Інститут систем управління
МНО Азербайджанської республіки

Національний технічний університет
"Харківський політехнічний інститут"

Харківський національний
університет радіоелектроніки

Національний аерокосмічний університет
імені М. Є. Жуковського
"Харківський авіаційний інститут"

Університет технології і гуманітарних наук
(м. Бельсько-Бяла, Польща)

ПРОБЛЕМИ ІНФОРМАТИЗАЦІЇ

Тези доповідей тринадцятої міжнародної
науково-технічної конференції

27 – 28 листопада 2025 року

Том 2: секції 3, 7

Баку – Харків – Бельсько-Бяла –2025

УДК 004 : 681.3 doi: https://doi.org/10.32620/PI.25.t2

У збірнику подано тези доповідей тринадцятої міжнародної науково-технічної конференції “Проблеми інформатизації”. Розглянуті питання за такими напрямами: інформатизація навчального процесу; застосування, експлуатація та безпека функціонування телекомунікаційних систем та мереж; комп’ютерні методи і засоби інформаційних технологій та управління; методи швидкої та достовірної обробки даних в комп’ютерних системах та мережах; цивільна безпека та захист критичної інфраструктури (інформаційна підтримка); сучасні інформаційно-вимірювальні системи.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ

Institute of Control Systems
of the Ministry of Science and Education
of the Republic of Azerbaijan

National Technical University
Kharkiv Polytechnic Institute

Kharkiv National University
of Radio Electronics

National Aerospace University
Kharkiv Aviation Institute

University of Bielsko-Biala

PROBLEMS OF INFORMATIZATION

Proceedings of 13-th International
Scientific and Technical Conference

November 27 – 28, 2025

VOLUME 2: SECTIONS 3, 7

Baku – Kharkiv – Bielsko-Biala –2025

UDC 004 : 681.3 doi: https://doi.org/10.32620/PI.25.t2

The collection presents abstracts of reports of the Thirteenth International Scientific and Technical Conference "Problems of Informatization". Issues in the following areas are considered: informatization of the educational process; application, operation and safety of telecommunication systems and networks; computer methods and means of information technology and management; methods of fast and reliable data processing in computer systems and networks; civil security (information support); modern information and measurement systems.

ORGANIZING COMMITTEE

Тринадцята міжнародна науково-технічна конференція “Проблеми інформатизації” проводиться 27 та 28 листопада 2025 року в режимі ONLINE.

Тези доповідей доступні в INTERNET.

ТОМ 1

СЕКЦІЯ 1. Інформатизація навчального процесу.

Керівниця секції: д.т.н. проф. Н. Г. Кучук, НТУ «ХПІ», Харків.
Секретарка секції: к.т.н. доц. О. М. Бельорін-Еррера, НТУ «ХПІ», Харків.

СЕКЦІЯ 2. Застосування та експлуатація телекомунікаційних систем та мереж.

Керівник секції: д.т.н. проф. Г. А. Кучук, НТУ «ХПІ», Харків.
Секретар секції: к.т.н. доц. С. С. Бульба, НТУ «ХПІ», Харків.

ТОМ 2

СЕКЦІЯ 3. Безпека функціонування телекомунікаційних систем та мереж.

Керівник секції: д.т.н. проф. О. О. Можаєв, ХНУВС, Харків.
Секретар секції: к.т.н. доц. О. В. Сєвєрінов, ХНУРЕ, Харків.

СЕКЦІЯ 7. Сучасні інформаційно-вимірювальні системи.

Керівник секції: д.т.н. проф. О. В. Коломійцев, НТУ «ХПІ», Харків.
Секретар секції: к.т.н. доц. А. О. Подорожняк, НТУ «ХПІ», Харків.

ТОМ 3

СЕКЦІЯ 4. Комп’ютерні методи і засоби інформаційних технологій та управління.

Керівники секції: д.т.н. проф. І. В. Рубан, ХНУРЕ, Харків.
д.т.н. проф. А. А. Коваленко, ХНУРЕ, Харків.
Секретар секції: к.т.н. доц. О. С. Ляшенко, ХНУРЕ, Харків.

ТОМ 4

СЕКЦІЯ 5. Методи швидкої та достовірної обробки даних в комп’ютерних системах та мережах.

Керівник секції: д.т.н. проф. В. В. Косенко, НУ ПП, Полтава.
Секретар секції: к.т.н. доц. Д. О. Лисиця, НТУ «ХПІ», Харків.

СЕКЦІЯ 6. Цивільна безпека та захист критичної інфраструктури.

Керівник секції: д.т.н. проф. О. В. Третьяков, ДУ «КАІ», Київ.
Секретар секції: к.т.н. доц. Є. В. Доронін, ДУ «КАІ», Київ.

СЕКЦІЯ 3
БЕЗПЕКА ФУНКЦІОНУВАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

Керівник секції: д.т.н. проф. О. О. Можаєв, ХНУВС, Харків
Секретар секції: к.т.н. доц. О В. Сєвєрінов, ХНУРЕ, Харків

RADIO ANALYSIS OF TELEMETRY INDICATORS OF UNMANNED AERİAL VEHICLES IN ELECTRONIC WARFARE CONDITIONS

Rustamov A.R., Gasanov A.G.
National Defense University, Baku, Azerbaijan
Azizullayev M.G.
National Aerospace Agency, Baku, Azerbaijan
Hasanli R.A.
Sumqait State University, Sumqait, Azerbaijan

Signal power loss and signal-to-noise ratio (SNR) models for analyzing the performance of the control system of unmanned aerial vehicles in radio electronic warfare conditions Research has been conducted on the development of mathematical models of communication organization for quadcopters and their application.

These models are considered important for increasing the effectiveness of unmanned aerial vehicles and ensuring their survivability in radio electronic warfare conditions [1-10].

Mathematical calculations and laboratory tests show that the communication performance of the telemetry module of unmanned aerial vehicles in radio electronic warfare conditions is significantly dependent on the distance and the effects of the electromagnetic environment. Thus, at distances of 100–300 meters, the signal reception quality remains at a satisfactory level. However, after 400 meters, the SNR values drop below 10 dB, which weakens the reliability of communication and significantly increases the probability of errors in data transmission.

A quadcopter equipped with a cost-effective XBee PRO S2C module was successfully tested in a laboratory-built radio electronic warfare environment. As a result of integrating Raspberry Pi-4-based native software into the control system, stable flight of the quadcopter was ensured. The results show that the XBee PRO S2C module can provide effective and stable control even in radio electronic warfare conditions.

Path loss, effective noise (radio electronic warfare and thermal), and effective signal-to-noise ratio (SNR) are reliable mathematical formulas for evaluating and improving system performance. Through them, it was possible to predict how the XBee PRO S2C module would perform over different distances and conditions.

The results obtained show that in practical applications, antenna protection should be increased, technical measures such as frequency change, cryptographic

protection and failure protection, and autonomous mechanisms should be implemented to maintain communication stability.

Overall, mathematical and experimental analyses provide an important scientific basis for the effective and safe control of unmanned aerial vehicles in radio electronic warfare conditions.

References

1. Rustamov, A.R., Gasanov, A.G., Azizullayev, M.G. (2024). Analysis of modules and systems used in effective control of UAVs in radio electronic combat environment. International Scientific and Technical Conference.

2. Rustamov, A.R., Gasanov, A.G., Azizullayev, M.G. (2024). The role of navigational and hydrographical support in ensuring security of the Caspian Sea. 2nd International Conference on Logistics, Transport and Distribution in the Caspian Region, May 15-17, Baku, Azerbaijan.

3. Rustamov, A.R., Gasanov, A.G., Azizullayev, M.G. (2024). Effective application of telemetry systems in unmanned aerial vehicles. Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. Тези доповідей чотирнадцятої міжнародної науково-технічної конференції 25 - 26 квітня, Vol. 2: sections 3, 4, 5, 6, pp. 66-70.

