382041

COMPARATIVE ANALYSIS OF THE EFFICIENCY OF VARIOUS TYPES OF GRAVITATIONAL ENERGY STORAGES

Zulfugarov B.S.
National Defense University, Baku, Azerbaijan

The future of energy is associated with the massive use of energy storage devices. On an industrial scale, gravitational energy storage devices will most likely play a leading role [1-2]. Currently, about 10-12 different types of gravity storage devices are being built around the world, and therefore, there is a problem of choosing the optimal type of gravity storage device for use on an industrial scale [3, 4].

The choice of energy storage type is a pressing problem due to the need to transition to sustainable energy sources [5]. Differences in designs and technologies of gravity storage devices require comparative analysis to determine the most effective solutions [3, 6]. This will allow us to develop recommendations for choosing the optimal type of drive.

The study purpose is to conduct the most objective comparative analysis to determine the most effective type of gravity storage device for use on an industrial scale.

Such methods of scientific research as comparison, abstraction, axiomatic, analysis, synthesis, formalization and induction are use during the research. The research is conduct in two stages: 1) data collection 2) evaluation.

Sampling parameters for the study include different types of gravity storage devices, geographic diversity, and scale of projects. The technological and economic

features of each type of storage device are also take into account. A representative and diverse sample will allow for an objective comparison of the effectiveness of different gravity storage devices.

Preliminary results of the planned comprehensive study have shown that the effectiveness of various types of gravitational energy storage devices depends on the design, technological features and operating conditions. Some types, such as water lift mechanisms, are more effective in regions with available water resources. Economic analysis has shown that some storage tanks may be more expensive to build but are highly durable and efficient in the long term. The choice of the optimal type of gravitational energy storage device can be based on a comprehensive analysis of technological, economic and environmental factors, taking into account the specifics of the project and its location.

The research findings show that the choice of the optimal type of gravity storage depends on the operating conditions. The efficiency of different types of drives varies depending on the project. Such decisions require a comprehensive analysis taking into account economic and environmental factors in each specific case.

The study revealed that the efficiency of gravitational energy storage devices depends on their design, technological features and operating conditions. The optimal choice of storage type should be based on an analysis of specific factors, including economic and environmental aspects.

The study helps engineers and energy decision-makers select the most appropriate type of gravity storage for a given project. This allows you to optimize costs, increase efficiency and reduce negative environmental impacts.

References

1. Hasanov, A. H., Hashimov, E. G., Zulfugarov, B. S. Comparative analysis of the efficiency of various energy storages // Advanced Information Systems, – 2023, Volume 7, Number 1, – p. 74-80

2. Zulfugarov, B., Hasanov, A., & Hashimov, E. (2023). Comparative analysis of the efficiency of various energy storages. Modeling, Control and Information Technologies: Proceedings of International Scientific and Practical Conference, (6), 42–45. https://doi.org/10.31713/MCIT.2023.010

3. Berrada, A., Loudiyi, K., Zorkani, I. System design and economic performance of gravity energy storage // *Journal of Cleaner Production*, – 2017, Volume 156, – p. 317-326

4. Chen, K. Types, applications and future developments of gravity energy storage // *Highlights in Science Engineering and Technology*, – 2022, Volume 3, – p. 23-30

5. Tong, W. Solid gravity energy storage: A review / W. Tong, Z. Lu, W. Chen [et al.] // *Journal of Energy Storage*, – 2022, Volume 53, – p. 1-30

6. Abdmouleh, Z., Alammari, R. A. M., Gastli, A. Review of policies encouraging renewable energy integration & best practices // *Renewable and Sustainable Energy Reviews*, – 2015, Volume 45, – p. 249-262

ECOCIDE IN THE NAGORNO-KARABAKH CONFLICT: AN ANALYSIS OF ARMENIA'S ENVIRONMENTAL IMPACT ON AZERBAIJAN

Akhundov R.G.
Military Scientific Research Institute, Baku, Azerbaijan

The Nagorno-Karabakh conflict between Armenia and Azerbaijan has had devastating effects not only on the human population but also on the environment. This thesis explores the concept of ecocide as it relates to the conflict, focusing on Armenia's actions and their environmental impact on Azerbaijan. Ecocide, defined as the extensive damage to, destruction of, or loss of ecosystems of a given territory, poses serious challenges to the affected region's ecological balance, biodiversity, and long-term sustainability [1]. Terrorist acts aimed at disrupting the ecological balance in any state are part of the ecocide and pursue the goal of creating environmental problems. The main purpose of the Prevention of environmental terrorism is to ensure the environmental safety of the population, protect the environment and prevent the loss of living beings. Damage caused by any country or persons deliberately by harming the nature, flora and fauna of another country and destroying its natural resources is considered ecological terror.

Starting from 1988, the war started against Azerbaijan by the Armenians and the forces supporting them, resulted in the occupation of our lands for nearly 30 years, the destruction of cities and villages, the genocide of the peaceful population, and at the same time, the destruction of flora and fauna. Since the military conflict and war were conducted only on the territory of the Republic of Azerbaijan, the atmosphere, water sources and our lands were exposed to biological, chemical and physical pollution. For nearly 30 years, Armenia has caused a huge amount of irreparable damage to the natural resources and natural environment of the occupied territories. As a result of the patronage of the occupying state, the natural resources of the occupied territories were illegally exploited and looted by various companies. The damage caused to the surrounding natural environment of these territories caused a violation of the ecological balance in the region. Our occupied settlements were plundered by Armenian Armed Forces, houses were destroyed, water, electricity, gas and other communication lines were completely destroyed [2-4].

Railway lines of Republican importance were dismantled and rendered useless. In general, the territories of Azerbaijan, which have been subjected to environmental terror by Armenia, have become a regional ecological disaster zone.

The international normative legal documents and laws on the protection of the natural environment in the territories occupied by the armed forces of Armenia have not been followed. Thus, during the monitoring in the liberated territories, the facts of plundering of our natural resources, cutting down of perennial valuable trees in the forests (the personnel of the Armed Forces of Armenia and the military equipment belonging to it were used in their transportation) were revealed.

As a result of the enemy's placement of military units and military equipment in combat positions, the construction of engineering fortifications and access roads for the purpose of maneuvering personnel and equipment, the cutting down of trees

and bushes during soil excavation, the burning of pastures, etc., serious damage was caused to the flora and fauna. The work carried out by the enemy army in these areas should be assessed as an environmental terrorist act that led to the destruction of the nature of Azerbaijan. The Nagorno-Karabakh conflict has not only caused immense human suffering but has also resulted in severe environmental degradation. Armenia's actions in the conflict, including the deliberate destruction of natural resources, can be classified as ecocide. It is imperative for the international community to recognize and address the environmental dimensions of the conflict, ensuring that those responsible for ecocide are held accountable and that efforts are made to restore the damaged ecosystems.

References

1. Darbyshire E., Weir D. Environmental dimensions during and after the Nagorno-Karabakh conflict of 2020 //Integrated Environmental Assessment and Management. – 2023. – Т. 19. – №. 2. – p. 360-365.

2. Piriyev, H.K., Hashimov, E.G. The Second Karabakh War: military-political and military-technical aspects // - Baku: Proceedings of the Military Institute named after Heydar Aliyev, - 2023. No. 1 (40). - p. 7-16.

3. İmrani Z.T. et al. Economic and social conditions of frontline area population of the Goranboy district and perspective progress directions //National Security and Military Sciences. – 2018. – Т. 4. – №. 4.

4. İmrani, Z., Hashimov, E.G. Bayramov, A.A., Djafarova, N.R. Employment problems of the population in Fizuli region of the Republic of Azerbaijan // Регіон – 2020: стратегія оптимального розвитку: матеріали міжнародної науково-практичної конференції (м. Харків, 8 – 9 жовтня 2020 р.) / Гол. ред. колегії Л.М. Нємець. – Харків: ХНУ імені В.Н. Каразіна, 2020. с.9-12

PROVISION OF MULTICULTURAL SECURITY AS A PRIORITY OF THE AZERBAIJANI STATE

Qambarov B.A., Kerimova D.D.
Military Institute named after Heydar Aliyev, Baku, Azerbaijan

The existence of a normal multicultural mood in Azerbaijan - the living of different confessions and ethnic groups in conditions of friendship and friendliness is still nourished from the ancient times of history. Multiculturalism emerged as a state policy in the Republic of Azerbaijan at the time when the failure of multiculturalism as a political line was declared in a number of Western countries, in the same France, England, and Germany. Compared to Western European countries, Azerbaijan has little real experience in the field of democratic development. But his spiritual experience is great [1]. The traditions of multiculturalism in Azerbaijan are based on deep historical roots: "Thus, Turks, Talysh, Tats, Udins, Ingiloys, Kurds, Lezgis, Russians, who combine different traditions, cultural values, language and religious beliefs in different regions in the territory of Azerbaijan since ancient times. Jews, Turks and representatives of other ethnic groups live together in conditions of

friendship, mutual understanding and tolerance [2]. Today, the new, democratic society formed in Azerbaijan actively participates in the building of an independent state. His national identity does not prevent him from feeling like an Azerbaijani today. He can speak, write and fulfill his cultural needs in his native language. Article 44 of the Constitution of Azerbaijan entitled "The right to nationality" states: "Everyone has the right to preserve his nationality. No one can be forced to change his nationality" [3]. Representatives of different nations living in Azerbaijan can be seen today in every field of independent Azerbaijan - in politics, economy, education, sports, spiritual life, in short, in all fields. One important principle of multicultural security is the provision of support by the state and society for the development of cultural diversity in the country. Multicultural security principles are as important and necessary as the principles of other security doctrines for countries like Azerbaijan, which are small but have deep roots and history. The establishment of the principles listed here in Azerbaijan was possible as a result of the joint effort and work of the citizens of Azerbaijan. The prevention of foreign ideological interventions and the weakening of subversive tendencies to a minimum depends on the implementation of these principles. As we get closer to the ideological goal clearly indicated by the great leader, the world knows us more adequately and learns with more interest. This means the strengthening of loyalty to Azerbaijan in various places.

The unique qualities of multiculturalism in Azerbaijan suggest that, since time immemorial, people living in these areas with different ethnic, religious, and traditional backgrounds live in conditions of mutual understanding and friendship and form a single Azerbaijani nation, as well as its national unity, tolerance, rich culture, and hospitality, were able to create a national ideology [2]. During the war, there were many attempts to break the multicultural environment in our country and discriminate. External and internal forces aimed to prevent the society from united struggle by using this factor. But when they saw that this did not happen, they were once again convinced that it is simply impossible to somehow violate the values and principles that have been formed for centuries, and to create discord between peoples. The people of Azerbaijan clearly demonstrated their unity, their unity, and their ability to unite around their state in the Second Karabakh War: regardless of their religion and nationality, everyone had only one action in their thoughts - to fight for every inch of Azerbaijan's land and to take our occupied lands. liberate. With this, our people demonstrated to the whole world that they are ready for everything to strengthen and strengthen the state of Azerbaijan.

References

1. Abdulla, K. Azerbaijan multiculturalism / K.Abdulla. - Baku: BBMM, 2017. - 421 p.

2. Huseynov, R. "Kharibulbul" festival demonstrated our people's commitment to the values of multiculturalism: [Electronic resource], URL: https://ikisahil.az/post/219273-xaribulbul-festivali-xalqimizin-multikulturalizm-deyerlerine-sadiğliyini-numayish- made-sherh

3. Constitution of the Republic of Azerbaijan // adopted on November 12, 1995 (amendments and additions on August 24, 2002, March 18, 2009, September 26, 2016). - Baku: Law, - 2016, - p. 48

MODERN EDUCATIONAL METHODS AND THE EFFECTIVENESS OF THEIR APPLICATION IN MILITARY EDUCATIONAL INSTITUTIONS

Mammadova M.F., Nasirov E.V., Gullarli G.H.
Military Institute named after Heydar Aliyev, Baku, Azerbaijan

The model of application of modern teaching methods in special educational institutions is considered as the main goal for the educational systems of many countries [1-3]. In the current period, the application of interactive and immersive teaching methods to the educational process supposed as a method that serves to increase the interest of the young generation in education. The application, development and connection of these methods with modern technologies pose important tasks to educational institutions. Because the old rules and methods of training cannot satisfy the requirements of technical progress, which the modern youth is entering [4-5]. The complexity of the specified problem makes its study relevant. From this point of view, the methods of interactive and immersive learning are explained in detail in the article, the main tasks facing the educational process are analyzed and studied. In particular, it was given the advantages and disadvantages of these teaching methods.

The following qualities will be developed in cadets while using the mentioned methods in the lessons conducted as a result of the research:

1. Development of critical thinking. Learners must analyze the work of other learners to evaluate it against criteria, which helps develop critical thinking.

2. Development of assessment skills. Trainees learn to evaluate work against predetermined criteria and standards, which helps them develop their evaluation skills.

3. Increasing responsibility. When trainees know that their work will be evaluated by other trainees, they feel more responsible for their work.

4. Increasing motivation. Trainees may feel more motivated when they know that their work will be evaluated by other trainees.

5. Evaluation effectiveness. Peer evaluation by students can be more effective than teacher evaluation alone, as it allows for a more detailed analysis of the work from different perspectives.

Let's note that we have shown the positive and negative aspects of interactive and immersive technologies in the section. Apparently, the positive effect of using such modern methods is more than its disadvantages. Most of the shortcomings can be solved during the course of teaching.

Interactive and immersive education and training methods are an effective way of absorbing information and are best used by combining different tools. According to experts, such an innovative solution should form the basis of the current curriculum of many educational institutions. Without them, it will be more difficult for students to achieve high academic performance.

References

1. Cebrián, G.; Junyent, M.; Mulà, I. Competencies in Education for Sustainable Development: Emerging Teaching and Research Developments. Sustainability 2020, 12, 579.

2. Albareda-Tiana, S.; Vidal-Raméntol, S.; Fernández-Morilla, M. Implementing the Sustainable Development Goals at University level. Int. J. Sustain. High. Educ. 2018, 19, 473–497. [CrossRef]

3. Elmassah, S., Bacheer, S. M., & James, R. (2020). What shapes students' perceptions of group work: personality or past experience?. *International Journal of Educational Management*, *34*(9), 1457-1473.

4. Piriyev, H.K., Hashimov, E.G., Talibov, A.M. Some issues of pedagogical staff training for special-purpose higher education institutions // Military knowledge, 2014, No. 4, p. 3-9

5. Agayev, S.O., Talibov, A.M., Hashimov, E.G. Modern pedagogical technologies in military education. Textbook. Part I. // - Baku: Military Publishing House, 2016, 152 p.

TEACHING INNOVATION IN COMPUTER EDUCATION

Mamedova M.F.
Military Institute named after Heydar Aliyev, Baku, Azerbaijan

The computer technique presents quickly developing trend, especially in the network security, the Multi-Media technique and in the artificial intelligence domain, this trend drives the development of the computer education quickly. How to carry on professional education and quality education for undergraduates of the department of computer science & technology, how to do a good teaching for the computer course, it is already an urgent affair and has impormant meaning.