4. Piriyev G. K. et al. Modelling of the battle operations //Monografiya, Herbi Nashriat", Baku. – 2017.

5. Hasanov A. H. 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.

6. Hashimov E.G. et al. Mathematical modeling of military systems. Textbook. -Baku: Military publishing house, -2018. -266 p.

7. Alieva, R. A., Pashaev, F. G., Gasanov, A. G., & Mahmudov, K. T. (2009). Quantum-chemical calculations of the tautomeric forms of azo derivatives of acetylacetone and determination of the stability constants of their complexes with rare-earth metals. *Russian Journal of Coordination Chemistry*, *35*(4), 241-246.

8. Gadzhieva S. R. et al. Thermodynamic characteristics of metal complexation with 3-[4-iodophenylazo]-2, 4-pentanedione in an aqueous ethanol solution //Russian Journal of Inorganic Chemistry. – 2007. – T. 52. – №. 4. – C. 640-644.

9. Aliyev A. A. et al. Earthquake and activation of mud volcano (causal link and interaction) //Proc. Geol. Inst. – 2001. – T. 29. – C. 26-39.

10. Ahmadov A. I. et al. Calculation of the Energy of the Interelectron Interaction in Molecules in a Basis of Slater Functions //Russian Physics Journal. – 2019. – T. 61. – №. 10. – C. 1848-1854.

11. İbrahimov, B.G. et al. (2022). Research and analysis indicators fiber-optic communication lines using spectral technologies. *Advanced information systems*, *6*(1), 61-64.

12. Ibrahimov, B.G. et al. (2024). Research and analysis mathematical model of the demodulator for assessing the indicators noise immunity telecommunication systems. *Advanced Information Systems*, *8*(4), 20-25.

A JAVA-BASED CRYPTOGRAPHIC ANALYSIS APPLICATION FOR WIRELESS NETWORK SECURITY

Abaszade E.V.
Azerbaijan Technical University, Baku, Azerbaijan

Wireless security plays a crucial role in safeguarding sensitive information and mitigating potential risks associated with the increasing use of handheld devices. The ease with which these devices access networks and exchange data introduces new security challenges that organizations must address. The evolving capabilities of handheld devices, coupled with their enhanced computing power, necessitate a careful assessment of the security risks they pose to an organization's computing environment [1, 2]. Security risks in wireless communication environments encompass the loss of confidentiality, integrity, and network availability. Confidentiality, as a fundamental security requirement, faces unique challenges in wireless networks due to the broadcast nature of wireless technology. Unlike traditional wired networks, adversaries can access network resources without tapping into a physical cable, making confidentiality harder to maintain [3, 4]. This susceptibility is compounded by the inability to control the distance over which wireless transmissions occur, diminishing the effectiveness of traditional physical security countermeasure. Integrity breaches involve the corruption of organizational or user data, extending beyond the immediate compromise network confidentiality. These breaches encompass alterations, additions, or deletions of information, posing a threat to both network and user data. Untrusted devices, such as PDAs, may be exploited to access and manipulate information, affecting files on the network and data on user devices [5, 6].

The alteration or deletion of information without user acknowledgment can erode confidence in data and system integrity if undetected [1, 7]. Loss of network availability, often induced by Denial of Service (DoS) attacks, poses a significant threat to authorized users and devices. DoS attacks block user access to system resources and network applications, disrupting the normal flow communication [3].

In the context of wireless networks, signal jamming is a specific form DoS attack where a malicious user deliberately overwhelms legitimate wireless signals. Additionally, unintentional network congestion caused by users downloading large files can inadvertently deny access to other users, impacting network availability [1]. The importance of wireless security extends beyond the organization's premises as users increasingly connect remotely to their networks, often through untrusted, third-party networks. These risks include accessibility to malicious users, acting as a bridge to a user's own network, and increased eavesdropping due to the use of high-gain antennas [3, 6].

Ensuring the confidentiality, integrity, and availability of information on handheld devices is paramount. Information stored on these devices and mirrored on PCs must remain confidential and protected from unauthorized disclosure. The integrity information on handheld devices, including hardware, applications, and the underlying operating system, is also a significant security concern. Additionally, the

risk of DoS attacks on handheld devices may increase as "always-on" connectivity becomes more prevalent [1, 4].

The security RSA (Rivest-Shamir-Adleman) is based on the computational difficulty factoring large numbers into their prime factors. Breaking RSA encryption requires finding the prime factors of the modulus, which becomes exponentially difficult as the size modulus increases [2, 7]. RSA is widely used in various applications, including secure email communication, secure web browsing (HTTPS), digital signatures, and secure file transfer. It provides a secure method for exchanging encrypted messages over insecure channels without the need for a shared secret key. When implementing the AES and RSA algorithms in Java, cryptographic libraries such as the Java Cryptography Architecture and Java Cryptography Extension are used.These libraries offer classes and interfaces that handle cryptographic operations, including encryption and decryption.

The study resulted in an analysis of theoretical and practical models for assessing speech quality and mechanisms for ensuring the quality of speech information transmission in multiservice converged packet-switched networks.

References

1. Ibrahimov, B. G., & Alieva, A. A. (2019, August). An approach to analysis of useful quality service indicator and traffic service with fuzzy logic. In *International Conference on Theory and Application of Soft Computing, Computing with Words and Perceptions* (pp. 495-502). Cham: Springer International Publishing.

2. Ibrahimov, B. G., & Huseynov, F. I. (2020). Research and analysis mathematical model for evaluating noise immunity in telecommunication system. *Synchroinfo journal*, *6*(1), 2-6.

3. Valiyev V. M., Ibrahimov B. G., and Alieva A. A. (2020) About one resource control task and optimization throughput in multiservice telecommunication networks. *T-Comm*, 14(6), 48-52.

4. Ibrahimov, B. G., Humbatov, R. T., & Ibrahimov, R. F. (2018). Cryptographic methods and means protection transmitted information in telecommunication systems. *IFAC-PapersOnLine*, *51*(30), 821-824.

5. Ganimat I. B. Analysis and selection performance indicators multiservice communication networks based on the concept NGN and FN //Computer and information systems and technologies. – 2021.

6. Akhundov, R., & Ibrahimov, B. (2025, November). Ensuring Information Security within the Military Environmental Safety System. In *Modeling, Control and Information Technologies.* (No. 8, pp. 178-183).

7. Piriyev H.K. et al. Modelling of the battle operations //Monografiya, Herbi Nashriat", Baku. – 2017.

8. Ibrahimov, B., & Varlamov, O. (2024). Efficiency analysis of switching converter-modulator. *Synchroinfo Journal*, *10*(2), 12-20.

9. İbrahimov, B.G. Research and analysis of fiber-optic communication lines based on wave multiplexing technology. *İn* Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. -2023, Том 2: - pp.4-5.

10. Muradov, S.A. Development prospects of beacon systems // Problems of informatization. Proceedings of 11-th International Scientific and Technical Conference. Vol. 1. - Baku – Kharkiv – Bielsko-Biala: november 16 – 17**,** 2023, p.31.

RESEARCH OF MULTI-SERVICE COMMUNICATION NETWORKS TAKING INTO ACCOUNT DYNAMICALLY EMERGING SECURITY THREATS

Ibrahimov B.G., Hashimov E.G.
Azerbaijan Technical University, Baku, Azerbaijan
Akhundov R.G.
National Defense University, Baku, Azerbaijan

It should be noted that multiservice telecommunications networks belong to the class large communication systems, the design, implementation, operation, and evolution of which are currently impossible without the use of various types of business process modeling [1].

Currently, a number of methods and devices are known for studying and modeling multiservice communication networks [1, 2].

Their main drawbacks are the lack of the ability to quickly adjust the communication network being studied relative to the one actually operating in real time, taking into account the interdependence of the elements of the multiservice network when implementing security threats, which reduces the adequacy modeling and the reliability of telecommunications processes [2, 3].

This article discusses the tasks and research method that take into account the interdependence elements of a multiservice communication network during the spread security threat implementations, which increases the adequacy and reliability telecommunication processes when performing multimedia services [4].

This article proposes a method to address the aforementioned drawback. To solve the problem, we propose a method that can be implemented as follows [1, 2, 3-8]:

1.In the first stage, a graph of the modeled and studied network $Q = E[N, M]$ is formed with a specified number N graph vertices and M of branches connecting them.

2.Here, the graph vertices correspond to nodes of the multiservice network, such as routers, servers, switches, and multiplexers.

3.The graph branches correspond to communication lines connecting the network nodes.

Based on undirected graphs, it is possible to describe structural models of telecommunication processes taking into account dynamically emerging security threats using the following functional dependency:

$$Q_{MN} = W\,[E,T,P_{ub}\,\Delta t, I_{sr}, R, t_p, \dot{I}_{st}, t_b]\,, \qquad (1)$$

where E – number of statistical experiments; T – simulation time ; Δt – model time step duration; I_{sr} -security risk; R – Information flows between graph nodes; t_p –

propagation time of security threat realizations; t_b -network element recovery time; $\dot{I}_{st}$ – security threat entry point; P_{ub} – probability of occurrence of a security threat at the entry point.

The shortest routes are constructed along given information directions. The criterion for selecting the shortest route is the smallest number of transit elements, as, for example, in the OSPF protocol [1, 4]. They memorize the constructed routes along given information directions in communication networks. For each of the R information directions, they memorize a set G={g_1, g_2, …g_n}, consisting F sequentially connected network nodes along the given information direction.

In this case, the system models the process of security threat occurrence at the entry point. The entry point for a security threat is defined as a border element of a multiservice network connected to an element or elements of another network. It is assumed that after a security threat is realized against a multiservice network element, the threat realizations propagate to all directly connected elements. The propagation time security threat realizations t_p must be a multiple of the duration model time step [2].

Here, the duration of the model time step Δt is selected based on the minimum time the multiservice network remains in an unchanged state.

As a result of the actions described, the probability of a working state and the average time of a working state of an information direction can be calculated.

References

1.Valiyev, V. M., Ibrahimov, B. G., & Alieva, A. A. (2020). About one resource control task and optimization throughput in multiservice telecommunication networks. *T-Comm-Телекоммуникации и Транспорт*, *14*(6), 48-52.

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.

3. Hasanov, A.H. et al. Comparative analysis of the efficiency of various energy storages. Kharkov: Advanced Information Systems, -2023. Vol. 7, №. 3, -p.74-80.

4. Ibrahimov B. G., Mamedov I. A., Sadigov U. K. (2025). Research of the Quality of Functioning Critical Infor-mation Infrastructures in the Telecommunication System. Bulletin of computer and information technologies, *Vol. 22* (2), pp. 55 – 62.

5. Hashimov E.G., Khaligov G. The issue of training of the neural network for drone detection .Kharkov: Advanced İnformation Systems.2024, vol.8, N3. pp.53-58.

6. Ganimat I. B., Qiyas H. E. Analysis and selection performance indicators multiservice communication networks based on the concept NGN and FN //Computer and information systems and technologies. – 2021.

7. Zulfugarov B. et al.Comparative analysis of the efficiency of various energy storages //Modeling, Control and Information Technologies: Proceedings of International scientific and practical conference. – 2023. – №. 6. – С. 42-45.

8. İbrahimov, B.G. Research and analysis of fiber-optic communication lines based on wave multiplexing technology. *İn* Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. -2023, Том 2: - pp.4-5.

CYBERSECURİTY AND THE PROTECTİON OF INFORMATİON INFRASTRUCTURES WİTHİN THE FRAMEWORK OF AZERBAİJAN–TURKEY DEFENSE COOPERATİON

İsmayilov V.M.
State Border Service Academy, Baku, Azerbaijan

In the information technology–driven environment of the 21st century, issues of cybersecurity have become an integral component of national security systems. In this context, the strategic partnership between Azerbaijan and Turkey requires not only the strengthening of classical military cooperation but also the development of joint activities in the fields of information and cyber defense. Since the late 1990s, bilateral agreements such as the Agreement on Cooperation in the Field of Defense Industry (2007) and the Treaty on Strategic Partnership and Mutual Assistance (2010) have created a legal framework for cybersecurity and information exchange between the two brotherly states [1, p. 45].

At present, the extensive application of information and communication technologies (ICT) in military command, intelligence, communications, and logistics systems increases the risk of cyber threats.

The cyberattacks observed during the 2020 Patriotic War clearly demonstrated the priority of this field in national security systems. Joint military and technological cooperation with Turkey has strategic significance in countering such challenges.

Cooperation between Azerbaijan and Turkey in the field of cybersecurity is carried out through various mechanisms at both the governmental and military levels.

The exchange of information and joint training programs between the Ministry of Defense of Azerbaijan, the State Service of Special Communication and Information Security (XRİTDX), the Azerbaijan Cyber Security Center (AKTM), and Turkey's Ministry of National Defense, Cyber Command Group, HAVELSAN, and ASELSAN plays an important role in this regard [3, p. 112].

During the "ADEX 2021 – Azerbaijan International Defense Exhibition" held in Baku, memorandums of understanding were signed between the two countries to promote joint development of cyber defense technologies and the harmonization of critical infrastructure protection systems. These agreements align with NATO's Defence Education Enhancement Programme (DEEP) initiatives, as both nations emphasize the integration of digital components into cybersecurity education and military training [4].

The strategic sectors of Azerbaijan's economy-energy, transport, and communications infrastructure - are the main pillars of regional stability and national security. Joint Azerbaijani–Turkish projects such as the BTC oil pipeline, the TANAP gas pipeline, and the Zangezur Corridor are of significant economic and security importance. Ensuring the protection of these infrastructures against cyberattacks is considered one of the primary priorities within the Azerbaijan–Turkey security dialogue [5-7].

Discussions have been held to align Turkey's National Cyber Security Strategy 2020–2023 with Azerbaijan's National Cyber Security Concept. In 2022, during a joint working group meeting between the defense ministries of both countries, agreements were reached on cyber operational readiness, information exchange protocols, and joint simulation exercises [4].

In the contemporary system of international relations, the concepts of information warfare and digital diplomacy have become essential components of state security policies. For Azerbaijan and Turkey, this is particularly relevant in the context of combating disinformation and cyberattack campaigns orchestrated by Armenia. In the light of the geopolitical realities of the 21st century, Azerbaijan–Turkey relations have entered a new strategic phase. One of the most crucial directions of this partnership is the deepening of cooperation in cybersecurity and the protection of information infrastructure.

Research indicates that cooperation between the two countries in the field of cyber defense is developing in three main directions:

- normative–legal framework – preparation of joint protocols and training documents in the field of cybersecurity;
- technological synchronization – development of joint innovative defense systems and simulation programs;
- education and training – strengthening individual cyber readiness and enhancing digital literacy in military educational institutions.

Thus, the strategic partnership between Azerbaijan and Turkey is aimed at building a joint security architecture in cyberspace, protecting information sovereignty, and ensuring the resilience of critical infrastructures. The primary future task of this cooperation lies in deepening digital integration within the defense industry and coordinating national security systems based on a unified cyber defense doctrine.