Outstanding Teaching Problems at Present. A criticism often heard these days is that subjects taught in universities tend to be too academic, and contribute liitle to preparing a young person for the real-tasks he or she will have to perform after graduation.

Traditional Computer teaching in universities makes theory divorce from practice, it is a common problem that undergraduates makes theory divorce from practice. It is a comon problem that undergraduates, have inferios operational capacity undergraduates see computer as a course instead of skills, this phenomenon leads to low practical ability.

References

1. Bialystok, E. (2001). Bilingualism in development: Language, Literacy and Cognition. Cambridge: Cambridge University Press.

2. Piriyev, H.K., Hashimov, E.G., Talibov, A.M. Some issues of pedagogical staff training for special-purpose higher education institutions // Military knowledge, 2014, No. 4, p. 3-9

3. Cummis, J (2000) Language, Power and pedagogy. Clevedon: Multilingual Matters.

4. Agayev, S.O., Talibov, A.M., Hashimov, E.G. Modern pedagogical technologies in military education. Textbook. Part I. // - Baku: Military Publishing House, 2016, 152 p.

5. Piriyev, H.K., Hashimov, E.G., Hasanov, A.H. Provide interactive training methods. Methodological materials // - Baku: Military publishing house, 2016, 33 p.

6. Piriyev, H.K., Hamidov, M.P., Hashimov, E.G. Training methods in military education. Methodological materials // - Baku: Military publishing house, 2017, 52 p

THE ROLE OF NAVIGATIONAL AND HIDROGRAPHICAL SUPPORT IN ENSURING SECURITY OF THE CASPIAN SEA

Rustamov A.R., Mammadzada V.M., Hashimov R.İ.
National Defense University, Baku, Azerbaijan

The rich hydrocarbon resources of the Caspian Sea and the efforts of the Caspian littoral countries to take advantage of these rich hydrocarbon resources in accordance with their national interests already come to the fore as the main factor affecting its security environment.

Western countries are increasing their efforts to protect their interests in the region. In particular, it should be mentioned that according to the forecasts of the European Union (EU), the use of natural gas continues to increase year by year [1].

In terms of factors affecting the security environment in the Caspian region, the lack of action in taking necessary measures to ensure safe shipping [2. p.2].

This, in its turn, determines the necessity to increase the efficiency of navigational and hydrographical support in the existing transportation routes in the Caspian Sea.

For the purpose of providing to ensure the safety of free navigation of ships have been proposed to place bouy number 4 at the coordinates Lat=39^0 48,0' N; Lng=49^0 53,6', to connect the reccomended road number 8 with the cources 179^0,5 - 359^0,5 by making it 1,4 nautical miles wide and reciprocal lined to the bouy number 1's circular traffic system indicating the beginning of the fairway, to establish the fairway with cources 270^0,0 - 90^0,0 having reciprocal lines, 1.4 nautical miles wide and running 78 nautical miles to the East, to place bouy number 5 at the end of it.

Among the numerous works to be done in connection with increasing the effectiveness of navigational support, issues of hydrographical support should also be brought to the fore [3].

As a conclusion of the research carried by the method of analysis and synthesis, and the experience gained during the long-term service, the necessity to make changes in the traffic seperation scheme, fairways, and recommended roads is confirmed.

References

1. IEA-International Energy Agency. Baseline European Union gas demand and supply in 2023. – [Electronic resource] // – January 2021, pp. 12-14. URL: https://www.iea.org/reports/how-to-avoid-gas-shortages-in-the-european-union-in-2023/baseline-european-union-gas-demand-and-supply-in-2023

2. Zelenkov M. Maritime terrorism as a threat to confidence in water transport and logistic systems // M. Zelenkov, Y. Laamarti, M. Charaeva, T. Rogova, O. Novoselova, A. Mongush. – [Electronic resource] // – June 2022, pp. 2-33. URL: file:///C:/Users/AdMin/Desktop/1-s2.0-S2352146522005117-main.pdf

3. Vaqif Bayramov. Why is the water of the Caspian drawn? // [Electronic resource] – 25.07.2023. // URL: https://xalqqazeti.az/az/ekologiya/133575-xezerin-suyu-niye-cekilir

MODELING THE EFFECT OF ELECTROMAGNETIC RADIATION ON THE HUMAN HEAD

Hasanov A.H.
Military Research Institute of the National Defense University, Baku, Azerbaijan
Islamov I.J.
Military Research Institute of the National Defense University, Baku, Azerbaijan
Baku Engineering University, Baku, Azerbaijan

The effects of cell phones on the body are still being studied. Scientists are trying to determine the harm caused by long-term use of the devices. However, it is already known that even short-term exposure can cause harm. Phones emit more energy during calls, and the strength varies depending on the quality of the signal.

The dangers and illnesses associated with being near sources of microwave electromagnetic fields depend on several factors: distances between the source and the person; duration of exposure; radio frequency range; intensity of impact; sensitivity of the body to the effects. Exposure to electromagnetic fields is partially absorbed by body tissue, creating high-frequency currents and heat. Therefore, the stronger the impact, the more damage it can cause. Long-term exposure may cause fatigue, headaches, problems with sleep and heart health. High frequency fields can also cause cataracts, thyroid enlargement, and blood and hair problems.

Mobile operators use the GSM 900 standard system: the operating frequency range of base stations is 925...965 *MHz*, mobile radiotelephones - 890...915 *MHz* and the GSM 1800 standard: 1805...1880 *MHz*, 1710...1785 *MHz*, respectively. The antennas of the base stations of the cellular communication system, which are used by mobile operators, emit power in the range of 8...16 *W*. They are placed on the roofs of houses, chimneys, etc. or on special masts at heights of 30...35 *m* above the ground. These antennas have circular radiation patterns in the horizontal plane and sharp ones in the vertical plane, inclined to the horizontal at an angle of 1...2 degrees, having the shape of an umbrella [1].

A mobile radiotelephone is a small-sized transceiver. Its radiation power (in transmission mode) is in the range of 0,1...1,0 *W*. It is a variable quantity and depends on the state of the communication channel "mobile radiotelephone – base station", that is, the stronger the base station signal at the receiving point, the lower the radiation power of the mobile radiotelephone. However, in real conditions, as experience suggests, on average it does not exceed 0,25 *W* when working in a populated area in an open area.

The radiation emitted by the mobile phone in standby mode is quite weak. But its main radiation is during incoming and outgoing calls. The radiation emitted by the mobile phone is absorbed by the body. The radiation level of a mobile phone is measured based on the specific absorption coefficient - *SAR* (Specific Absorption Rate). This indicator shows the amount of radiation absorbed by the human body. The power of an electromagnetic wave passing through 1 *kg* of human weight (*W*) is called Specific Absorption Rate (*SAR*) and is defined as follows [2]:

$$SAR = \frac{\sigma |E|^2}{\rho}, \frac{W}{kg}, \quad (1)$$

where σ - conductivity of the material in a given volume, Sm/m; E - field intensity, V/m; ρ - density, kg/m^3.. The power flux density of the electromagnetic field P emitted by the antenna is calculated by the formula:

$$P = \frac{P_1 G}{4\pi r^2} F(\theta) \cdot F(\varphi) \cdot n, \quad (2)$$

where P_1 is the radiation power of the antenna, G is its gain, $F(\theta)$ and $F(\varphi)$ are the normalized directivity functions of the antenna, r is the distance in free space between the antenna and the observation point, which is located in the far zone of the antenna field, k is reflection coefficient module.

According to the formulas (1) and (2) given above, the graph characterizing the distribution of the *SAR* parameter in the layers of the six-layer human head model at the more common frequencies of 450 *MHz*, 900 *MHz* (GSM) and 1800 *MHz* (GSM) is shown in Figure 1. During the calculation, the values of the angles φ and θ were taken equal to 0.

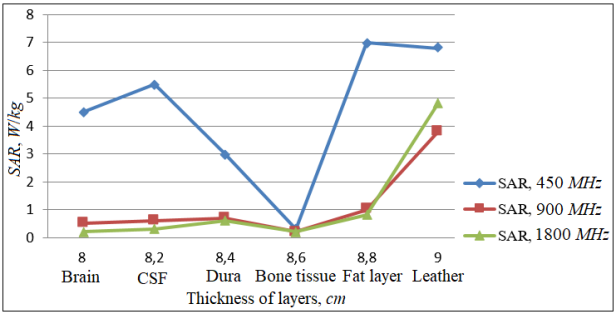


Figure 1. Distribution of SAR across layers of the model

As can be seen from Figure 1, for all frequency bands, the SAR value is higher in the area of the first layer of the structure (Leather layer). In addition, as the operating frequency increases, SAR and electric field voltage values decrease in the inner layers of the structure.

References

1. Hasanov A. H., Hashimov E. G. Analysis of the effectivness of communication and automated management systems //Modern directions of development of information and communication technologies and management tools, Abstracts of reports of the 12th Int. Scientific and Technical Conf. – 2022. – T. 1. – p. 1-4.

2. Abdul-Al, M.; Amar, A.S.I.; et al. Wireless Electromagnetic Radiation Assessment Based on the Specific Absorption Rate (SAR): A Review Case Study. Electronics 2022, 11, 511. https://doi.org/10.3390/electronics11040511.

MATHEMATICAL ASPECTS OF IDENTIFICATION OF MOVING TECHNIQUE

Umudov S.U., Karimov E.Y.
Military Institute named after Heydar Aliev, Baku, Azerbaijan
Talibov A.M.
Military Scientific Research Institute, Baku, Azerbaijan

The report deals with the mathematical formalization of the task of identifying heavy armored vehicles that are stealthily moving in mountainous terrain.

Detection, localization and identification by ground means of unobserved heavy armored vehicles moving several kilometers away in mountainous terrain is one of the urgent tasks of military science. Many works [1–4] are devoted to the solution of these questions.

In this work, the problems of identification of covertly moving armored vehicles with the use of a seismic station are considered [5-7]. The algorithm for determining the course and coordinates of the movement of armored vehicles is also considered.

The main purpose of the work: to develop an algorithm for identifying and determining the course of unobserved heavy armored vehicles moving in mountainous terrain at a distance of 3-5 km.

The analysis of seismoacoustic signals formed in solid ground during the movement of cars, the flight of helicopters and airplanes was performed. The developed algorithm for determining the course and coordinates of the movement of armored vehicles

References

1. Bayramov, A.A., Hashimov, E.G.: Assessment of invisible areas and military objects in mountainous terrain // Defense Sciense Journal, 68(4), 343–346 (2018). https://doi.org/10.14429/dsj.68.11623
2. Hashimov E. G. et al. Determination of the bearing angle of unobserved ground targets by use of seismic location cells //2017 International Conference on Military Technologies (ICMT). – IEEE, 2017. – С. 185-188.
3. Bayramov A. A. et al. The detection of invisible objects on the terrain on the basis of GIS technology // Geography and nature sources. – 2016. – С. 124-126.
4. Hashimov E. G., Bayramov A. A. Detection unobserved moving armored vehicles by seismic method //National Security and Military Sciences. – 2015. – Т. 1. – №. 1. – С. 128-132.
5. Bayramov A., Hashimov E. Seismic location station for detection of unobserved moving military machineries //Journal of Management and Information Science. – 2016. – Т. 4. – №. 2. – С. 61-66.
6. Hashimov E.G., Bayramov A.A. Application of GIS and seismology methods for detection of invisible military objects. Monograph//- Baku: Military publishing house, 2017, 246 p.
7. Piriyev, G. K. et al. Modelling of the battle operations. Monograph // H.K.Piriyev, E.G.Hashimov, A.A.Bayramov / -Baku: Herbi Nashriat. – 2017. -256 p.

DETECTION AND PRACTICE OF WRITING DISORDERS FOR SPECIAL EDUCATION STUDENTS

Jayhoon Dehqanzada,
Istanbul University-Cerrahpasa, Istanbul, Turkey
Hasanli R.A.
Sumqayit State University, Sumqayit, Azerbaijan

There is a general consensus that education is a force that determines individuals' life trajectories and is a fundamental right for every person. This view, expressed by Himmetoğlu Shikhkamalova and Shikhkamalova [1], emphasizes that education is not only a privilege but also a necessity. From this perspective, Bağ [2] states that one of the primary goals of national education systems is to provide equal learning opportunities for every student. In addition to the points highlighted by Bağ, it has been mentioned that standard educational services may be inadequate for students with special education needs, and therefore, the development of customized education programs tailored to these students' needs is critical [2]. The transformative role of technology in education processes necessitates a shift from traditional approaches to more contemporary and comprehensive methodologies in education systems due to its potential to enrich educational and learning experiences [3].

Education is defined as the process of bringing about desired changes in behavior [4], and special education is accepted as a process that helps overcome barriers to maximize an individual's potential and integrate them into society [5]. In the information age, educating every individual in accordance with the requirements of the age and accepting them as part of society, especially for students with special education needs, should become a fundamental goal of receiving quality education.

Literature review reveals that special education is a significant field aimed at providing personalized education for individuals with different learning needs.

The primary goal of this project is to provide an interactive and comprehensive learning platform for students with special education needs. This system allows teachers to create their own classes and add students to these classes. Additionally, school administrators can register families and their children in the system. Families can choose one of two methods to log into the system: 1) Username and password 2) A link sent by the teacher every 30 days.

Teachers can create their own resource lesson content according to the lesson category. This system allows for the creation of resources such as puzzles and writing exercises. For puzzle resources, teachers will add four images according to the category. For writing resources, teachers will record the letters or words they want to teach students into the system.

Teachers can thus create their own lesson content resources and share these resources with other teachers through a special code. The shared resource usage is designed to turn a resource into multiple test questions. When defining a test for a class, teachers can include the image for a puzzle or the letters or words for writing by simply clicking, based on the resource category.

Students registered in classes can solve the tests created by the teacher. During this process, the student's parent will log into the system using the login methods, access the class the child is registered in, click on the test to be solved, and start the test solution. After solving the test, applause and visuals will be displayed to motivate the students. In puzzle tests, images will be randomly presented to students, and students will click on the image to rotate it to correctly assemble the picture. In writing tests, the letters or words included in the test by the teacher will be written on the screen in order, and students will try to write over them by following the text on the screen. If the speaker button on the screen is clicked, the letter or word will be pronounced, and students can use an eraser to delete the parts they get wrong. Tools will be provided to enlarge the writing font, and students will be prevented from drawing on parts of the screen that are outside a certain margin of error. This error-free learning method will serve the purpose of teaching writing.

Teachers can closely monitor students' performance through a comprehensive reporting system that keeps detailed information on how much time a student spends on each test. The time a student spends on each test is an important component of this process and provides valuable insights to teachers about the student's learning speed and depth of understanding.

The reporting system is designed to allow students to observe their progress on a class basis, test basis, and even on an individual question basis. The detailed and layered reporting enables both the family and the teacher to effectively monitor the student's development.

This system focuses on improving students' writing and puzzle-solving skills while also offering them the opportunity to learn from their mistakes and convert them into corrected behaviors. Allowing students to solve a test multiple times emphasizes the importance of flexibility and repetition in the learning process. By enabling students to progress at their own pace without the requirement of class attendance, individual learning paths are supported. These features detail how the project specifically responds to the needs of special education students and plays an empowering role in their educational journeys.