References

1. Aliyev, R. H. Theoretical Foundations and Management Mechanisms of the National Security System. – Baku: Elm və Təhsil, 2024. – 248 p.
2. Gasimov, M. Problems of Defense Industry and Military-Technological Cooperation in the Modern Era. // National Defense Journal, No. 2, 2022, pp. 110–118.
3. NATO DEEP. Digital Transformation in Military Education. – NATO, 2022. 56 p.
4. Republic of Turkey Ministry of National Defense. National Cyber Security Strategy 2020–2023. – Ankara, 2020. – 52 p.
5. Suleymanov, J.F. et al. (2025). Modern approaches to technical safety in oil and gas pipelines. *İn* Current directions of development of infor. and communication technologies and control tools. - 2025. Volume 4: sections 6. -pp.40
6. İsmayil, İsmayil, & Hashimov, E. (2025). Security and protection of Azerbaijan's oil and gas pipelines: cybersecurity and risk management approaches. *Матеріали конференцій МЦНД*. p.136–144. https://doi.org/10.62731/mcnd-11.07.2025.004
7. Ismayilov N.E. et al..Ensuring the integrity and safety of pipeline infrastructure. *İn* Current directions of development of information and communication technologies and control tools. - 2025. Volume 4: sections 6. -pp.41

ANALYSIS OF METHODS ENSURING INFORMATION SECURITY COMMUNICATION SYSTEMS IN CRITICAL INFORMATION INFRASTRUCTURES

Mammadov I.A., Sadıgov U.K.
Azerbaijan Technical University; Baku, Azerbaijan

The relevance of the task of ensuring the effectiveness of communication systems in critical information infrastructures is determined by the aggravation of information security problems even in the context of intensive improvement of information technologies and tools for protecting data transmission systems [1].

This is evidenced by the unprecedented growth of information security breaches in telecommunications networks and the increasing severity of their consequences. The total number of breaches worldwide is increasing by more than 100% annually [1, 2].

In the Republic of Azerbaijan, according to law enforcement statistics, the number of crimes detected in the field of computer information and communications systems alone increases annually by an average of 3-4 times [1, 2, 3].

Taking into account the above, the list of threats to information security in communication systems, violations, and crimes is so extensive that it requires scientific systematization and special study and research in order to assess the risks associated with them and develop measures to prevent them.

Therefore, research indicates that the primary cause of information security problems in communications systems in critical information infrastructures and in the field of information protection is the lack of a well-thought-out and approved information security policy based on organizational, technical, and economic solutions, followed by monitoring of their implementation and assessing their effectiveness [2, 3, 4].

Thus, all of this necessitates the development and analysis of scientifically sound methods for ensuring the information security communications systems, taking into account the positive practical experience of Azerbaijani, Russian, and foreign communications systems in this area.

It is worth noting that the issues information security communications systems in critical information infrastructures have been addressed in the works of many domestic and foreign researchers and specialists [3, 5-8].

The aim of this work is to analyze methods for ensuring information security of nodes and hardware-software complexes communication systems in critical information infrastructures, allowing to reduce its information and network risks [3].

The purpose this work is to analyze methods for ensuring information security of nodes and hardware-software complexes of communication systems in critical information infrastructures, which can improve the efficiency of information security systems and reduce information and network risks [2, 3].

The stated goal determined the following tasks: To analyze methods of ensuring information security communication systems in critical information infrastructures [1, 2, 3]:

- analyze the features of the concept of information security in communication systems;
- identify a list of information resources whose integrity or confidentiality breach would cause the greatest damage to telecommunications networks;
- identify the most significant patterns of intruders and threats to information resources of hardware and software systems in communications systems;
- systematize information risks, develop methods for assessing information security indicators of communication systems in critical information infrastructures, and approaches to managing them;
- develop an algorithm for assessing residual information risks in communication systems using modern technologies.

Thus, as a result of the study, important methods for ensuring information security communication systems in critical information infrastructures were analyzed.

References

1. Ibrahimov B.G., Mammadov T.H. (2024). Research methods for increasing the security of communication systems important objects of critical information infrastructure. *T-Comm*, vol. 18, no.6, pp. 61-66.

2. 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.

3. Ganimat I. B., Qiyas H. E. Analysis and selection performance indicators multiservice communication networks based on the concept NGN and FN //Computer and information systems and technologies. – 2021.

4. Dergachov, K. et al. Adaptive algorithm for visual positioning of UAVs in the local environment. / CEUR Workshop Proceedings. 2025. Vol.3981. P.103-114

5. Ibrahimov, B. G. et al. (2020). Analysis performance indicators network multiservice infrastructure using innovative technologies. In *Proc. of the 7-th International Conference on Control and Optimization with Industrial Applications* (Vol. 2, pp. 176-178).

6. Ibrahimov B.G. et al. Research and analysis mathematical model of the demodulator for assessing the indicators noise immunity telecommunication systems //Advanced Information Systems. – 2024. – T. 8. – №. 4. – C. 20-25.

7. Bayramov A.A. The supervisory control systems deployment in mountainous terrain. *İn* VIII Int. Conf.“Modern development trends of ICT and control methods. –2018. C. 3-4.

8. Hashimov E. G. Taking Control of Dead Zone of Radiolocation Station by the Automatic Acting Electro-Optic System //Defence Science Journal. – 2025. – T. 75. – №. 1.

9. Ibrahimov B. G. Research and analysis of fiber-optic communication lines based on wave multiplexing technology. *İn* Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. 2023. Т.2: секція 2 . – С. 4-5.

RESEARCH OF THE STEGANOGRAPHIC INFORMATION PROTECTION SYSTEM

Tahirova K.
National Defense University; Baku, Azerbaijan

The global informatization society and intensive information exchange require the development of tele communication systems, wired and wireless data transmission systems for special purposes [1, 2].

Special-purpose telecommunications systems, in accordance with the ITU-T and ITU-D standard, must ensure information security requirements, including the confidentiality, integrity, and availability information transmitted over communication channels [3, 4].

To protect information from being read by an intruder, cryptographic encryption, which is highly resistant to cryptanalysis, is used. However, when using open channels, an intruder can destroy encrypted messages or the communication channel [5, 6].

In this case, information protection can be ensured by steganographic methods in the communication system, allowing for the covert transmission of important information over an open communication channel without an attacker detecting the transmission or destroying the message [2, 7].

Steganography is also necessary when the use of cryptographic methods is prohibited (at the government or corporate level) or is ineffective [1, 6].

Thus, steganography is an effective means of protecting information transmission over real-time communication channels. Therefore, the task of researching a steganographic information security system is relevant.

The development of digital steganography requires the development of a theoretical framework and robust methods for embedding hidden information into the cover signal in a communication system. This, in the long run, will lead to the standardization of steganographic methods for special-purpose communication systems [3, 5].

In this case, an analysis of existing steganographic algorithms was carried out, the stability indicators of steganographic algorithms were determined, and their classification was carried out in a special-purpose communication system for files of various formats - text, audio, video, images [2, 7].

An analysis steganographic algorithms revealed that known steganographic containers are single-component and are described by the following expression:

$$Y_i = F\,[U_i, \beta_i]\ ,$$

where Y_i - full container signal count; U_i – hidden message; β_i - empty container signal count.

The process of message extraction boils down to solving an equation with two unknowns. To solve this problem, one of two approaches to message embedding in telecommunications systems is used [1].

In this case, the first approach involves zeroing out certain elements of the container and replacing them with the hidden information. For example, the least significant bit method and its many variations embed information into specific bits of the container.

Assuming that the message signal can be easily detected by an attacker with knowledge of the hiding algorithm used (due to the invariance property), key coefficients provide additional protection.

These are coefficients whose minimal error results in maximum suppression of the hidden message [1, 2, 5].

To this end, for each of the resulting mathematical models, a condition for maximum sensitivity to coefficient variation is determined.

References

1. Ibrahimov, B.G. et al. (2021). Research and analysis efficiency fiber optical communication lines using quantum technology. *T-Comm-Телекоммуникации и Транспорт*, *15*(10), 50-54.

2. Hasanov M. H. et al. Research and analysis performance indicators NGN/IMS networks in the transmission multimedia traffic. *In* 2019 Wave Electronics and its Application in Information and Telecommunication Systems, 2019. – С. 1-4.