References

1. Himmetoğlu, B., Shikhkamalova, V., & Bayrak, C. (2022). Problems faced by special education teachers and the role of school administrators in solving these problems. *Trakya Education Journal*, 12(3), 1597-1618.

2. Bağ, L., & Namdar Oğuz. (2021). Examination of the use of creative drama in classes by special education teachers [Master's thesis, Rize-Recep Tayyip Erdoğan University]/

3. Ficarra, F. V. C. (2010). Educational games and communicability: Design, learning, and interactive applications. In F. Edvard & H. Kulle (Eds.), *Educational games: Design, learning, and applications (pp. 37-75)*. Nova Science Publishers

4. Ertürk, S. (1972). *Program development in education*. Yelkentepe Publications.

5. Ataman, A. (2003). *Special needs children and introduction to special education (2nd edition)*. Gündüz Education and Publishing

DEVELOPMENT OF AN AUTOMATED UNMANNED PERİMETER PROTECTİON SYSTEM

Suleymanov S.S.
Institute of Geology and Geophysics, Baku, Azerbaijan
Bayramov A.A.
İnstitute of Control Systems, Baku, Azerbaijan
Abdullayev F.N.
Republican Seismic Survey Center, Baku, Azerbaijan

The most effective method is an automated control, which is carried out remotely. Such control can be carried out around the clock, in any weather, at any area and distance. Here the human factor plays a minimal role, so the probability of error is minimized here [1-3].

This paper presents the developed unified automated unmanned system for remote control of a given territory and access protection. Seismic sensors, acoustic sensors, fuses, video observation blocks, etc. can serve as remote sensor units that are activated by coded radio signals. The advantage of this unmanned system is that it is controlled by coded signals, the frequency and control protocol of which are set by the developers, so this system is safe and not available to a third party [4,5].

The purpose of the report is to present the results of the development, preparation and preliminary laboratory and field tests of the security system working in the telemetry mode. The working principle, management, operation rules, management and telemetry of the security system were explained. Cryptographic coding based on the Neyman algorithm was used to encrypt the telemetry of the security system. During 100 laboratory and field tests of the security robotic system, no violations of the system's operation mode were observed.

References

1. Sundhararajan M., Gao X., Nejad H. Artificial intelligent techniques and its applications. Journal of Intelligent & Fuzzy Systems, 34 (2018), pp. 755–760.
2. Bajaj, S., Bopardikar, S., Moll, A., Torng, E., Casbeer., D.: Perimeter Defense using a Turret with Finite Range and Service Times. arXiv:2302.02186v1 [eess.SY] 4 Feb 2023
3. Guerrero-Bonilla, L., Nieto-Granda, C., Egerstedt, M.: Robust Perimeter Defense using Control Barrier Functions. In 2021 International Symposium on Multi-Robot and Multi-Agent Systems (MRS). IEEE, pp. 164–172. (2021).
4. Bayramov A. A., Hashimov E. G. Assessment of invisible areas and military objects in mountainous terrain //Defence Science Journal. – 2018. – Т. 68. – №. 4. – p. 343-346
5. Bayramov A., Hashimov E. Seismic location station for detection of unobserved moving military machineries //Journal of Management and Information Science. – 2016. – Т. 4. – №. 2. – С. 61-66.
6. Hashimov E. G., Bayramov A. A. Detection unobserved moving armored vehicles by seismic method //National Security and Military Sciences. – 2015. – Т. 1. – №. 1. – С. 128-132.
7. Hashimov E. G. et al. Determination of the bearing angle of unobserved ground targets by use of seismic location cells //2017 International Conference on Military Technologies (ICMT). – IEEE, 2017. – p. 185-188.

VEHICLE TRANSPORT COST CALCULATION METHOD

Talibov A.M.
Military Scientific Research Institute
Hashimov E.G.
Azerbaijan Technical University, Baku

The dependence of the efficiency of vehicle cargo transportation on a large number of parameters makes it difficult to determine the criteria for optimizing transportation in this area. However, experience shows that among these factors, the determination of transportation costs is one of the main factors [1-4]. The transportation process of cargo transportation consists of elements that are repeated in sequence. Together, these elements are called the transportation cycle as the completed operation of cargo delivery. Calculation of transport costs during the execution of the transport cycle mainly consists of the sum of car depreciation, consumption of fuel and lubricants, maintenance and repair costs. Calculation of 11 types of cost items was carried out for the calculation of transport costs in cargo transportation. In the methodology, the cost incurred during the journey of 1 car for a distance of 1 km is determined. Transportation costs in military vehicle cargo transportation can be calculated using the following expression:

$$X_{1km} = Y_x + M_{yx} + T_{yx} + P_{yx} + X_{yx} + A_x + S_x + AT_x + E_{TX} + E_{OT} + E_{MR} .$$

Here, Y_x fuel consumption price, M_{yx} motor oil consumption price, T_{yx} transmission oil consumption price, P_{yx} plastic oil consumption price, X_{yx} special oil (fluid) consumption price, A_x car battery maintenance costs, S_x tire maintenance costs, AT_x car amortization costs, E_{TX} the share of technical service costs per 1 km during the car's operation, E_{OT} the share of the average repair costs per 1 km, E_{MR} the share of the major repairs per 1 km.

As can be seen from the above-mentioned statements, the maintenance and operation costs spent on freight transportation were maximally taken into account in the calculation of transport costs. Using these expressions, a description of the mathematical formulation of the problem of calculation of transport costs in military cargo transportation and a block diagram of the algorithmic process were prepared.

1. References

2. Talibov A.M., Guliyev B.V. A method for assessing the military-economic indicators with the purpose of locating a logistics center for redeploying troops // Advanced Information Systems. 2021. Vol. 5, No. 2. doi: https://doi.org/10.20998/2522-9052.2021.2.23

3. Bayramov, A. A., Talibov, A., Pashaev, A., & Sabziev, E. (2019). Математическая модель логистики технического снабжения в зонах военных действий. *Сучасні інформаційні технології у сфері безпеки та оборони*, *35*(2), 77-80.

4. Talibov A. et al. Optimal placement of logistics centers in the Republic of Azerbaijan //2nd International Conference on Problems of Logistics, Management and Operation in The East-West Transport Corridor (PLMO 2023).–Baku: may.– 2023.–p. 24-26.

5. Talibov A. M. et al. On the optimal placement of logistics centers //Baku: Informatics and Control Problems. – 2023. – №. 43. – С. 51-58.

THE IMPACT OF THE WAR AGAINST UKRAINE ON RUSSIA'S INTERNATIONAL IMAGE

Huseynov R.S., Asgerov G.R., Esedov F.M.
Military Institute named after Heydar Aliyev, Baku, Azerbaijan

Russia, the successor of the USSR, continued its imperialist interests and carried out its occupation policy against its neighbors (mainly post-Soviet countries) (Georgia, Moldova, etc.) not only caused the disruption of interstate relations, but also the increase of citizens' hatred towards it.

It seems that the inability to govern people in a democratic, legal way and to ensure social justice increases the tendency towards totalitarian regimes.

Those who think that it is impossible to live within the framework of mutual understanding, national interests, and friendship with the states try to find a way out by uniting them in the form of an empire to make them dependent on themselves.

For this, by sending troops into the territory of a neighboring country like Ukraine, violating its sovereignty and territorial integrity, occupying its territory, ordering the killing of tens of thousands of innocent people, it is a gross violation of the law and a crime against humanity [1].

The war of aggression against Ukraine increased the already existing hatred of Russia, the successor of the USSR, in the society. The fact that the citizens rose to the struggle and united against Russia once again showed that they are tired of Russia.

The local population considers the Russian authorities, which are still trying to preserve the principles of the former Soviet-totalitarian society and imperial thinking, to be a great danger and threat to them.

Shortly after the start of the war, Ukrainian President Volodymyr Zelensky signed the law on the de-Sovietization of legislation once again showed that Ukrainians wanted to completely rid themselves of the remnants of Soviet thinking.

Because both the state and the society understood well that the Soviet way of thinking still remains as a certain cause of economic-social-political problems [2].

Due to the fact that the processes continued for a long time, citizens of other post-Soviet republics, such as Ukrainians, began to see Russia as the culprit of their problems. Even this situation is developing to the level of contempt in many cases.

Despite being superior many times, the weakness of its economic capabilities, backwardness in terms of military technology, the inability of the army to make an effective impact in terms of modern requirements, and the military's traditional way of conducting war, and the inability to apply a modern approach, hinder the victory that Russia wants to achieve.

It is true that the indirect participation of the Western countries, including NATO, in the war against Russia, their support for Ukraine, and the deadly sanctions they imposed against Russia had their effect. This had a great impact on Russia's economic weakening as well as serious losses on the military front [3].

Although Russia's natural and economic resources allow it to resist these sanctions, even for a certain period of time.

But it can be thought that no one doubts that Russia, which is unable to fully ensure its economic security and depends on exports in many cases, will face economic difficulties in the next period.

If we take into account the fact that the NATO countries once again declared their condemnation of this aggression against Ukraine, the introduction of a new package of economic sanctions, followed by the fact that they will provide new support to Ukraine, it shows that the war will continue in the coming months [4].

This situation makes it inevitable that not only Ukrainians, but also ordinary citizens who bear the impact of sanctions will expand their protests, increase dissatisfaction between the government and the people, and disrupt political stability.

References

1. Huseynov, R. This increased hatred of Russia, the successor of the USSR [Electronic resource] /Demokrat.az. URL: https://demokrat.az/az/news/110152/bu-ssri-nin-davamcisi-rusiyaya-qarsi-nifreti-daha-da-artirdi

2. Юрченко, Н. Зеленский подписал закон о десоветизации украинского законодательства. [Електронний ресурс] / RBC. URL: https://www.rbc.ua/rus/news/zelenskiy-podpisal-zakon-desovetizatsii-ukrainskogo-1651842699.html

3. What are the sanctions on Russia and have they affected its economy? [Electron resource] / BBC. URL: https://www.bbc.com/news/world-europe-60125659

4. NATO's response to Russia's invasion of Ukraine. [Electron resource] / URL: https://www.nato.int/cps/en/natohq/topics_192648.htm

OPERATIONAL DEVELOPMENT OF ORTHOPHOTOPLAN OF THE TERRITORY

Bayramov A.A., Talibov A.M.
İnstitute of Control Systems, Baku, Azerbaijan

It is known that detailed information about the territory, maps and other descriptions of the territory are used to organize and plan various actions [1-7].

The article is about the application of Geographical Information Systems (GIS) and photogrammetric technologies in the military fields, determining the coordinates of the target, operational decision-making, etc. dedicated to the preparation of the orthophoto plan of the territory for the works and the construction of the 3-dimensional model of the territory for the organization of future operational works.

In order to use military application of GIS and photogrammetric technologies in the study of the territory to be explored, the following measures should be taken first:

1) shooting must be performed according to photogrammetric requirements;

2) the photos taken should be sent to the center in real time via radio communication;

3) determining the coordinates of the stationary target that the operator is looking for, making operational decisions, etc. for works, he should promptly prepare an orthophoto plan of the area or perform the work of building a 3-dimensional model of the area.

References

1. Piriyev, H.K. et al. Modelling of battle operations. Monograph. Baku: Military publishing house, 2016. 250 p.

2. Nasibov Y. A. et al. Modelling of the rationally deployment of observing systems //Сучасні інформаційні системи. – 2019. – №. 3,№ 2. – С. 10-13.

3. Hashimov E. G., Bayramov A. A. Destruction of enemy combat power in indeterminacy condition //Proc.of Vth Intern. Scientific Techn. conference "Modern development directions of data communication technology and control means.–2015.–p. 23-24.

4. Bayramov A. A., Hashimov E. G. Assessment of invisible areas and military objects in mountainous terrain //Defence Science Journal. – 2018. – Т. 68. – №. 4. – С. 343.

5. Hashimov E. G. et al. Application of relief digital model for combat operation planning //Military Knowledge. – 2015. – №. 4. – С. 63-69.

6. Hashimov E. G. et al. Terrain orthophotoplanes making for military objects revealing //National security and military sciences. – 2016. – Т. 2. – №. 4. – С. 14-20.

7. Hashimov E. G., Bayramov A. A., Khalilov B. M. Terrain orthophotomap making and combat control //Proceeding of Internatonal Conf."Modern Call of Security and Defence". I-st. – 2016. – Т. 19. – С. 68-71.

ФОРТИФІКАЦІЙНІ СПОРУДИ У СЕРЕДНЬОВІЧНОМУ АЗЕРБАЙДЖАНІ (IX – ПОЧАТКУ XIII СТ.)

Алієв Н.А.
Військовий Науково-дослідний інститут, Баку, Азербайджан

Фортифікаційні споруди міст Азербайджану в XI-XIII століттях мали багато спільних рис з оборонними спорудами мусульманського Сходу, але були не позбавлені і своїх специфічних особливостей. Фортеці та інші оборонні споруди зводилися в стратегічно і тактично важливих пунктах країни, при цьому місцеві архітектори продовжували максимально використовувати рельєф місцевості, пристосовуючи природні перешкоди до оборони фортеці [1, с .61].

У цей період в Азербайджані набувають найбільшого розвитку три архітектурні школи військового зодчества – Нахчівано-Тебрізська, Ширвано-Абшеронська та Арранська [1, 69-70]. Всі оборонні споруди країни дослідники умовно ділять на п'ять видів: міста-фортеці, фортеці, феодальні замки, спостережно-сигнальні вежі та оборонні вали [2, с.169-170; 3, с.154-160].

Найбільшими укріпленими в Азербайджані були міста Тебріз, Гянджа, Ардебіл, Дербенд, Бейлаган, Шамкір, Шамахи, Баку, Нахчіван, Габала, Кіран, Хой, Урмія, Хамадан та ін. Всі ці міста грали важливу участь у оборонній системі країни [1, с.61-87].

Міста Азербайджану розвивалися, спираючись на місцеві традиції містобудівництва.

Однак, був і вплив культур сусідніх країн Сходу – результат взаємозв'язку між країнами, обумовлений їх політичним та економічним становищем у цей період.

Система фортифікації міст включала такі елементи як фортечні стіни, цитадель, вежі, рови, вали, укріплені ворота з підйомними мостами. Особливістю міської фортифікації в цей період було укрупнення фортечних стін, а також зведення круглих веж, замість колишніх квадратних, що було пов'язано з появою нових видів облогової техніки. Стіни зміцнювалися не тільки вежами, а й контрфорсами – прямокутними або напівкруглими монолітними укріпленнями, що примикають як зсередини, так і ззовні до стіни.

Археологічні розкопки в Дербенте і фортеці Сабаїл підтвердили відомості писемних джерел про те, що існував спосіб зміцнення кам'яних стін металевими штирями, що вставляються в отвори з подальшою заливкою цих отворів свинцем [2, с.171].

У захисті міста чималу роль відігравали не тільки його власні зміцнення, а й окремі замки і вежі, які служили резиденціями правителів та їх сімей і призначені для оборони шляхів сполучення і підступів до го ¬роду.