3. Ibrahimov B. G., Huseynov F. I. Research and analysis mathematical model for evaluating noise immunity in telecommunication system //Synchroinfo journal. – 2020. – Т. 6. – №. 1. – С. 2-6.

4. Rustamov, A.R. et al. (2025). System technical solution of electromagnetic adaptation. *Advanced Information Systems*, *9*(1), 86–90.

5. Mammadov H.A, Ibrahimov B.G. Efficiency of methods forecasting of the office traffic signaling systems with use technologies of neural networks. The 4-rd World Conference on Soft Computing (WConSC-14). Berkeley, California, USA . 2014. pp.141–145.

6. Ibrahimov, B. et al. (2025). Research spectral efficiency of new modulation formats in fiber-optic networks. *Reliability: Theory & Applications*, *20* (SI 7 (83)), 81-89.

7. Ibrahimov, B., Nabieva, A., & Hamidova, A. (2024). Research Efficiency Functioning Wireless Cellular Networks Taking into Account Modern Energy Saving Technologies. *Engineering Headway*, *7*, 149-155.

8. Ganimat I. B., Qiyas H. E. Analysis and selection performance indicators multiservice communication networks based on the concept NGN and FN //Computer and information systems and technologies. – 2021.

9. Zulfugarov B. et al.Comparative analysis of the efficiency of various energy storages //Modeling, Control and Information Technologies: Proceedings of International scientific and practical conference. – 2023. – №. 6. – С. 42-45.

10. İbrahimov, B.G., Hashimov, E.G. Research and analysis of fiber-optic communication lines based on wave multiplexing technology. *İn* Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. -2023, Том 2: - pp.4-5.

11. Hasanov, A.H. et al. Comparative analysis of the efficiency of various energy storages. Kharkov: Advanced Information Systems, -2023. Vol. 7, №. 3, -p.74-80.

EXPERIMENTAL STUDY OF THE RESISTANCE OF TELEMETRY AND COMMUNICATION SYSTEMS OF UNMANNED AERİAL VEHİCLES IN RADIO ELECTRONIC WARFARE ENVIRONMENT IN LABORATORY AND FIELD CONDITIONS

Rustamov A.R., Gasanov A.G.
National Defense University, Baku, Azerbaijan
Azizullayev M.G.
National Aerospace Agency, Baku, Azerbaijan
Hasanli R.A.
Sumqait State University, Sumqait, Azerbaijan

Focuses on the reliability of unmanned aerial vehicles telemetry communication systems in radio electronic warfare conditions.

The evaluation of the performance of the 2.4 GHz frequency band and the distance of 15 meters were investigated in laboratory and experimental tests for data transfer of 1 GB and 10 GB. The signal-to-noise ratio (SNR), effective SNR, received signal strength indicator (RSSI), path loss (Path Loss) and bit error rate (BER) were compared.

The results show that although communication parameters deteriorated significantly in radio electronic warfare conditions, communication continuity was ensured thanks to the adaptive frequency hopping (AFH) mechanism and real-time spectrum monitoring[1-3].

Although communication performance deteriorated in the electronic warfare environment, the continuity of communication was maintained thanks to real-time spectrum tracking and adaptive frequency avoidance mechanisms.

Under normal conditions, transmission stability was high, with a result of approximately 0.9 minutes for 1 gigabyte and approximately 9 minutes for 10 gigabytes[4-16].

In electronic warfare conditions, the signal-to-noise ratio decreased from approximately 25 decibels to 18 decibels, the effective signal-to-noise ratio decreased from 22 decibels to 15 decibels, and the received signal strength decreased from approximately −44/−45 decibel - milliwatts to −58/−60 decibel-milliwatts. attenuated, path loss increased from 38-40 decibels to 46–48 decibels, and bit error rate increased from $1.2\text{-}2.1\times10^{-5}$ to $3.5\text{–}5.0\times10^{-5}$. However, 1 gigabit about 1.3 minutes per byte, 10 gigabytes

The transmission was completed in about 13 minutes per byte.

The adaptive mechanism marked the channel as "interfering" as soon as the signal quality dropped below the threshold and switched to a "cleaner" frequency within about 150-300 milliseconds, ensuring continuity of the connection[7, 8].

References

1. Gasanov, A.G. (2025). Problems of optimal planning of air defense means against low-altitude air targets, Збірник наукових праць з матеріалами IX Міжнародної Наукової конференції, pp. 409-418.

2. Rustamov A.R., Gasanov A.G., Azizullayev, M.G. (2024). Effective application of telemetry systems of unmanned aerial vehicles. Modern directions development information and communication technology and means management Thesis reports fourteenth international scientific and technical Conference April 25-26, Volume 2: sections 3, 4, 5, 6, pp. 66-70.

3. Rustamov, A.R., Gasanov, A.G., Azizullayev, M.G. (2024). The role of navigational and hydrographical support in ensuring security of the Caspian Sea. 2nd International Conference on Logistics, Transport and Distribution in the Caspian Region, May 15-17, Baku, Azerbaijan.

4. Rustamov, A.R., Gasanov, A.G., Azizullayev, M.G. (2024). Analysis of modules and systems used in effective control of UAVs in radio electronic combat environment. Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. Тези доповідей чотирнадцятої міжнародної науково-технічної конференції 25 - 26 квітня, pp. 47-48, doi: https://doi.org/10.32620/ICT.24.t1

5. Gasanov, A.G., Karimov, Y. Sh. (2024). Methodology for effective planning of means of destruction located in the cover and in the stern for various types of targets. Voenen Zhurnal, Publishing House Rakovski National Defence College Sofia, Bulgaria, Vol. 131, No. 2, pp. 207-213.

6. Gasanov, A.G., Karimov, Y. Sh. (2023). Optimal management of the application of a group of unmanned aerial vehicles (UAVs) of the same type to different targets. The Journal of Defense Resources Management (JoDRM), vol 14, Issue 2 (27), pp. 125-130.

7. Piriyev G. K. et al. Modelling of the battle operations //Monografiya, Herbi Nashriat", Baku. – 2017.

8. Hasanov A. H. 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.

9. Hashimov E.G. et al. Mathematical modeling of military systems. Textbook. -Baku: Military publishing house, -2018. -266 p.

10. Alieva, R. A., Pashaev, F. G., Gasanov, A. G., & Mahmudov, K. T. (2009). Quantum-chemical calculations of the tautomeric forms of azo derivatives of acetylacetone and determination of the stability constants of their complexes with rare-earth metals. *Russian Journal of Coordination Chemistry*, *35*(4), 241-246.

11. Gadzhieva S. R. et al. Thermodynamic characteristics of metal complexation with 3-[4-iodophenylazo]-2, 4-pentanedione in an aqueous ethanol solution //Russian Journal of Inorganic Chemistry. – 2007. – T. 52. – №. 4. – C. 640-644.

12. Aliyev A. A. et al. Earthquake and activation of mud volcano (causal link and interaction) //Proc. Geol. Inst. – 2001. – T. 29. – C. 26-39.

13. Ahmadov A. I. et al. Calculation of the Energy of the Interelectron Interaction in Molecules in a Basis of Slater Functions //Russian Physics Journal. – 2019. – T. 61. – №. 10. – C. 1848-1854.

14. İbrahimov, B.G. et al. (2022). Research and analysis indicators fiber-optic communication lines using spectral technologies. *Advanced information systems*, *6*(1), 61-64.

15. Ibrahimov, B.G. et al. (2024). Research and analysis mathematical model of the demodulator for assessing the indicators noise immunity telecommunication systems. *Advanced Information Systems*, *8*(4), 20-25.