Особливе місце в оборонній системі середньовічних держав грали фортеці. Фортеці виконували суто військові функції та їх за призначенням ділять на тактичні та стратегічні.

При дослідженні середньовічних міст і фортець археологами були виявлені різні підземні ходи та споруди. Вони часом пов'язували між собою міста-фортеці і через них у разі довготривалої облоги гарнізони забезпечувалися водою та продуктом [2, с.184].

В обороні міста також важливу роль відігравали позаміські фортеці, штучні вали та інші польові споруди, що стоять на підступах до міста, як наприклад у Бейлагані та Шемах [4, с.19].

Оборонні споруди міст Азербайджану відражали рівень військового мистецтва свого часу і були пристосовані до протистояння облогової техніки - ме¬тательним знаряддям, стінобитним машинам і т.п. Про захист укріплень від різних облогових засобів середньовіччя повідомляється і у творах Низамі Гянджеві (камнеметные машини - манджанік, аррада, арусак тощо.), і навіть інших середньовічних авторів [4, з. 22].

Оборона міст і фортець здійснювалася за певними, виробленими століттями правилами [5, с.290-291]. Для того, щоб не дати противнику оточити зміцнення і почати планомірну атаку, робилися раптові вилазки. При виникненні смертельної загрози зміцненню, в обороні приймав участь не тільки гарнізон, але і громадянське населення [5, с.292-293].

В цілому, загальний рівень розвитку військово-фортифікаційної системи в найбільших середньовічних містах Азербайджану відповідав досягненням військової справи на всьому Сході. У той же час підвищилося значення оборонних споруд у розвитку військового мистецтва в Азербайджані, ефективному застосуванні різних видів та типів облогової техніки у військах, а також удосконаленні тактичних прийомів та методів при захисті та облозі фортець.

Список літератури

1. Археологія Азербайджану. Середньовіччя ст. - Том VI. - Баку: Схід-Захід, - 2008, - 632 с.

2. Мамедов, С.Г. Історія воєн та військового мистецтва Азербайджану (нариси) (з найдавніших часів до XVII століття). -Баку: Nafta-Press, -1997.-385 с.

3. Алієв, Н.А. Військова історія Азербайджану. - II частина. Військова справа та військове мистецтво в Азербайджані в III-XV ст.-Баку:Azpoliqraf,-2017.-276 с.

4. Нагієв, Г.Г. Фортифікація та топографія середньовічних міст Азербайджану (V – початок XIII ст.) // Автореф. дис... канд.іст.наук. - М., - 1994, - 24 с. // cheloveknauka.com/v/484766/a#?page=24

5. Алієв Н., Ахмедов С., Амірбекова Н. Військова історія Азербайджану (з давнього періоду до початку XX століття). - Баку: AZpoliqrAF, - 2023, - 976 с.

ПРИЧИНИ ТРАНСФОРМАЦІЇ СУЧАСНИХ ВІЙСЬКОВИХ КОНФЛІКТІВ

Наджафов З.Н.
Інститут військового управління, Баку, Азербайджан

Збройне насильство не можна виключити з процесу історичного розвитку. Завдяки цьому сформувалися нові геополітичні реалії, співвідношення сил, сфери впливу, розвиток продуктивних сил і нові правила гри. В цілому війна заперечує старий статус-кво і створює порядок, заснований на новій геополітичній реальності. Війна виникає через необхідність оновлення поглядів, статусів, впливу, правил гри, кризи чи трансформації менеджменту в цілому.

Хоча форма, засоби та актори воєн, які вічно поставлені перед дилемою занепаду та прогресу, змінилися, незмінною залишається їхня соціальна сутність. «Торгова війна», «мережева війна», «когнітивна війна», «нафтогазова війна», «гібридна війна» тощо, з якими ми досі стикалися в науковій літературі. хоча це дає підстави говорити про те, що його війни зазнали серйозних змін у плані форми, він підтверджує, що в плані суті він зберіг свій класичний зміст.

Збройна боротьба залишається військово-політичним виміром геополітичних змін і боротьби.

Досягнення переваги, розширення географічних кордонів контролю, недопущення контрзаходів, повне або часткове знищення противника вважаються стратегічними цілями, що стоять перед кожною війною. У наш час війна є продовженням політики не лише насильницькими [1-3], але навіть ненасильницькими способами та засобами. Війни втратили політичну сутність і стали знаряддям злочинної діяльності.

У сьогоднішніх війнах політичні цілі були замінені кримінальною співпрацею. Сучасні війни підпорядковують держави за допомогою стратегій непрямих дій – інформаційного насильства, кольорових революцій, мережевих, мас-медіа-війн, когнітивних війн, і захоплюють контроль над її територією, політичною системою та суверенітетом, не створюючи масової бойової сцени.

Цей тип війни створює анексію в обхід міжнародного права.

Відбулося розширення простору безпеки та його нова структура.

Предметна сфера міжнародної безпеки розширилася за рахунок невійськових цивільних загроз. На думку більшості вітчизняних та зарубіжних дослідників, окрім закінчення «холодної війни», глобалізації, процесів демократизації у світі, розвитку науково-технічної революції, посилення ролі недержавних акторів, тенденція до зміни функцій держав і балансу сил призводять до формування нової структури сучасного простору безпеки.мали великий вплив.

В останні десятиліття предметна сфера міжнародної безпеки розширилася. Протягом майже 350 років існування Вестфальської світової системи взаємодії держави були провідними, майже монопольними, акторами у питаннях війни та миру, а згодом і міжнародної безпеки. Іноді значний вплив на стан миру мають недержавні групи - пірати, озброєні групи великих торговельних компаній, бойові осередки транскордонних ідеологічних рухів (наприклад, анархістів, соціалістів), озброєні групи народів, які борються за самовизначення та міжнародної безпеки в різних регіонах [4].

За останні роки інші транскордонні загрози значно зросли через кіберзлочинність, незаконне виробництво та транспортування наркотиків, піратство (не лише на північно-східному узбережжі Африки), нелегальну міграцію та кримінальні недержавні організації та особи, які займаються великою масштаби фінансових злочинів.

Від внутрішніх і транснаціональних загроз кримінального характеру, пов'язаних із неполітичним насильством – злом інформаційних мереж, незаконний обіг наркотиків, піратство, незаконна торгівля зброєю, транснаціональна організована злочинність тощо. Сфера глобальної та регіональної безпеки викликає занепокоєння. Такі загрози часто називають «сірими» загрозами, оскільки вони знаходяться на перетині військових і цивільних загроз. Віднесення їх до особливоїкатегорії загроз, пов'язаних із неполітичним насильством, виправдано характером цих загроз, а також врахуванням особливостей боротьби з ними. Ця категорія загроз раніше займала важливе місце в національних комплексах внутрішньої або державної безпеки.

Однак сьогодні, коли ці загрози набувають глобалізованого, транснаціонального характеру, посилюється міжнародне співробітництво у боротьбі з ними, ця «сіра» зона небезпеки та боротьба з ними стають важливою складовою загальної системи міжнародної безпеки.

Список літератури

1. Carl Von Clausewitz. On war / Edited and Translated by Michael Howard and Peter Paret/ Princeton University Press, Princeton, New Jersey. – 637 p.

2. Hashimov, E.G. Iskandarov, Kh.I., Sadiyev S.S. The role the Armed Forces likely to play in future conflicts // Civitas Et Lex. Kwartalnik. University of Warmia and Mazury in Olsztyn, 2019, 1(21), p.p. 25-35. DOI: https://doi.org/10.31648/cetl.2873

3. Piriyev G. K., Hashimov E. G., Bayramov A. A. Modelling of the battle operations //Monografiya, Herbi Nashriat", Baku. – 2017.

4. Вєтринський, І.М. (2016) Сучасні геополітичні виклики для міжнародної безпеки. Модернізація і безпека розвитку в умовах глобалізації: збірник наукових праць. – К.: ДУ «Інститут всесвітньої історії НАН України». с. 141-150.

ПОБУДОВА КАРТИ ПРИМІЩЕНЬ ТА НАВІГАЦІЇ ДЛЯ РУХОМОЇ РОБОТИЗОВАНОЇ ПЛАТФОРМИ

Малєєва Ю.А., Костуренко В.В.
Національний аерокосмічний університет ім. М Є. Жуковського «Харківський авіаційний інститут», м. Харків, Україна

На сьогоднішній день існує багато автономних мобільних роботів, область застосування яких є дуже широкою. Такі робототехнічні системи знаходять застосування і в цивільній сфері в якості сервісної робототехніки. Це і пошук та знешкодження небезпечних об'єктів, завдання радіаційної та хімічної розвідки, робота в зоні техногенних і природних катастроф тощо. Для виконання таких завдань, перш за все, потрібно мати систему навігації та локалізації (визначення точного положення робота на карті) високої точності для того, щоб уникнути зіткнень та аварій [1]. Метою дослідження є забезпечення автономної навігації та побудови цифрової карти приміщень для мобільної робототехнічної платформи.

Картографування та локалізація є взаємозалежними процесами: для локалізації роботу необхідне існування карти, щоб порівняти дані спостережень середовища із модельованими даними, тоді як створення карти вимагає точної оцінки місцезнаходження роботу. Цю проблему можна вирішити з допомогою одночасного визначення положення робота в середовищі і побудови карти цього середовища – System of Localization and Mapping (SLAM). В роботі використано алгоритм SLAM за допомогою розширеного фільтра Калмана (EKF-SLAM). Фільтр Калмана, відомий також як лінійно-квадратичне оцінювання, – це алгоритм, що використовує послідовності вимірювань протягом часу, які містять шум (випадкові відхилення) та інші неточності, й видає оцінки невідомих змінних, що є потенційно точнішими за базовані на самих лише вимірюваннях. Програми для керування роботом створені в середовищі Node-RED. Для управління сервоприводами рухомої передньої частини робота, де знаходяться ультразвуковий далекомір та камера, використано бібліотеку pca9685.

Таким чином, в роботі розглянуто алгоритми навігації та картографування для мобільних роботизованих платформ, що інтегрують інформацію від декількох датчиків, у тому числі ультразвукового далекоміру та лазерного радару, що дає можливість побудувати цифрову карту приміщення.

Аналіз отриманої карти та руху датчика показує, що форми та розміри всередині приміщення відтворюються правильно.

Список літератури

1. Навігація мобільних наземних роботів у недетермінованих середовищах. Сергієнко О.Ю., Карташов В.М., Колендовська М.М. Харків: ХНУРЕ, 2020. 297 с.

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ INTERSYSTEMS IRIS ДЛЯ РОЗРОБКИ OLAP-ДОДАТКІВ АНАЛІЗУ РОБОТИ ТРАНСПОРТНО-ЛОГІСТИЧНИХ КОМПАНІЙ

Лещенко О.Б., Анікін А.М.
Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна

Оптимальне керування логістикою транспортних підприємств можливо тільки при удосконаленні логістичних процесів. Велика кількість проблем логістичних компаній пов'язані з оптимізацією роботи транспорту у ланцюзі логістичних систем, особливо якщо це пов'язано з воєнним станом [1]. Зниження собівартості перевезень та їх оптимізацію можливо за допомогою якісного планування та організацію перевезення.

Метою доповіді є використання інформаційних технологій InterSystems IRIS для розробки аналітичних OLAP-додатків транспортно-логістичних компаній. При використанні технологій InterSystems IRIS з'являється можливість зберігати великі об'єми даних, аналізувати та застосовувати їх для подальшого прогнозування діяльності компанії.

В доповіді наводяться особливості перевезення вантажу транспортом, які дають можливість зробити висновки щодо ефективності перевезення вантажу. На вартість перевезень впливають багато чинників, такі як: тип та вага вантажу, вага причепу, стан доріг, витрати пального транспортом, відстань між точками трансферу тощо [1].

Запропоноване рішення у вигляді OLAP-додатка виконане на основі трирівневої технології клієнт-сервер. Інтерфейс кінцевого користувача розроблений за допомогою сучасних методів та інформаційних технологій, таких як: HTML, CSS, JavaScript, InterSystems ZEN та API інтерфейсом до сервісу картографії. Для розробки та розгортання додатків використані технології платформи InterSystems IRIS, що забезпечує високий рівень продуктивності. Серверна частина додатка виконана під управлінням об'єктно-реляційній системи керування базами даних InterSystems IRIS [2].

Розроблений OLAP-додаток дозволить вирішати питання прогнозування маршрутів та витрат під час процесу перевезення вантажів. У зв'язку з великою кількістю чинників, що впливають на даний процес, розроблений OLAP-додаток дозволить ефективно керувати процесом організації транспортно-логістичних перевезень.

Список літератури

1. Мельник, З. Відновлення транспортного сектору України – як зробити його "зеленим"? [Електронний ресурс] / З. Мельник. – Режим доступу: https://brdo.com.ua/analytics/vidnovlennya-transportnogo-sektoru-ukrayiny-yak-zrobyty-jogo-zelenym/..

2. Лещенко, О. Б. Застосування технології DeepSee InterSystems для побудови багатовимірних баз даних і сховищ інформації : навч. посіб. / О. Б. Лещенко, Ю. О. Лещенко. – Харків : Нац. аерокосм. ун-т «Харків. авіац. ін-т», 2021. – 66 с.

РОЗРОБКА СИСТЕМИ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ ВИБУХОНЕБЕЗПЕЧНИХ ПРЕДМЕТІВ НА ЗОБРАЖЕННЯХ

Присяжнюк О.В.
Національний аерокосмічний університет Імені М. Є. Жуковського
"Харківський авіаційний інститут", Харків, Україна

Виявлення та розпізнавання вибухонебезпечних предметів (ВНП) є важливою задачею для сучасної України. Один із можливих шляхів її розв'язання – використання навчених згорткових нейромереж або систем штучного інтелекту (ШІ). Їх навчання можливе по реальних зображеннях, але їх отримання є проблематичним

У нашому дослідженні розглянуто методику створення синтетичних наборів даних для навчання моделей ШІ [1–3] виявляти вибухонебезпечні предмети на кольорових зображеннях.

Особливу увагу приділено розробці алгоритмів, які моделюють реальні умови знаходження ВНП, що дозволяє моделям ШІ адаптуватися до широкого спектру сценаріїв.

Ефективність виявлення залежить від багатьох факторів, в тому числі адекватності даних, що використовуються для навчання. Тому було розроблено програмний код, що дозволяє автоматично вставляти зображення ВНП основних відомих типів у різноманітні сцени з рандомізацією розміру, положення та орієнтації ВНП.

Це дозволяє швидко генерувати велику кількість анотованих даних для ефективного навчання ШІ.

Кожне вставлене зображення автоматично анотується, що включає ідентифікацію класу об'єкта та його положення на основному зображенні, що є критично важливим для точності навчання моделей ШІ.

Результати дослідження демонструють, що використання синтетичних даних може значно підвищити ефективність навчання моделей ШІ для виявлення вибухонебезпечних предметів, відкриваючи нові можливості для покращення систем безпеки.

Список літератури

1. Liu, W., Anguelov, D., Erhan, D., Szegedy, C., Reed, S., Fu, C.-Y., & Berg, A. C. (2016). "SSD: Single Shot MultiBox Detector". Proceedings of the European conference on computer vision (ECCV), pp. 21-37. DOI: 10.1007/978-3-319-46448-0_2.

2. Ren, S., He, K., Girshick, R., & Sun, J. (2017). "Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks". IEEE Transactions on Pattern Analysis and Machine Intelligence, 39(6), pp. 1137-1149. DOI: 10.1109/TPAMI.2016.2577031.

3. Redmon, J., Divvala, S., Girshick, R., & Farhadi, A. (2016). "You Only Look Once: Unified, Real-Time Object Detection". Proceedings of the IEEE conference on computer vision and pattern recognition (CVPR), pp. 779-788. DOI: 10.1109/CVPR.2016.91.

АВТОМАТИЗОВАНІ СИСТЕМИ УПРАВЛІННЯ ДАНИМИ ТА КОМУНІКАЦІЯМИ У СИТУАЦІЯХ НАДЗВИЧАЙНИХ СИТУАЦІЙ

Дерев'янко К.А., Гук А.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Автоматизовані системи управління даними та комунікаціями в надзвичайних ситуаціях є важливими інструментами для ефективного реагування та координації дій. Вони дозволяють збирати, аналізувати та обробляти інформацію з різних джерел, включаючи такі, як:

сенсори,
відеокамери
мережі зв'язку.

Завдяки цьому, вони можуть виявляти потенційні небезпечні ситуації, швидко реагувати на них та організовувати необхідні заходи безпеки [1].

Ці системи також грають важливу роль у забезпеченні ефективного зв'язку між рятувальними службами, органами влади та громадськістю під час надзвичайних ситуацій.

Вони забезпечують резервні шляхи зв'язку та автоматичне перемикання на них у випадку відмови основних мереж, що забезпечує неперервність комунікації та координації дій.

Усі ці можливості роблять автоматизовані системи управління даними та комунікаціями в надзвичайних ситуаціях невід'ємною частиною сучасних систем безпеки та рятувальних операцій, допомагаючи зберегти життя та майно у критичних ситуаціях.[2]

Метою доповіді є розгляд ролі та важливості автоматизованих систем управління даними та комунікаціями в надзвичайних ситуаціях.

Метою є висвітлення можливостей цих систем у забезпеченні швидкого та ефективного реагування на надзвичайні події, а також їх внеску в збереження життя та майна.

У доповіді буде обговорено перспективи подальшого розвитку цих технологій та виклики, які стоїть перед ними.

Список літератури

1. Карпенко М. К. Автоматизовані системи управління / М. К. Карпенко, А. О. Бурчук. – Дніпро: Українське видання, 2001. – С. 390-403 – (Дніпротех).

2. Чуйбас А. Р. Дані, Комунікації та Надзвичайні Ситуації: Автоматизовані Системи для Ефективного Управління та Координації / Андрій Романович Чуйбас. – Львів: Книгарня, 2009. – С. 81-92 – (Освітні Технології).

ОЦІНКА РИЗИКІВ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Кічата Н.М., Третьяков О.В.
Національний авіаційний університет, Київ, Україна

Дослідження у сфері запобігання та протидії загрозам різного походження підтверджують необхідність впровадження ризик-орієнтованого підходу у державну систему захисту населення від надзвичайних ситуацій природного та техногенного характеру. Це необхідно для ефективного передбачення та зменшення ризику виникнення різних катастроф для об'єктів критичної інфраструктури [1].

Оцінка ризиків на об'єктах критичної інфраструктури є складним завданням через різноманітність параметрів, галузей, секторів, учасників тощо. Крім того, вони рідко функціонують ізольовано, кожен об'єкт критичної інфраструктури зазвичай тісно пов'язаний з взаємозалежною інфраструктурою.

Метою доповіді є розробка рекомендацій щодо запобігання можливим небезпечним подіям на об'єктах критичної інфраструктури.

Оцінка ризику включає в себе послідовний перелік етапів, які дозволяють урахувати вплив основних факторів небезпеки. Небезпечні процеси включають виникнення відмов, ушкоджень, руйнувань, загибелі, аварій, катастроф.

Для запобігання можливим небезпечним подіям на об'єктах критичної інфраструктури необхідно:

1. Розвивати системи попередження та моніторингу, що дозволяють виявляти потенційні загрози та ризики заздалегідь.
2. Впроваджувати технології та практики ризик-менеджменту для ідентифікації, оцінки та управління ризиками.
3. Забезпечувати регулярне оновлення та підтримку інфраструктури з метою підвищення її стійкості та резервності.
4. Здійснювати регулярні навчальні заходи та тренування для персоналу з підготовки до екстрених ситуацій та кризового управління.
5. Співпрацювати з іншими організаціями, урядовими структурами та міжнародними партнерами для обміну досвідом та ресурсами у сфері безпеки.
6. Постійно аналізувати та оновлювати стратегії та плани заходів у разі виникнення кризових ситуацій, щоб вони відповідали сучасним умовам та загрозам.

Список літератури

1. Іванюта С. П., Качинський А. Б. Екологічна та природно-техногенна безпека України: регіональний вимір загроз і ризиків: монографія / Нац. ін-т стратегічних досліджень. Київ: НІСД, 2012. 308 с..

2. Бірюков Д. С. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні / Д. С. Бірюков, С. І. Кондратов. – К.: НІСД, 2012. – 96 с.

КІЛЬКІСНА ОЦІНКА СТІЙКОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Третьяков О.В.
Національний авіаційний університет, Київ, Україна
Пуха М.С.
Державна служба спеціального зв'язку та захисту інформації України, Київ, Україна

У сфері національної безпеки визначати національну політику щодо зміцнення та підтримки безпечної, функціональної та стійкої критичної інфраструктури в секторах, які є важливими для національної безпеки, громадського здоров'я та безпеки, економічної життєздатності та загальної якості життя. При цьому стійкість визначається як здатність готуватися до мінливих умов та адаптуватися до них, а також витримувати збої й швидко відновлюватися після них, включно з навмисними атаками, аваріями або природними загрозами [1]. Для визначення пріоритетних заходів для підвищення стікості об'єктів критичної інфраструктури необхідно мати кількісні показники, які дозволять проводити порівняльний аналіз і визначати першочергові завдання.

Метою доповіді є розробка кількісного показника для оцінки стікості об'єктів критичної інфраструктури незалежно від їх приналежності до секторів.

В доповіді наводиться обґрунтуваання визначення коефіцієнту стійкості як добутку часу, потрібного на відновлення об'єкту, або його частина, після настання небезпечної події будь якої природи, на загальну сукупність витрат на його відновлення з урахуванням усіх видів витрат (матеріальних, енергетичних, людських тощо) до повного відновлення обсягу надання послуг об'єктом критичної інфраструктури до події. Такий підхід дозволяє врахувати усі чотири основні елементи – складові стійкості: опір, надійність, резервування і посилення реагування і відновлення [2]. Посилення реагування та відновлення включає будь-які заходи, спрямовані на підвищення швидкості відновлення інфраструктурних послуг після збоїв. Цей елемент не є фактичною реакцією та відновленням з боку організації, що підтримує інфраструктуру. Це більше стосується проектування активів та мереж, які будуть швидше відновлюватися після збоїв.

Список літератури

1. АПКБІ, «Національний план захисту інфраструктури (НПЗІ) 2013: партнерство заради безпеки та стійкості критичної інфраструктури». 2013 р. Дата перегляду: 13.02.2020 року. www.cisa.gov/national-infrastructure-protection-plan

2. Вудс, Девід Д . Чотири концепції стійкості та наслідки для майбутнього стійкості інжиніринг, Надійність, інженерія та безпека систем, том 141, 2015, с. 5-9, ISSN 0951- 8320, https://doi.org/10.1016/j.ress2015.03.018.

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СИСТЕМ ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Доронін Є.В., Вальченко О.І.
Національний авіаційний університет, Київ, Україна
Бондаренко С.В.
Національна академія Національної гвардії України, Харків, Україна

Об'єкти критичної інфраструктури – системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам. Події останніх років показали, що стійкість об'єктів критичної інфраструктури (ОКІ) в умовах російської агресії є актуальною задачею.

Головною метою забезпечення надійного функціонування будь-якого об'єктів критичної інфраструктури під час виникнення надзвичайної ситуації є створення умов його сталої роботи шляхом збору інформації про стійкість, якість роботи усіх систем захисту, які забезпечують надійну працю усього підприємства вцілому.

Збір такої інформації дозволить вчасно виявити слабкі місця в усіх системах захисту ОКІ і шляхом оперативного втручання забезпечити їх сталу роботу та дозволити ОКІ виконувати свої функції в штатному режимі [1–3].

Метою доповіді є визначення слабких місць в системах захисту об'єктів критичної інфраструктури та приведення їх у такий стан, що забезпечить надійну сталу роботу усього ОКІ при будь-якому впливі зовнішніх втручань.

В доповіді наводиться матеріали досліджень стану сучасних систем захисту ОКІ, визначені їх основні недоліки та рекомендації на поліпшення опіру, надійності, резервування і посилення реагування і відновлення, що впливає на підвищення швидкості відновлення інфраструктурних послуг і дозволить забезпечити штатну роботу об'єктів критичної інфраструктури в умовах надзвичайних ситуацій, пов'язаних з активізацією бойових дій країни-агресора.

Список літератури

1. АПКБІ, «Національний план захисту інфраструктури (НПЗІ) 2013: партнерство заради безпеки та стійкості критичної інфраструктури». 2013 р.. URL:www.cisa.gov/national-infrastructure-protection-plan (дата звернення: 13.02.2020(

2. Закон України Про критичну інфраструктуру від 16.11.2021 р. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 18.10.2023)

3. Закон України Про правовий режим воєнного стану від 14.04.2022 р. URL: https://zakon.rada.gov.ua/laws/show/389-19#Text (дата звернення 18.10.2023)

СПІВСТАВЛЕННЯ ВИМОГ ДИРЕКТИВИ ЄС № 2557 ТА УКРАЇНСЬКОГО ЗАКОНОДАВСТВА З КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Ревурко О.Є, Третяков О.В.
Національний авіаційний університет, Київ, Україна

Критична інфраструктура є необхідною складовою для забезпечення безпеки, стабільності та розвитку суспільства держави. У воєнних умовах вона постійно піддається атакам ворога, що може призвести до серйозних наслідків для життя кожного громадянина та для економічної стабільності та безпеки країни в цілому [1].

Апотеозою можуть стати, як і економічні кризові ситуації, так і необоротні наслідки для життя людей та всіх біологічних видів [2].

Метою доповіді є дослідження забезпечення відповідності законодавства України з питань захисту критичної інфраструктури вимогам міжнародних стандартів та заходи з підтримки оптимального функціонування української законодавчої системи в умовах внутрішніх та зовнішніх загроз.

У доповіді проводиться глибокий аналіз відповідності положень Директиви ЄС № 2557 від 14 грудня 2022 року [3] законодавству України. Також проведені дослідження з визначення відповідності директиви прямою або опосередкованою частиною правового порядку України. Проведено аналіз ефективності заходів, вжитих в Україні для виконання вимог Директиви, особливо в умовах воєнного конфлікту та можливості розширення цих заходів.

Результати перевірки відповідності українських регулюючих законів міжнародним стандартам та конвенціям, які є важливими для нашої країни в контексті воєнних реалій.

У зв'язку з цим чинності набувають методи, як аналіз даних та статистичні методи аналізу текстів, кейс-стаді аналіз, дослідження реальних прикладів застосування законодавства, яке посприяє глибшому розумінню його впливу та ефективності, порівняльний аналіз.

Список літератури

1. Зелена книга з питань захисту критичної інфраструктури в Україні: зб. матер. міжнар. експерт. нарад / упоряд. Д. С. Бірюков, С. І. Кондратов; за заг. ред. О. М. Суходолі. К.: НІСД, 2016. 176 с.

2. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України : аналіт. доп. / [Бобро Д. Г., Іванюта С. П., Кондратов С. І., Суходоля О. М.] / за заг. ред. О. М. Суходолі. – К. : НІСД, 2019. – 224 с.

3. European Parliament and Council. (2022). Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2557

ОЦІНКА ЕФЕКТИВНОСТІ ЗАСТОСУВАННЯ БЕЗПІЛОТНИХ АВІАЦІЙНИХ СИСТЕМ ПРИ ВИКОНАННІ РОБІТ ІЗ АВІАЦІЙНОГО ПОШУКУ І РЯТУВАННЯ

Федина В.П., Якимець І.В.
Національний авіаційний університет, Київ, Україна

Роль авіаційного транспорту в сучасному житті стрімко зростає. Цьому сприяє технологічний розвиток авіаційної галузі, глобалізація економіки і все тісніші ділові та культурні зв'язки між різними країнами світу.

У повітряному просторі постійно знаходиться велика кількість літальних апаратів. У зв'язку із цим різко зростає ймовірність виникнення різноманітних надзвичайних ситуацій, пов'язаних із експлуатацією авіаційної техніки. Статистика свідчить, що кожного року надзвичайні ситуації на авіатранспорті обчислюються тисячами випадків.

До основних видів ураження при авіаційних подіях (катастрофах) належать механічні (динамічні) та опікові травми.

Серед потерпілих особи з механічними пошкодженнями можуть становити до 90%, у тому числі в стані шоку – 10% , з черепно-мозковою травмою - 40%, у 10-20% - можуть бути сумісні травми та опіки. Близько половини постраждалих, як правило, мають тяжкий та дуже тяжкий ступінь травми [1].

Тому проблеми пошуку і рятування людей, майна і техніки стають в ранг складної світової організаційної і технічної проблеми.

Метою доповіді є аналіз стану та оцінка ефективності системи авіаційного пошуку і рятування в Україні.

Важливим етапом виконання робіт із авіаційного пошуку і рятування є встановлення місць виникнення надзвичайних ситуацій і пошук людей, які потерпають від наслідків НС [2]. Враховуючи той факт, що часто авіаційні надзвичайні ситуації виникають в важкодоступній гірській і лісистій місцевості, що в свою чергу затрудняє використання наземної техніки для виконання відповідних заходів.

В доповіді наводяться результати досліджень із оцінки можливості застосування безпілотних літальних апаратів для виконання робіт із авіаційного пошуку і рятування.

Список літератури

1.Аветисян В.Г., Сенчихін Ю.М., Ораєвський Д.В. Організація аварійно-рятувальних робіт на авіаційному транспорті: Навчальний посібник– Х: НУЦЗУ, 2012. – 108 с.

2.Застосування безпілотних авіаційних систем у сфері цивільного захисту : колективна монографія / Д. В. Бондар та ін. Київ : ІДУНДЦЗ, 2022. 312 с.

РОЗРОБКА УНІФІКОВАНОГО МЕТОДУ ВИЗНАЧЕННЯ РИЗИКІВ НАДЗВИЧАЙНОЇ СИТУАЦІЇ ТРАНСПОРТНОЇ ІНФРАСТРУКТУРИ

Третьяков О.В., Козлітін О.О., Ремська А.В.
Національний авіаційний університет, Київ, Україна

У статті розглянуто проблему визначення ризиків надзвичайних ситуацій у транспортній інфраструктурі та запропоновано уніфікований метод їх аналізу, який поєднує в собі сучасні методи аналізу ризиків з урахуванням специфіки транспортної інфраструктури.