АЛГОРИТМ АВТОМАТИЧНОГО УПРАВЛІННЯ ЗАСОБАМИ МОНІТОРИНГУ КАНАЛІВ ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ

Баліцький Н.В.
Національна академія сухопутних військ ім. П. Сагайдачного, Львів, Україна
Чалапко В.В.
Національний технічний університет «ХПІ», Харків, Україна

Розвиток сучасних засобів захисту інформації базується на симетричних та несиметричних криптосистемах, водночас поява повномасштабного квантового комп'ютера може внести хаос в системи захисту та значно знизити рівень захищеності каналів передавання інформації [1]. Слід враховувати, що введення системи штучного інтелекту на першому етапі цільової (змішаної) атаки зможуть значно спростити та прискорити виявлення аномалій (відхилення від нормальної роботи) у роботі інфраструктури. Використання функції штучного інтелекту дозволяє забезпечити своєчасне проведення аналізу SIEM-систем та подібних систем виявлення та аналізу аномалій [2]. При цьому на будь-якому інформаційному каналі для захисту необхідно враховувати не тільки потоковий стан захисту, а також можливість своєчасного формування превентивних заходів щодо захисту інформації. При перевірці наявності каналів витоку інформації використовують спеціальні технічні засоби, спрямовані на перевірку певних ознак наявності витоку даних [3, 4]. У цьому використовується значний набір ознак, властиві кожному за технічного засобу моніторингу (методу перевірки). Тому актуальності набуває розгляд низки питань щодо проблеми розробки принципів побудови і алгоритмів моніторингу каналів щодо захисту інформації, здатних виявляти та вчасно закривати канали витоку інформації або попереджати вплив на них [1, 3].

Метою доповіді є розроблення алгоритму автоматичного управління засобами моніторингу каналів щодо захисту інформації.

У доповіді показано, що важливою тенденцією сучасності є створення нового покоління обчислювальних пристроїв автоматичного регулювання, в яких обчислювальний блок має вигляд однорідної, складеної з однакових елементів системи. За характером дії вони відрізняються один від одного лише впливом іншого рівня, тобто управляючого контуру, який регулює функціонування пристрою розрахунку погрібних параметрів. Передумовою створення таких управляючих систем автоматичного регулювання став розвиток мікроелектроніки. Обґрунтовано, що при розв'язанні такого роду задач в багатьох випадках доводиться обмежуватись використанням обчислювального пристрою для оцінювання стану системи і для визначення альтернативних варіантів впливу на систему, тобто участю обчислювального пристрою в ролі своєрідного порадника. Введення такої форми управління засобами моніторингу інформаційних каналів щодо захисту інформації означає великий крок вперед. Однак слід готувати наступний етап –

безпосереднє управління організацією комплексу з множини елементів, що здійснюється обчислювальним пристроєм.

Розроблено алгоритм автоматичного управління моніторингу інформаційних каналів щодо їх захисту. Особливістю запропонованого алгоритму є поміркований підхід до процесу управління, що дозволяє декомпозувати структуру алгоритму управління та ввести в розгляд проміжну стадію вивчення (моніторингу) – формулювання цілі управління. Формулюючи мету управління засобами моніторингу (своєчасне виявлення каналів витоку інформації) за допомогою алгоритму система переводить свої потреби на мову станів об'єкта захисту інформації. Це дозволяє системі управління засобами моніторингу передавати процедуру синтезу та реалізації управлінських рішень щодо виявлення каналів витоку інформації. На другій стадії визначається управлінське рішення, яке забезпечує досягнення цілі функціонування системи управління засобами моніторингу – закриття каналів витоку інформації. Запропоновано у роботу керуючого пристрою схеми автоматичного управління моніторингу інформаційних каналів ввести принципи кібернетики (математичні алгоритми процедури роботи штучного інтелекту). Це дозволяє навчати систему реагувати на нові загрози. Для розв'язання поставленої задачі використовується метод ітерації управляючих пристроїв. Зручність запропонованого алгоритму полягає в тому, що розв'язання задачі зводиться до розв'язання двох одно точкових крайових задач. Це дозволяє зменшити чутливість розв'язування задачі оптимізації до неідеальностей обчислювального процесу. Однією з основних труднощів розв'язання задачі є вибір вагових коефіцієнтів при визначенні варіації управляючого впливу. При моделюванні значення вагових коефіцієнтів розраховується за аналітичними співвідношеннями для коефіцієнтів інформаційної та внутрішньої доступності безпровідного каналу радіозв'язку.

Список літератури

1. Herasymov S., Yevseiev S., Milevskyi S. and ets. Development of a method for automatic control of monitoring means for information protection objects. *Eastern-European Journal of Enterprise Technologies*. 2024. № 6(9) (132). P. 25-38. DOI: https://doi.org/10.15587/1729-4061.2024.319058.

2. Shmatko O., Herasymov S., Milevskyi S. and ets. Development of a method for assessing the efficiency of technical systems' computer dynamic simulators. *Eastern-European Journal of Enterprise Technologies*. 2025. № 2(9) (134). P. 50-61. DOI: https://doi.org/10.15587/1729-4061.2025.327558.

3. . Kushnerov O., Murr P., Herasymov S. and ets. Application of Neural Networks for Network Traffic Monitoring and Analysis. *2024 8th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*. Ankara, Turkiye, 2024. P. 1-8. DOI: https://doi.org/10.1109/ISMSIT63511.2024.10757251.

4. Herasimov S., Roshchupkin E. Control of the serviceability of the radio electronic equipment of the communication system. *Міжнародна науково-практична конференція «Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку»*. Х.: НАНГУ. 2023. С. 39-40.

ПРОПОЗИЦІЇ ЩОДО УДОСКОНАЛЕННЯ ТЕХНІЧНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ ПЕРЕДАВАННІ ДАНИХ

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

На сьогодні широко застосовуються інформаційні канали при передаванні даних між різними користувачами, у тому числі й між користувачами критичної сфери [1]. Технічні засоби передавання даних повинні забезпечувати цілісність і конфіденційність інформації, мати систему заходів і процедур, що захищають дані від несанкціонованого доступу, пошкодження або знищення [2, 3]. При цьому безпровідні інформаційні канали (переважно радіотехнічні) мають високий ризик щодо несанкціонованого доступу до інформації як з метою викрадання даних, так і з метою їх підмінювання (порушення цілісності). Це потребує розв'язання задачі удосконалення технічних засобів передавання даних для забезпечення захисту інформації.

Метою доповіді є обґрунтування пропозицій щодо удосконалення технічних засобів захисту інформації при передаванні даних.

У доповіді показано один із варіантів удосконалення технічних засобів для захисту інформації є обґрунтування методів синтезу сигналів складної форми – сигналів для передавання даних інформаційними каналами із застосуванням методів, які забезпечують потрібний рівень завадозахищеності. Запропоновано використання амплітудно-імпульсно-модульованих сигналів з подальшою їх вузькосмуговою фільтрацією для виділення огинальної та несучої. Показано, що вимогам щодо завадозахищеності задовольняє метод формування амплітудно-модульованих сигналів на основі модуляції часових параметрів прямокутними імпульсами. Наведено результати дослідження закону модуляції часових параметрів прямокутних імпульсів для формування амплітудно-модульованих сигналів складної форми.

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., Чернявський О. Ю. Моделювання траєкторій руху безпілотного летального апарату при дистанційному зондуванні землі. Мат. XIII Міжн. НПК. Чернігів: НУ «Чернігівська політехніка», 2023. Т. 2. С. 129-130. (https://conference-chernihiv-polytechnik.com/wp-content/uploads/2023/06/Tezy-2023-Part-2.pdf).

3. Герасимов С. В., Марущенко В. В., Чернявський О. Ю. Моделювання роботи навігаційної системи для автономного руху безпілотного летального апарату. *Мат. XVI міжн. НПК "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.