Обґрунтовується актуальність питання з урахуванням зростаючої складності транспортних систем і потенційно небезпечних ситуацій, що можуть виникнути. Описано процес розробки методу, включаючи ідентифікацію потенційних загроз, оцінку вразливості системи та ймовірності виникнення надзвичайних ситуацій, а також розрахунок ризиків з урахуванням їхнього впливу на транспортну інфраструктуру.

Проводиться порівняльний аналіз розробленого методу з існуючими підходами, виявляються переваги та недоліки.

Мета роботи полягає у розробці та впровадженні уніфікованого методу, який має на меті систематизацію та аналіз потенційних небезпек, які можуть виникнути на транспортних об'єктах та сприяти попередженню подій надзвичайного характеру.

У роботі описано особливості управління ризиками в сучасних транспортних процесах.

Проведено аналіз сучасних методів визначення ризиків надзвичайних ситуацій у транспортній інфраструктурі, на основі якого розроблено уніфікований метод, який враховує специфіку та особливості різних видів транспортних систем.

Розроблений підхід може слугувати основою для подальших досліджень у галузі безпеки та стабільності транспортних систем, сприяючи покращенню їхньої роботи та зменшенню можливих негативних наслідків надзвичайних ситуацій.

Список літератури

1. Чумаченко С. М., Кутовий О. П., Михайлова А. В. Застосування експертно-аналітичних методів для оцінювання загроз об’єктам критичної інфраструктури оборонно-промислового комплексу на сході України. Інженерія природокористування. 2020. №4(18). С. 114-123.

2. Азаренко О., Гончаренко Ю., Дівізінюк М., Шевченко Р., Шевченко О. Поняття загрози та ризику. Їх загальні риси та принципіальні відмінності (стосовно ядерних та інших стратегічних об'єктів). Комунальне господарство міст. 2023. №177. Том 3. URL:https://pdfs.semanticscholar.org/f.pdf

3. Жарська Н.В. безпека життєдіяльності в умовах надзвичайних ситуацій:Лекція з навчальної дисципліни.URL: https://repository.ldufk.edu.ua/bitstream/.pdf

ВИКОРИСТАННЯ РОЗРАХУНКОВИХ МЕТОДІВ ДЛЯ ОЦІНКИ МОЖЛИВОСТЕЙ РАДІОЛОКАЦІЙНИХ ЗАСОБІВ ПО ВИКОНАННЮ ЗАВДАНЬ ЗА ПРИ ЗНАЧЕННЯМ

Алєксєєв В.О., Нечитайло С.В., Луценко А.С., Коломієць О.Л.
Харківський національний університет Повітряних Сил, Харків, Україна

Застосування в сучасних війнах засобів повітряного нападу з малою ефективною поверхнею розсіювання, що рухаються з огинанням рельєфу місцевості, обумовлює пошук шляхів оптимального розташування радіотехнічних засобів на місцевості з метою виконання завдання засобами протиповітряної оборони по прикриттю об'єктів [1-4].

Метою доповіді є підвищення ефективності угрупування протиповітряної оборони по прикриттю об'єктів.

Досліджувались методи розрахунку характеристик діаграм направленості радіолокаційних засобів та ефективних поверхонь розсіювання засобів повітряного нападу.

Наведено методику розрахунку характеристик радіолокаційних засобів, що є на озброєнні Повітряних Сил Збройних Сил України.

За результатами аналізу отриманих даних оцінювались можливості радіолокаційних засобів по виявленню та супроводженню повітряних цілей з урахуванням рельєфу місцевості.

В доповіді наведені пропозиції щодо оптимізації розміщення рухомих радіолокаційних підрозділів за критерієм мінімуму імовірності пропуску цілі в залежності від характеристик удару повітряного противника та об'єктів прикриття.

Список літератури

1. Сухаревський О. І., Василець В. О., Нечитайло С. В., Резніченко О. А. Дослідження радіолокаційних характеристик моделі баражуючого боєприпасу "Shahed-136". *Наука і техніка Повітряних Сил Збройних Сил України*. 2023. № 2 (51). С. 56-62.

2. O. Sukharevsky S., Nechitaylo V., Vasilets and I. Ryapolov. Calculation Method for High-Resolution Range Profiles of Complex Shape Radar Objects. *2020 IEEE Ukrainian Microwave Week (UkrMW).* Kharkiv, Ukraine. 2020. Pp. 1026-1029. DOI: https://doi.org/10.1109/UkrMW49653.2020.9252634.

3. Герасимов С. В., Чернявський О. Ю., Нанівський Р. А. и др. Комплектування полігону навчально-тренувальними комплексами для підготовки операторів безпілотних летальних апаратів. *Збірник наукових праць Військової академії (м. Одеса)*. 2023. № 2 (20). С. 63-72. DOI: https://doi.org/10.37129/2313-7509.2023.20.63-72.

4. Сухаревский О. И., Шрамков А. Ю., Рощупкин Е. С. Высокочастотный метод расчета диаграммы направленности антенны с учетом неоднородностей рельефа местности на позиции РЛС. *Моделювання та інформаційні технології*. 2005. № 33. С. 174-181.

5. Кукобко С. В., Місценко Р. В., Бритов Д. М., Рощупкін Є. С., Гайбадулов Б. В. Пропозиції щодо автоматизації процесу прийняття рішення при класифікації ситуацій у повітряному просторі. Міжнародна НТК "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку". Харків. 2023.

РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ НАПРЯМКІВ УДОСКОНАЛЕННЯ СЛІДКУВАЛЬНОЇ КООРДИНАТНОЇ СИСТЕМИ БАГАТОКАНАЛЬНОЇ СТАНЦІЇ НАВЕДЕННЯ РАКЕТ

Викиданець В.В., Гайбадулов Б.В., Чміль Ю.О., Долейко О.С.
Харківський університет Повітряних Сил імені І. Кожедуба, Харків, Україна

Супроводження повітряних цілей радіотехнічними засобами контролю повітряного простору суттєво залежить від якості вимірювання первинних координат (кута місця, азимуту, похилої дальності та допплерівського зсуву частоти) та оцінки їх похибок [1-5].

Метою доповіді є розробка пропозицій щодо удосконалення можливостей багатоканальних радіотехнічних засобів контролю повітряних цілей по виявленню маневру та стійкому супроводженню цілей, що маневрують.

Досліджувались апаратура та способи слідкуючих вимірювань первинних координат радіотехнічними засобами контролю повітряного простору.

В доповіді наводяться результати аналізу режимів роботи слідкуючої координатної системи багатоканальної станції наведення ракет при супроводженні повітряних цілей різних типів.

Розглянуто існуючі способи слідкуючих вимірювань координат та засобів, що їх реалізують

Наведено пропозиції з підвищення слідкуючих вимірювань первинних координат багатоканальною станцією наведення ракет.

Список літератури

1. Викиданець В. В., Кукобко С. В., Шулежко В. В., Коробков Ю. В. Аналіз слідкуючої координатної системи багатоканальної радіолокаційної станції спеціального призначення. *XVII Міжнародна науково-практична конференція магістрантів та аспірантів «Теоретичні та практичні дослідження молодих вчених» (TPRYS-2023).* Харків. 2023.

2. Dzhus V., Roshchupkin Y., Kukobko S., Herasymov S., Drob N., Trofymova M. Estimation of noise radiance point sources multichannel direction finding systems resolution by linear prediction method. *Sistemi obrobki ìnformacìï.* 2021. № 4(167). С. 19-26.

3. Герасимов С. В., Ізосімов Д. М., Рощупкін Є. С., Богдановський О. М. Оцінка параметрів руху повітряних об'єктів при об'єднанні результатів незалежних первинних вимірювань в активній багатопозиційній системі радіолокації. *Системи озброєння і військова техніка*. 2010. №3. С. 110-113.

4. S. Herasimov, M. Pavlenko, E. Roshchupkin, M. Lytvynenko, O. Pukhovyi, and A. Salii, Aircraft flight route search method with the use of cellular automata, *International Journal of Advanced Trends in Computer Science and Engineering*. Vol. 9, is. 4. 2020. Pp. 5077-5082.

5. Кукобко С. В., Павленко М. А., Рощупкін Є. С. Структура спеціального математичного забезпечення імітації повітряної обстановки в підсистемі тренажу АСУ спеціального призначення. *Системи озброєння і військова техніка*. 2008. № 2. С. 44-48.

ПРОПОЗИЦІЇ ЩОДО УДОСКОНАЛЕННЯ ПОРЯДКУ РОЗГОРТАННЯ НА НЕОБЛАДНАНІЙ ПОЗИЦІЇ ЗЕНІТНОЇ РАКЕТНОЇ СИСТЕМИ

Вурста К. ., Джус В.В., Романчук Р.А.
Харківський університет Повітряних Сил імені І. Кожедуба, Харків, Україна
Мирюгін В.І.
Державний науково-дослідний інститут випробування та сертифікації озброєння та військової техніки, Чернігів, Україна

Встановлено, що результати роботи технічних засобів протиповітряної оборони суттєво залежать від часу їх розгортання та точності топоприв'язки та орієнтування [1-4].

Метою доповіді є розробка пропозицій щодо скорочення часу розгортання та підвищення точності орієнтування технічних засобів зенітної ракетної батареї на необладнаній позиції.

Досліджувались штатні та перспективні засоби та методи орієнтування радіотехнічних засобів у просторі в умовах впливу перешкод.

В доповіді наводяться результати аналізу існуючих способів орієнтування та горизонтування технічних засобів зенітної ракетної батареї при розгортанні на необладнаній позиції, та досліджень щодо побудови та застосування оптичних засобів вимірювання.

Наведені пропозиції щодо застосування оптичних засобів для орієнтування та горизонтування засобів зенітної ракетної батареї та методики щодо їх застосування.

Список літератури

1. Вурста К. І., Галицький О. Ф., Скорик А. Б., Джус В. В. Аналіз апаратури навігації топоприв'язки та орієнтування зенітної ракетної системи С-300В1. XVII Міжнародна науково-практична конференція магістрантів та аспірантів «Теоретичні та практичні дослідження молодих вчених» (TPRYS-2023). Харків. 2023.

2. Джус В., Гайбадулов Б., Калугін Д., Титаренко Р., Кукобко С. Вплив похибок топоприв'язки та орієнтування радіотехнічних засобів контролю повітряного простору на оцінки координатної інформації, що видаються ними. Наукові праці Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки, 2021. № 8. С. 31-43.

3. Бурковський С. І., Рощупкін Є. С., Шрамков А. Ю. Вплив похибок визначення координат виносних пунктів пасивної багатопозиційної системи на точність вимірювання координат джерела випромінювання. Збірник наукових праць ХІ ВПС, 2004. № 11. С. 103–108.

4. Рощупкин Е. С. Ошибки определения прямоугольных координат источника излучения в пассивных гиперболических измерительных системах. Зб. наук. праць Об'єднаного науково-дослідного інституту Збройних Сил. 2007. № 2 (7). С. 156–161.

ПРОПОЗИЦІЇ ЩОДО УДОСКОНАЛЕННЯ ПРИСТРОЮ ПЕРВИННОЇ ОБРОБКИ СИГНАЛІВ СТАНЦІЇ НАВЕДЕННЯ

Вурста Ю.І., Скорик А.Б., Лаврик Р.В.
Харківський університет Повітряних Сил імені І. Кожедуба, Харків, Україна
Бритов Д.М.
Державний науково-дослідний інститут випробування та сертифікації озброєння та військової техніки, Чернігів, Україна

Прискорення виявлення повітряних цілей можливо шляхом автоматизації процедур та удосконалення алгоритмів роботи приймальних пристроїв радіотехнічних засобів [1-4]. Разом з тим, удосконалення апаратури та алгоритмів не повинні збільшувати її ваго-габаритні характеристики та час обробки інформації.

Метою доповіді є розробка пропозицій щодо удосконалення виявлення повітряних цілей.

Досліджувались процедури та алгоритми напівавтоматичного виявлення повітряних цілей в сучасних радіотехнічних засобах.

В доповіді наводяться результати аналізу побудови та алгоритмів функціонування пристрою первинної обробки станції наведення при виявленні аеродинамічних цілей.

За результатами досліджень сучасних цифрових пристроїв обробки НВЧ-сигналів наведені пропозицій щодо удосконалення пристрою первинної обробки шляхом впровадження сучасної елементної бази та додаткових алгоритмів функціонування.

Список літератури

1. Вурста Ю. І., Гайбадулов Б. В., Камчатний М. І., Кукобко С. В. Аналіз пристрою первинної обробки багатоканальної радіолокаційної станції середньої дальності спеціального призначення. XVII Міжнародна науково-практична конференція магістрантів та аспірантів «Теоретичні та практичні дослідження молодих вчених» (TPRYS-2023). Харків. 2023.

2. Кукобко С. В., Місценко Р. В., Бритов Д. М., Рощупкін Є. С., Гайбадулов Б. В. Пропозиції щодо автоматизації процесу прийняття рішення при класифікації ситуацій у повітряному просторі. Міжнародна науково-практична конференція "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку". Харків. 2023.

3. Tymchenko S., Kaplun Y., Roshchupkin E., Kukobko S. Substantiation of Time Distribution Law for Modeling the Activity of Automated Control System Operator. Mathematical Modeling and Simulation of Systems. MODS 2022. Lecture Notes in Networks and Systems, vol 667. Springer, Cham.

4. Гайбадулов Б. В., Джус В. В., Коробков Ю. В., Крючков Д. М., Рощупкін Є. С. Тренажні імітаційні комплекси зенітного ракетного озброєння – досвід використання, проблемні питання та пропозиції щодо їх розв'язання. Спільні дії військових формувань і правоохоронних органів держави: Проблеми та перспективи. Одеса. 2022.

РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ НАПРЯМКІВ ПІДВИЩЕННЯ ЯКОСТІ АВТОСУПРОВОДЖЕННЯ МАНЕВРУЮЧИХ ПОВІТРЯНИХ ЦІЛЕЙ БАГАТОКАНАЛЬНОЮ СТАНЦІЄЮ НАВЕДЕННЯ РАКЕТ

Горобинський М.А., Гречка О.В., Овчаренко О.Ю., Сургай В.І.
Харківський університет Повітряних Сил імені І. Кожедуба, Харків, Україна

Одним з способів протидії вогневим засобам ураження з боку повітряних цілей є здійснення ними маневру.

Зрив цілі с супроводження в більшості випадків суттєво знижує імовірність її ураження [1-5].

Метою доповіді є розробка пропозицій щодо удосконалення можливостей багатоканальних радіотехнічних засобів контролю повітряних цілей по виявленню маневру та стійкому супроводженню цілей, що маневрують.

Досліджувались алгоритми виявлення маневру та супроводження маневруючих цілей.

В доповіді наводяться результати аналізу алгоритмів автосупроводження, реалізованих в багатоканальній станції наведення ракет.