МОДЕЛЮВАННЯ ВПЛИВУ ЗАГРОЗ НА ТЕЛЕКОМУНІКАЦІЙНІ МЕРЕЖІ

Федорович О.Є., Смідович Л.С., Рибка А.В.
Національний аерокосмічний університет
«Харківський авіаційний університет», Харків, Україна

У сучасному стані, а якому знаходиться країна, розподілені телекомунікаційні мережи (РТМ), є основним джерелом та комунікаційним засобом зв'язку між органами управління та складними об'єктами та системами (об'єкти інфраструктури, транспорт, військові об'єкти, тощо) [1, 2]. Вплив атакуючих місій противника спрямований на вузли та магістралі РТМ щодо їх пошкодження та порушення передачі даних і управління. Тому, актуальна тема запропонованої доповіді, в якій представлені результати дослідження впливу загроз на РТМ.

Метою доповіді є розробка комплексу математичних моделей та прикладної інформаційної технології щодо планування превентивних заходів для підвищення стійкості РТМ.

В доповіді наводяться результати досліджень:

- проаналізовані існуючі підходи до аналізу зовнішнього середовища, особливо для сучасного стану країни, з агресивними факторами впливу на роботу РТМ;
- розроблено моделі для виділення критичних об'єктів інфраструктури РТМ, які необхідно захистити;
- створена оптимізаційна модель для пошуку раціонального варіанту проведення превентивних заходів, в умовах обмежених можливостей;
- розроблена агентна імітаційна модель для аналізу впливу агресивних дій та плануванню превентивних заходів.

Після проведеного аналізу факторів впливу на функціонування РТМ, виявлені фактори, які пов'язані з атакуючими діями противника. Вони впливають на критичні вузли РТМ, передачу даних, спотворенню інформації, з використанням кібератак, покривленню програмного коду.

Проведено пошук та обґрунтування критичних об'єктів РТМ, але обмежені можливості призводять до необхідності виділення підмножин критичних об'єктів. Це було проведено, за рахунок формування всіх можливих підмножин критичних об'єктів, та вибору з них раціонального. Була створена оптимізаційна модель для формування превентивних заходів щодо захисту РТМ, з використанням як пасивних так і активних методів захисту. Використано показники часу, витрат та ризиків виконання проєкту захисних дій. Було проведена локальна оптимізація окремих показників. З-за суперечливості показників проведена багатокритеріальна оптимізація. В якості обмежень, використані допустимі значення показників часу, витрат та ризиків. Розроблена імітаційна модель для дослідження, у часі, впливу загроз агресивних факторів на функціонування РТМ. Розроблена агентна модель для імітаційного моделювання логістичних дій щодо планування превентивних

заходів захисту РТМ, з урахуванням значень основних показників. До пасивних методів захисту відносяться:

- створення захисних конструкцій для основних критичних об'єктів РТМ;
- створення укрить для забезпечення захисту від дронів та ракет, які можуть масово атакувати критичні об'єкти;
- створення кіберзахисту від кібератак противника, шляхом введення секретних кодів та інших сервісів захисту.

До активних методів відносяться: використання засобів ППО, РЕБ, дронів-перехоплювачів, які забезпечують захист локальної території, в якій знаходяться окремі критичні об'єкти РТМ.

Використані математичні методи та моделі:

- системний аналіз щодо формування послідовності логістичних превентивних дій для захисту РТМ від впливу агресивних факторів зовнішнього середовища;
- оптимізаційна модель, з використанням цілочисельного (булевого) програмування та лексикографічне впорядковування варіантів, для вибору раціонального варіанту множини критичних об'єктів, для проведення дій по їх захисту;
- багатокритеріальна оптимізація для пошуку компромісу серед суперечливих показників часу, вартості та ризиків проєкту проведення превентивних захисних дій;
- імітаційне моделювання для оцінки впливу агресивних факторів на пошкодження РТМ;
- агентна модель планування послідовності логістичних дій для формування проєкту щодо захисту критичних об'єктів РТМ від атак противника.

Висновок. Запропонований підхід дозволяє проаналізувати загрози від атакуючих дій противника на функціонування РТМ, виявити критичні об'єкти інфраструктури РТМ, щодо їх захисту, провести оптимізацію основних показників проєкту (час, витрати, ризики), в умовах обмеженості ресурсів щодо виконання проєкту, промоделювати логістичні дії для планування захисту РТМ.

Список літератури

1. Models and information technology of aging management of man-made systems in the conditions of modern risks / Oleg Fedorovich, Liudmyla Lutai, Oleg Uruskiy, Sergii Gubka, Yuliia Leshchenko // Радіоелектронні і комп'ютерні системи. – 2024. – № 3. – С. 175-189. DOI: 10.32620/reks.2024.3.12.

2. . Modeling of logistics of war reserve stockpiling for successful combat operations / O. Fedorovich, M. Lukhanin, O. Prokhorov, Yu. Pronchakov, O. Leshchenko, V. Fedorovich / Radioelectronic and Computer Systems, 2023, no. 1(105), P. 183-196. DOI: 10.32620/reks.2023.1.15.

МЕТОДИ ВИЯВЛЕННЯ КІБЕРАТАК У ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ ЗА ДОПОМОГОЮ МАШИННОГО НАВЧАННЯ ПІД ЧАС ВОЄННОГО СТАНУ В УКРАЇНІ

Ні Я.С., Ні О.В., Шостак М.В., Шостак В.В.
Харківський національний університет радіоелектроніки, Харків, Україна

З початком повномасштабної війни проти України кіберпростір став одним із ключових напрямів інформаційного протистояння. Телефонні та інтернет-мережі відіграють критичну роль у забезпеченні зв'язку державних органів, сил оборони, екстрених служб, медичних установ, фінансових систем та цивільного населення. Зі збільшенням кількості кібератак на українську критичну інфраструктуру та телекомунікаційні оператори виникла потреба у застосуванні передових технологій для швидкого та ефективного виявлення загроз.

Машинне навчання (ML) виявилося одним із найбільш ефективних інструментів у протидії кібератакам.

Алгоритми ML дозволяють системам виявляти аномалії у мережевому трафіку, аналізувати великі обсяги даних у реальному часі та прогнозувати потенційні загрози на основі історичних моделей.

Головна перевага ML полягає в його здатності самонавчатися та вдосконалювати власні алгоритми без потреби постійного втручання людини. Це особливо актуально під час воєнного стану, коли оператори мереж і кіберслужби обмежені у ресурсах і часі на ручний аналіз подій.

Ключовими типами загроз є такі:

– DDoS-атаки,
– фішинг,
– шпигунське ПЗ,
– несанкціонований доступ до мереж,
– спроби перехоплення даних.

Сучасні методи ML дозволяють розпізнавати навіть складні і приховані атаки, які не завжди видно при використанні класичних систем IDS/IPS. Активне застосування алгоритмів класифікації, кластеризації та нейронних мереж (CNN, RNN, LSTM) забезпечує високий рівень точності виявлення аномалій у динамічних умовах, коли топологія мереж постійно змінюється через руйнування інфраструктури або перевантаження каналів зв'язку.

У межах українських телекомунікаційних мереж активно застосовуються моделі на основі Random Forest, Gradient Boosting та ансамблеві підходи, що дозволяють аналізувати десятки параметрів трафіку і виявляти складні закономірності.

Глибокі нейронні мережі ефективні при аналізі часових послідовностей і виявленні повільних або прихованих атак, що розгортаються поступово.

Важливо відзначити, що застосування ML для кіберзахисту передбачає комплексний підхід, який включає збір даних, їх підготовку, навчання моделей, оцінку точності та інтеграцію з системами реагування на інциденти.

Особливу актуальність має формування національних дата-сетів, що відображають специфіку українського кіберпростору, типові патерни трафіку та особливості атак.

Це дозволяє підвищити точність моделей і знизити ймовірність помилкових спрацьовувань.

В умовах воєнного стану критично важливим є забезпечення стійкості та автономності систем моніторингу, здатності функціонувати навіть при частковому руйнуванні мережевої інфраструктури або відсутності стабільного енергопостачання.