Наведено результати досліджень існуючих алгоритмів виявлення маневру та принципів їх функціонування.

Обґрунтовані пропозиції щодо удосконалення алгоритмів автосупроводження повітряних цілей, що реалізуються спеціалізованою цифровою обчислювальною машиною багатоканальної станції наведення ракет.

Список літератури

1. Горобинський М. А., Чміль Ю. О., Борисов В. В., Гречка О. В. Аналіз радіотехнічних алгоритмів автосупроводження БСНР 9С32 ЗРС С-300В1. XVII Міжнародна науково-практична конференція магістрантів та аспірантів «Теоретичні та практичні дослідження молодих вчених» (TPRYS-2023). Харків, 2023.

2. Герасимов С. В., Рощупкін Є. С. Теоретические основы оценки ошибок значений сигналов с гармонически меняющимися параметрами. Озброєння та військова техніка. 2018. № 2. С. 43-49.

3. Крючков Д. М., Рощупкін Є. С., Джус В. В., Титаренко Р. В. Удосконалення підготовки персоналу для обслуговування радіотехнічних засобів контролю повітряного простору шляхом урахування питань технічної експлуатації в тренажних імітаційних комплексах. Сучасні інформаційні системи. 2020. Т. 4, № 3. С. 89-93.

4. Асавалюк А. В., Герасимов С. В., Рощупкін Є. С. Похибки визначення повного вектора швидкості в єдиній прямокутній системі координат системою оглядових станцій радіолокації с різною точністю. Системи озброєння і військова техніка. 2017. № 2. С. 53-56.

5. Герасимов С. В., Рощупкин Е. С., Федак Г. А., Бабий Я. В. Оценка параметров движения маневрирующих воздушных объектов в активной некогерентной системе при обработке информации от нескольких неравноточных источников с разным темпом обзора пространства. Військово-технічний збірник. 2012. № 1. С. 18-26..

ПРОПОЗИЦІЇ ЩОДО УДОСКОНАЛЕННЯ ПРОТИДІЇ БАЛІСТИЧНИМ ЗАСОБАМ

Кісіль О.А., Коробков Ю.В.
Харківський університет Повітряних Сил імені І. Кожедуба, Харків, Україна
Веретенніков І.М.
Національний технічний університет "ХПІ", Харків, Україна
Даниленко О.В.
Державний науково-дослідний інститут випробування та сертифікації озброєння та військової техніки, Чернігів, Україна

Сучасні повномасштабні бойові дії характеризуються широким застосуванням балістичних засобів нападу та пошуку ефективних шляхів протидії ним [1-5].

Метою доповіді є забезпечення знищення балістичних цілей зенітною ракетною батареєю.

Досліджувались характеристики балістичних засобів нападу та заходи протидії ним. В доповіді наводяться тенденції розвитку сучасних засобів протиракетної оборони.

Запропонований метод визначення дальності та радіальної швидкості балістичної цілі, та схема пристрою, що його реалізує.

Подальші дослідження будуть спрямовані на пошук елементної бази, що дозволить реалізувати запропонований пристрій, який працює за наведеним методом.

Список літератури

1. Кісіль О. А., Герасимов С. В., Джус В. В., Гордієнко Р. О., Титаренко Р. В. Аналіз балістичних засобів нападу як цілей ЗРС С-300В1. XVI Міжнародна науково-практична конференція магістрантів та аспірантів "Теоретичні та практичні дослідження молодих вчених" (TPRYS-2022), Харків. 2022.
2. Кісіль О. А., Чміль Ю. О., Сургай М. В., Борисов В. В., Гречка О. В., Гордієнко Р. О. Аналіз роботи ЗРК С-300В1 при роботі з балістичними цілями. Міжнародна науково-практична конференція “Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку”: Збірник тез доповідей. Харків. 2023. С. 188-189.
3. Ліцман А. М., Калугін Д. С., Рощупкін Є. С., Скопінцев О. О., Туленко М. В. Дослідження ураження типових групових об'єктів військового призначення при веденні бойових дій (проведення операцій) в сучасних умовах. Спільні дії військових формувань і правоохоронних органів держави: Проблеми та перспективи. Одеса. 2019.
4. Бєляєв Д. М., Кукобко С. В., Ліцман А. М., Рощупкін Є. С. Пропозиції щодо використання багатопозиційних систем для виявлення балістичних, аеробалістичних та аеродінамичних цілей з визначенням координат точок їх пуску. Спільні дії військових формувань і правоохоронних органів держави: Проблеми та перспективи. Одеса. 2019.
5. Herasimov S., Borysenko M., Roshchupkin E. et al. Spectrum Analyzer Based on a Dynamic Filter. J El ectron Test. 2021. № 37. P.p. 357-368. DOI: https://doi.org/10.1007/s10836-021-05954-0.

ПРОПОЗИЦІЇ ЩОДО ПОБУДОВИ ТА ФУНКЦІОНУВАННЯ СИСТЕМИ СИНХРОНІЗАЦІЇ БАГАТОКАНАЛЬНОЇ СТАНЦІЇ НАВЕДЕННЯ

Марченко Б.С., Галицький О.Ф., Сургай М.В.
Харківський університет Повітряних Сил імені І. Кожедуба, Харків, Україна
Горбань Г.В.
Державний науково-дослідний інститут випробування та сертифікації озброєння та військової техніки, Чернігів, Україна

Функціонування радіотехнічних засобів контролю повітряного простору забезпечується системою синхронізації, до якої на цей час висуваються достатньо жорсткі вимоги [1-5]. Це свідчить про актуальність проведених досліджень.

Метою доповіді є забезпечення стабільності функціонування багатока-нальної станції наведення ракет.

Досліджувались апаратура та алгоритми функціонування високостабільних пристроїв генерації сигналів.

В доповіді наводяться результати аналізу роботи системи синхронізації багатоканальної станції наведення ракет.

Розглянуті сучасні пристрої формування високостабільних сигналів на новітній елементній базі.

Наведено пропозиції з побудови системи синхронізації синхронізації багатоканальної станції наведення з застосуванням сучасних технологій.

Список літератури

1. Марченко Б. С., Чміль Ю. О., Сургай М. В., Борисов В. В., Гречка О. В. Пропозиції щодо удосконалення роботи багатоканального радіотехнічного засобу середньої дальності спеціального призначення при роботі по повітряних цілях в різних режимах роботи. XVI Міжнародна науково-практична конференція магістрантів та аспірантів "Теоретичні та практичні дослідження молодих вчених" (TPRYS-2022). Харків. 2022.

2. Марченко Б. С., Джус В. В., Сургай М. В., Борисов В. В. Пропозиції щодо удосконалення роботи систем радіотехнічного засобу спеціального призначення з сигналами різних типів, при переході з режиму у режим та зміні типів сигналів. Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. Тези доповідей тринадцятої міжнародної науково-технічної конференції. Баку-Харків-Жиліна. 2023. Том 1: секції 1, 3, 4,

3. Рощупкін Є., Герасимов С., Кукобко С. та інш. Постановка проблеми створення та експлуатації багатопозиційних систем інформаційного забезпечення та шляхи її розв'язання. Грааль науки, 2021. № 4. С. 243-252.

4. Artikula A., Britov D., Dzhus V. and etc. Measurement errors affecting the characteristics of multi-position systems, and ways to reduce them. InterConf. 2021. 333-346.

5. Herasimov S., Borysenko M., Roshchupkin E. et al. Spectrum Analyzer Based on a Dynamic Filter. J El ectron Test. 2021. № 37. Pp. 357-368. DOI: https://doi.org/10.1007/s10836-021-05954-0.

ОЦІНКА ЕФЕКТИВНОСТІ ВИКОНАННЯ ЗАВДАНЬ ЗА ПРИЗНАЧЕННЯМ В ПРИБЕРЕЖНИХ РАЙОНАХ

Молчанов Д.В., Закутін К.В., Титаренко Р.В.
Харківський університет Повітряних Сил імені І. Кожедуба, Харків, Україна
Магу О.М.
Державний науково-дослідний інститут випробування та сертифікації озброєння та військової техніки, Чернігів, Україна

Велика протяжність морських кордонів та агресивна політика сусідньої держави викликають необхідність забезпечення задач оборони з боку морської акваторії, виявлення загроз з якої має свою специфіку [1-5].

Метою доповіді є підвищення ефективності виконання завдань за призначенням угрупувань військ в прибережних районах.

Досліджувались особливості розповсюдження електромагнітних хвиль над морською поверхнею.

Наведено результати характеристик розсіювання надводних об'єктів та низьковисотних об'єктів, що рухаються над на тлі перевідбиттів від морської поверхні. Досліджувались залежності характеристик виявлення та супроводження цих об'єктів радіолокаційними засобами різних діапазонів хвиль в залежності від стану водної поверхні.

В доповіді наведені пропозиції щодо оптимізації номенклатури та роз-міщення радіолокаційних засобів виявлення об'єктів в прибережних районах.

Список літератури

1. Молчанов Д. В., Василець В. О., Сухаревський О. І. Моделювання характеристик розсіяння великого десантного корабля. Зб. наук. пр. Харків. ун-ту Повітр. сил. 2016. Вип. 2. С. 76-78.

2. Молчанов Д. В., Василець В. О., Сухаревський О. І. Метод розрахунку характеристик розсіяння надводних радіолокаційних об'єктів. Наука і техніка Повітр. сил Збройн. сил України. 2016. № 1. С. 72-75.

3. O. Sukharevsky, S. Nechitaylo, V. Vasilets and I. Ryapolov. Calculation Method for High-Resolution Range Profiles of Complex Shape Radar Objects. 2020 IEEE Ukrainian Microwave Week (UkrMW). Kharkiv, Ukraine. 2020. Pp. 1026-1029. DOI: https://doi.org/10.1109/UkrMW49653.2020.9252634.

4. Сухаревский О. И., Шрамков А. Ю., Рощупкин Е. С. Высокочастотный метод расчета диаграммы направленности антенны с учетом неоднородностей рельефа местности на позиции РЛС. Моделювання та інформаційні технології. 2005. № 33. С. 174-181.

5. Кукобко С. В., Місценко Р. В., Британов Д. М., Рощупкін Є. С., Гайбадулов Б. В. Пропозиції щодо автоматизації процесу прийняття рішення при класифікації ситуацій у повітряному просторі. Міжнародна науково-практична конференція "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку". Харків. 2023.

ПРОПОЗИЦІЇ ЩОДО ПІДВИЩЕННЯ ПЕРЕШКОДОСТІЙКОСТІ АПАРАТУРИ ОБМІНУ ІНФОРМАЦІЄЮ МІЖ ЗАСОБАМИ ЗЕНІТНОГО РАКЕТНОГО КОМПЛЕКСУ

Панько М.О., Шулежко В.В., Моргун Є.В., Ткач В.І.
Харківський університет Повітряних Сил імені І. Кожедуба, Харків, Україна

Функціонування будь-якого зенітного ракетного комплексу та захищеність його від сучасної керованої зброї суттєво залежить від характеристик засобів зв'язку, що забезпечують його роботу [1-5].

Метою доповіді є розробка пропозицій щодо удосконалення перешкодостійкості стійкого обміну інформацією між бойовими засобами комплексу.

Досліджувались сучасні засоби зв'язку та принципи їх функціонування.

В доповіді наводяться результати аналізу існуючого обміну інформацією між різними засобами зенітного ракетного комплексу в складній перешкодовій обстановці.

Наведено результати досліджень сучасних засобів зв'язку та принципів забезпечення їх перешкодозахисту, що може бути використано в зенітному ракетному комплексі. Запропоновано шляхи побудови пристроїв спряження засобів зв'язку з апаратурою комплексу та алгоритмів їх роботи.

Обґрунтовано пропозиції щодо потрібної для зенітної ракетної батареї номенклатури та кількості засобів зв'язку.

Список літератури

1. Молчанов Д. В., Василець В. О., Сухаревський О. І. Моделювання характеристик розсіяння великого десантного корабля. Зб. наук. пр. Харків. ун-ту Повітр. сил. 2016. Вип. 2. С. 76-78.

2. Молчанов Д. В., Василець В. О., Сухаревський О. І. Метод розрахунку характеристик розсіяння надводних радіолокаційних об'єктів. Наука і техніка Повітр. сил Збройн. сил України. 2016. № 1. С. 72-75.

3. O. Sukharevsky, S. Nechitaylo, V. Vasilets and I. Ryapolov. Calculation Method for High-Resolution Range Profiles of Complex Shape Radar Objects. 2020 IEEE Ukrainian Microwave Week (UkrMW). Kharkiv, Ukraine. 2020. Pp. 1026-1029. DOI: https://doi.org/10.1109/UkrMW49653.2020.9252634.

4. Сухаревский О. И., Шрамков А. Ю., Рощупкин Е. С. Высокочастотный метод расчета диаграммы направленности антенны с учетом неоднородностей рельефа местности на позиции РЛС. Моделювання та інформаційні технології. 2005. № 33. С. 174-181.

5. Кукобко С. В., Місценко Р. В., Британов Д. М., Рощупкін Є. С., Гайбадулов Б. В. Пропозиції щодо автоматизації процесу прийняття рішення при класифікації ситуацій у повітряному просторі. Міжнародна науково-практична конференція "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку". Харків. 2023.

РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ НАПРЯМКІВ УДОСКОНАЛЕННЯ ПРИЙМАЛЬНО-ПЕРЕДАВАЛЬНОГО ТРАКТУ БАГАТОКАНАЛЬНОЇ СТАНЦІЇ НАВЕДЕННЯ

Соболь М.Р., Крючков Д.М., Кущ П.С., Олійник Ю.В.
Харківський університет Повітряних Сил імені І. Кожедуба, Харків, Україна

Приймально-передавальні системи радіотехнічних засобів контролю повітряного простору визначають їх основні можливості по виявленню та супроводженню повітряних цілей, перешкодостійкість та захищеність від протирадіолокаційних засобів ураження [1-5].

Метою доповіді є розробка пропозицій щодо підвищення можливостей багатоканальної станції наведення ракет по виявленню та супроводженню повітряних цілей.

Досліджувались приймально-передавальні системи існуючих та перспективних радіотехнічних засобів.

В доповіді наводяться результати аналізу пропозицій щодо удосконалення приймально-передавального тракту багатоканальної станції наведення ракет та досліджень щодо побудови, принципів дії та елементної бази сучасних активних фазованих антенних решіток

Обґрунтовано пропозиції щодо впровадження активної фазованої антенної решітки в багатоканальну станцію наведення ракет та обґрунтування можливої до використання елементної бази.

Список літератури

1. Соболь М. Р., Герасимов С. В., Джус В. В., Титаренко Р. В. Аналіз антенно-хвилеводної системи багатоканальної радіолокаційної станції середньої дальності спеціального призначення. XVII Міжнародна науково-практична конференція магістрантів та аспірантів «Теоретичні та практичні дослідження молодих вчених» (TPRYS-2023). Харків.

2. Кузьменко Д. В., Рощупкін Є. С., Джус В. В. Удосконалення системи управління променем багатоканальної радіолокаційної станції спеціального призначення. XV Міжнародна науково-практична конференція магістрантів та аспірантів «Теоретичні та практичні дослідження молодих науковців» (TPRYS-2021). Харків. 2021.

3. Herasimov S., Roshchupkin E., Kutsenko V. Statistical analysis of harmonic signals for testing of Electronic Devices, International Journal of Emerging Trends in Engineering Research, Vol.8, is. 7. 2020. Pp. 3791-3798.

4. Brytov O., Bieliaiev D., Kukobko S., Chmil Y., Dzhus V., Herasymov S., Korobkov Y., Pomohaiev I., Roshchupkin Y. Justification of the method of evaluation of the efficiency of air reconnaissance by unmanned aviation of ground (sea) objects. InterConf, 2021. (93). Pp. 471-485.

5. Герасимов С. В., Кадубенко С. В., Рощупкін Є. С., Ліцман А. М. Контроль частотного розподілення радіосигналів при управлінні зенітними керованими ракетами. Інформаційні технології: наука, техніка, технологія, освіта, здоров'я (MicroCAD-2020). Харків: НТУ "ХПІ". 2020.

ПРОПОЗИЦІЇ ЩОДО УДОСКОНАЛЕННЯ ПРОТИДІЇ БПЛА ЗЕНІТНОЮ РАКЕТНОЮ БАТАРЕЄЮ

Швидкий А.В., Борисов В.В.., Камчатний М.І.
Харківський університет Повітряних Сил імені І. Кожедуба, Харків, Україна
Кукобко С.В.
Державний науково-дослідний інститут випробування та сертифікації озброєння та військової техніки, Чернігів, Україна

Досвід російсько-Української війни виявив тенденцію щодо зростання застосування безпілотних літальних апаратів (БПЛА) для виконання різноманітних задач, в тому числі і для нанесення ударів по критичних об’єктах інфраструктури держави: енергетичному комплексу, мостам, тощо [1-4].

Метою доповіді є забезпечення знищення БПЛА зенітною ракетною батареєю, озброєною зенітним ракетним комплексом.

Досліджувались характеристики багатоканальної станції наведення та сучасних БПЛА.

В доповіді наводяться результати аналізу застосування БПЛА в сучасних збройних конфліктах та характеристики їх ефективних поверхонь розсіювання. Розраховані дальності виявлення БПЛА багатоканальною станцією наведення та запропоновані технічні рішення щодо їх збільшення.

Наведено пропозиції щодо розташування мобільних вогневих груп в залежності від характеристик повітряного удару з застосуванням безпілотних засобів нападу.

Список літератури

1. Швидкий А. В., Рощупкін Є. С., Кукобко С. В., Шулежко В. В., Коробков Ю. В. Аналіз безпілотних літальних апаратів як цілей для зенітного ракетного комплексу С-300В1. XVI Міжнародна науково-практична конференція магістрантів та аспірантів "Теоретичні та практичні дослідження молодих вчених" (TPRYS-2022) Харків. 2022.

2. Швидкий А. В., Крючков Д. М., Шулежко В. В., Коробков Ю. В., Борисов В. В. Аналіз роботи БСНР 9С32 при виявленні та супроводжені БПЛА. Міжнародна науково-практична конференція “Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку”: Збірник тез доповідей. Харків: НАНГУ. 2023. С.182-184.

3. Herasimov S. V., Kukobko S. V., Roshchupkin E. S., Roshchupkina A. E. Assessment of possibilities of detection and tracking of drones the system of radiolocation stations of antiaircraft defense. Інформаційні технології: наука, техніка, технологія, освіта, здоров'я (MicroCAD-2020). Харків. 2020. С. 270.

4. Кукобко С. В., Рощупкін Є. С. Оцінювання радіолокаційної помітності безпілотних літальних апаратів як цілей для засобів радіолокації протиповітряної оборони Сухопутних військ / С.В. Кукобко, Є.С. Рощупкін // Інформаційні технології: наука, техніка, технологія, освіта, здоров’я: тези доповідей XXVII міжнародної науково-практичної конференції MicroCAD-2019, 15–17 травня 2019 р.: у 5 ч. Ч. V. / за ред. проф. Сокола Є.І. – Харків: НТУ “ХПІ”. – С. 99.

ESTIMATION OF THE HEATING TEMPERATURE OF SINGLE-CORE WIRES WITH IMPURITIES IN THE CORE MATERIALS

Katunin A.M.
National University of Civil Defense of Ukraine;
National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine
Kolomiitsev O.V.
National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine

The main physical characteristic of the materials (metals) used to conduct current in cable products is electrical conductivity. These materials, as components of products, are subject to requirements for mechanical properties that are determined by the specifics of their operation. The main requirement is metal strength.

The purpose of the report is to estimate the heating temperature of single-core wires with impurities in the core materials.

Increased strength is achieved by introducing impurity elements that reduce the electrical conductivity of the conductor metal. The double oppositely directed effect of impurities makes it necessary to look for ways to optimize the use of impurity elements in the metals of conductive cores of cable products. To this end, it is necessary to investigate the mechanisms of impurities' influence on the electrical conductivity of conductor metals and to estimate the heating temperature of cable products. Reference [1] provides data on the effect of impurities on the electrical resistance of copper and shows that even when 0.1% silver, a metal with a lower resistivity, is added to copper, the overall resistance of the metal alloy increases by several percent. Impurities such as phosphorus, iron, cobalt, and arsenic increase the electrical resistance and, consequently, reduce the electrical conductivity of copper.

The report presents the results of estimating the heating temperature of single-core wires with impurities in the core materials.

The results of calculations of the heating temperature of single-core wires with different impurities in the material of the conductor during operation allow us to state the following: the heating temperature of the wire during its operation significantly depends on the presence of impurities present in the material of the conductor; temperature and time characteristics of the operation of wires with different impurities in the material of conductors have approximately the same nonlinear character; with an increase in the operating time, the influence of impurities on the increase in the heating temperature of the wire increases.

References

1. Katunin, A., Kolomiitsev, O., Kulakov, O., Heiko, H., & Rudakov, I. (2023, October). Information technologies for calculating the effect of wire thickness and insulation material on its heating temperature during operation. In 2023 IEEE 4th KhPI Week on Advanced Technology (KhPIWeek) (pp. 1-5). IEEE.

PROPOSALS FOR ROUTE PLANNING AND FLIGHT CONTROL OF UNMANNED AERIAL VEHICLES TO IMPROVE FLIGHT SAFETY IN URBAN AREAS BASED ON MACHINE LEARNING TECHNOLOGIES

Kolomiitsev O.V., Rudakov I.S., Liubchenko O.V.,
Biesova A.O., Kolomiitsev V.O.
National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine

The development prospects of unmanned aerial vehicles (UAVs) are associated with their group use, with the creation of large groups of diverse information-related vehicles acting together in the interests of a common task. UAVs have a wide range of applications in the urban environment and can improve the efficiency and safety of many aspects of city life.

In order to successfully plan routes and manage UAV flights in urban areas, it is important to follow all relevant rules and restrictions to ensure safety, efficiency and successful completion of the tasks.

The task of routing a UAV is to determine a set of points in space that would correspond to its flight path and be identified on a map.

The following factors influence the choice of route: limited flight time, flight safety, and multiple routes. The specifics of the UAV group management task is the sequence of decision-making tasks and, to a lesser extent, dynamic tasks for implementing these decisions.

The aim of the report is to improve the safety of UAV flights in urban areas based on machine and deep learning technologies.

The report presents the results of the study of graph search methods and multi-agent algorithms: ant algorithm and "query-response-agreement" algorithm. The integration of graph search and multiagent search, which work in parallel, is proposed.

The formalisation of multifunctional UAVs for group performance of one or more tasks (influence functions) is carried out.

The problem of group behaviour of UAVs for the application of artificial intelligence (machine learning) technologies and trends in the creation of algorithms that can learn are presented. The main elements of the system of relations and conditions for the effectiveness of performing tasks during the control of a UAV group and actions in the group are formulated.

References

1. Коломійцев, О., Альошин, Г., Пустоваров, В., Третяк, В., Никорчук, А., & Споришев, К. (2020). Підвищення точності сегментації міських будов на цифрових космічних та аерофотознімках при автоматизованому моніторингу міського середовища. *Збірник наукових праць ЛОГОС,* 40-45. https://doi.org/10.36074/09.10.2020.v2.10.

PROPOSALS FOR THE DEVELOPMENT OF A DEVICE FOR THE TRANSMISSION OF INFORMATION USING LASER RADIATION IN THE "LAST MILE" TECHNOLOGY

Kolomiitsev O.V., Lvov A.S.
National Technical University “Kharkiv Polytechnic Institute”, Kharkiv, Ukraine
Komarov V.O.
Kruty Heroes Military Institute of Telecommunications
and Information Technology, Kyiv, Ukraine

Prospects for the development of laser communication, which transmits information using electromagnetic waves of the optical range, are associated with high bandwidth due to the high value of the carrier frequency and the ability to transmit large amounts of information at high speed. In addition, the small angular divergence of laser radiation (LR) provides spatial concealment and high energy stability of information transmission over an optical communication channel with relatively small dimensions of transceiver devices.

Therefore, the LW is actively used in atmospheric optical communication lines (AOCL). This technology creates reliable communication channels at distances from 100 to 7000 m in the atmosphere and up to 100,000 km in outer space, for example, for communication between satellites.

The purpose of the report is to increase the amount of information transmitted by laser radiation in the last mile technology.

The report presents the results of a study of wireless information transmission in the short-wave part of the electromagnetic spectrum.

It is noted that the main advantages of this method of information transmission include: high transmission speed, ease of installation and no need to pay for the use of the frequency range.

According to the price-quality criterion, AOCL is the best solution to the "last mile" problem with high security of the communication channel. Connecting a new cluster of clients to the access node via a dedicated high-speed communication line within one day without obtaining a radio frequency permit and leasing lines. The necessity of using the spectrum features of a single-mode multi-time division multiple-access line LR with synchronization of longitudinal modes is substantiated. A device for separating carrier frequencies from this spectrum for further modulation with information is proposed.

References

1. Альошин Г. В. Ефективність лазерних інформаційно-вимірювальних систем / Г. В. Альошин, О. В. Коломійцев, В. В. Посохов, С. І. Клівець // Збірник наукових праць Харківського національного університету Повітряних Сил. - 2018. - № 2. - С. 59-65. - Режим доступу: http://nbuv.gov.ua/UJRN/ZKhUPS_2018_2_9.

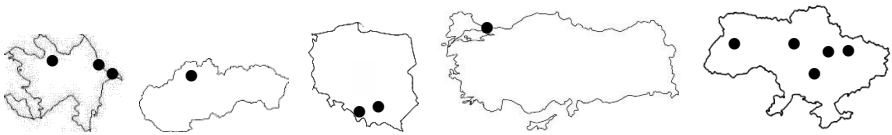
УЧАСНИКИ КОНФЕРЕНЦІЇ (секції 3, 4, 5, 6)

ОРГАНІЗАЦІЇ, ЯКІ ПРИЙНЯЛИ УЧАСТЬ У КОНФЕРЕНЦІЇ

Азербайджанський технічний університет, Баку, Азербайджан
Академія державної прикордонної служби, Баку, Азербайджан
Бакинський державний університет, Баку, Азербайджан
Бакинський інженерний університет, Баку, Азербайджан
Військовий науково-дослідний інститут, Баку, Азербайджан
Військовий інститут імені Гейдара Алієва, Баку, Азербайджан
Державна служба спеціального зв'язку та захисту інформації України, Київ, Україна
Державний біотехнологічний університет, Харків, Україна
Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, Черкаси, Україна
Державний університет інфраструктури та технологій, Київ, Україна
Інститут військового управління, Баку, Азербайджан
Інститут геології та геофізики, Баку, Азербайджан
Інститут систем управління Азербайджанської Національної академії наук, Баку, Азербайджан
Київський національний університет будівництва і архітектури, Київ, Україна
Кіровоградська льотна академія, Кропивницький
Космічне агентство Азербайджанської Республіки, Баку, Азербайджан
Мінгечавірський державний університет, Мінгечавір, Азербайджан
Національна авіаційна академія, Баку, Азербайджан
Національна академія Національної гвардії України, Харків, Україна
Національна академія сухопутних військ імені гетьмана Петра Сагайдачного, Львів, Україна
Національне аерокосмічне агентство, Баку, Азербайджан
Національний авіаційний університет, Київ, Україна
Національний аерокосмічний університет імені М. Є. Жуковського "Харківський авіаційний інститут", Харків, Україна
Національний технічний університет "Харківський політехнічний інститут", Харків, Україна
Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сикорського", Київ, Україна
Національний університет «Львівська політехніка», Львів, Україна

Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна
Національний університет оборони Азербайджанської республіки, Баку, Азербайджан
Національний університет оборони України, Київ, Україна
Національний університет цивільного захисту України, Харків, Україна
Педагогічний університет імені Комісії Національної Освіти в Кракові, Краків, Польща
Представництво «Оракл Іст Сентрал Юроп Сервісис Б.В.», Київ, Україна
Республіканський центр сейсморозвідки, Баку, Азербайджан
Стамбульський університет Cerrahpasa, Стамбул, Туреччина
Сумгаїтський державний університет, Сумгаїт, Азербайджан
Український державний університет залізничного транспорту, Харків, Україна
Університет міста Жиліна, Жиліна, Словаччина
Університет технології і гуманітарних наук, Бельсько-Бяла, Польща
Харківський військовий інститут танкових військ, Харків, Україна
Харківський національний автомобільно-дорожній університет, Харків, Україна
Харківський національний університет внутрішніх справ, Харків, Україна
Харківський національний економічний університет імені Саймона Кузнеця, Харків, Україна
Харківський національний університет імені В.Н. Каразіна, Харків, Україна
Харківський національний університет міського господарства імені О.М. Бекетова, Харків, Україна
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна
Харківський національний університет радіоелектроніки, Харків, Україна

АФІЛЯЦІЯ УЧАСНИКІВ КОНФЕРЕНЦІЇ



ЗМІСТ

НАУКОВЕ ВИДАННЯ

СУЧАСНІ НАПРЯМИ РОЗВИТКУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЗАСОБІВ УПРАВЛІННЯ

Тези доповідей
чотирнадцятої міжнародної науково-технічної конференції
(25 – 26 квітня 2024 року)
Том 2: секції 3, 4, 5, 6

Відповідальний за випуск *В. В. Косенко*
Технічний редактор *І. А. Лєбедева*
Коректор *В. В. Богомаз*
Комп'ютерне складання та верстання *Н. Г. Кучук*

Адреса оргкомітету: вул. Кирпичова, 2, Харків, 61002, Україна
Вечірній корпус, кімната 314
тел. +38 (057) 707 61 65

Підписано до друку 18.04.2024 Формат 60 × 84/16
Ум.-вид. арк. 9,0 . Тираж 100 пр. Зам. 419-24

Віддруковано з готових оригінал-макетів у цифровій друкарні Impress
61002, м. Харків, вул. Пушкінська, 56, тел. **+ 38 (057) 714-52-11**
e-mail: **irina@impress.biz.ua**