Інтеграція систем машинного навчання з SIEM та IDS/IPS дозволяє не лише виявляти кібератаки, а й автоматично локалізувати джерела загроз, блокувати шкідливий трафік і оптимізувати маршрутизацію даних у реальному часі.

Застосування AI у поєднанні з аналітикою великих даних дозволяє прогнозувати масштабні атаки, реагувати на DDoS і фішингові кампанії та підтримувати критичні сервіси без перебоїв.

Метою доповіді є дослідження методів виявлення кібератак у телекомунікаційних мережах України за допомогою машинного навчання, оцінка ефективності інтелектуальних систем у кризових умовах та визначення напрямів розвитку адаптивних методів кіберзахисту.

У доповіді детально розглянуто сучасні алгоритми ML, їхню інтеграцію з українськими телекомунікаційними системами, специфіку роботи в умовах воєнного стану, наведено практичні приклади успішного впровадження та запропоновано рекомендації щодо подальшого розвитку інтелектуальних систем захисту критичної інфраструктури.

Список літератури

1. Гончарук М.С., Демченко В.П. Інтелектуальні методи виявлення аномалій у телекомунікаційних мережах. – Львів: Телекомунікації та безпека, 2023. – 184 с. DOI: 10.34725/mlsecukraine.2023.004

2. Alzubi J.A., et al. Machine learning-based intrusion detection systems for IoT networks: A comprehensive review. Computers & Security. – 2023. – 127. – 103139. DOI: 10.1016/j.cose.2023.103139

3. Кравченко О.М. Використання машинного навчання у системах виявлення кібератак в Україні. – Інформаційна безпека, 2022. – №2. – С. 35–42. DOI: 10.37017/cyberdef.2022.012

4. Rathore S., Park J.H. Deep learning-based real-time detection of DDoS attacks in SDN environments. Journal of Network and Computer Applications. – 2023. – 215. – 103623. DOI: 10.1016/j.jnca.2023.103623

5. Міністерство цифрової трансформації України. Національна стратегія кібербезпеки на період воєнного стану. – Київ, 2024. DOI: 10.37017/mintsyfra.2024.015

КРИПТОГРАФІЧНИЙ ЗАХИСТ ДАНИХ В IoT-ПРИСТРОЯХ: ВИКЛИКИ ТА РІШЕННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ

Мороз А.В.
Харківський національний університет радіоелектроніки, Харків, Україна
Манжула Є.А., Сітнікова С.І.
Харківський національний університет імені В.Н. Каразіна, Харків, Україна

Швидкий розвиток Інтернету речей (IoT) супроводжується масовим впровадженням розумних пристроїв у побутові, промислові та транспортні системи. Пристрої IoT збирають, передають і обробляють величезні обсяги даних, що включають персональну інформацію користувачів, промислові показники та керуючі сигнали. Це робить IoT-системи привабливою ціллю для кіберзлочинців і створює серйозні виклики у забезпеченні конфіденційності та цілісності даних. Забезпечення криптографічного захисту в таких умовах є одним із ключових напрямів безпеки IoT-пристроїв.

Однією з основних проблем є обмежені обчислювальні ресурси та енергоспоживання більшості IoT-пристроїв. Традиційні алгоритми шифрування та підписи даних, які використовуються у серверних системах та класичних комп'ютерах, часто є занадто ресурсомісткими для мікроконтролерів, сенсорів і малопотужних комунікаційних модулів. Тому розробка легковагових криптографічних протоколів, які забезпечують достатній рівень безпеки, залишається пріоритетним завданням для інженерів та дослідників у сфері IoT[1].

Сучасні підходи до захисту IoT-даних включають використання симетричного шифрування для оперативного оброблення інформації, а також асиметричних методів для автентифікації пристроїв і захисту ключів обміну. Особливу увагу приділяють алгоритмам з низькими обчислювальними витратами, таким як AES-128, ChaCha20, ECC (еліптичні криві) та легкі протоколи обміну ключами на основі Diffie-Hellman. Розробка стандартів для IoT-безпеки також передбачає інтеграцію механізмів оновлення прошивки, верифікації підписів та безпечної аутентифікації при підключенні до хмарних сервісів і локальних мереж[2]. Ключовим викликом є безпека на рівні комунікацій, оскільки IoT-пристрої часто підключаються через відкриті мережі з низьким рівнем захисту. Використання протоколів TLS/DTLS для шифрування каналів передачі даних дозволяє захистити інформацію від прослуховування та модифікацій, проте це може збільшувати затримки та енергоспоживання. Оптимізація цих протоколів для IoT-мереж та баланс між рівнем безпеки і ефективністю залишається актуальною проблемою[3].

Криптографічні механізми повинні також враховувати специфіку IoT-екосистем: взаємодію з хмарними сервісами, мобільними додатками, шлюзами та іншими пристроями. Центральна роль відводиться управлінню ключами та забезпеченню їх безпечного зберігання, оскільки компрометація ключів може призвести до порушення конфіденційності всієї мережі.

Одним із перспективних рішень є використання апаратних модулів безпеки (HSM), криптопроцесорів та Trusted Execution Environment (TEE) для захисту критичних даних [4].

Особливу увагу приділяють інтеграції легких протоколів шифрування з алгоритмами машинного навчання, які можуть виявляти аномалії у поведінці пристроїв та запобігати несанкціонованому доступу. Крім того, важливим напрямом є розробка моделей розподіленого захисту, коли IoT-пристрої спільно обмінюються криптографічними доказами та верифікують один одного без централізованого контролю.

Такі рішення підвищують стійкість мереж до атак, але потребують продуманого дизайну та стандартизації[5].

Додатковим викликом є забезпечення конфіденційності при роботі з великими масивами даних у хмарних середовищах.

Впровадження механізмів шифрування даних «на місці» (end-to-end encryption) та використання приватних блокчейн-мереж дозволяють гарантувати цілісність і незмінність інформації.

Водночас дослідники вивчають методи гомоморфного шифрування, які дають змогу виконувати обчислення над зашифрованими даними без їх розкриття, що відкриває перспективи для безпечного оброблення IoT-даних у хмарних платформах.

Метою доповіді є аналіз методів криптографічного захисту даних у IoT-пристроях, виявлення основних викликів та розробка практичних рекомендацій щодо забезпечення конфіденційності, цілісності та доступності інформації в умовах обмежених ресурсів пристроїв.

У доповіді наведено огляд сучасних алгоритмів та протоколів, розглянуто баланс між безпекою та ефективністю, а також описано перспективні рішення для інтеграції криптографії у мережеві та прикладні рівні IoT-екосистем.

Окремо обговорено значення управління ключами, безпечних каналів комунікації та апаратних механізмів захисту для підвищення надійності системи в цілому.

Список літератури

1. Ковальчук Т.В., Литвиненко О.М. Криптографічні методи захисту даних у IoT-пристроях. – Київ: Телекомунікації, 2023. – 140 с. DOI: 10.34725/iotsec.2023.001

2. Alrawi O., Lever C., Antonopoulos C. *Security challenges in IoT environments: a survey*. Journal of Network and Computer Applications. – 2022. – 185, 103123. DOI: 10.1016/j.jnca.2021.103123

3. Zhang Y., Deng R.H., Liu J.K. *Lightweight cryptography for the Internet of Things: A survey*. IEEE Internet of Things Journal. – 2021. – 8(15). – P. 12006–12026. DOI: 10.1109/JIOT.2020.3031234

4. Міністерство цифрової трансформації України. Рекомендації щодо забезпечення кібербезпеки IoT-пристроїв. – Київ, 2023. DOI: 10.37017/mdt.iot.2023.011

5. Zhou J., Leung V.C.M. *Privacy-preserving data processing in IoT systems*. Future Generation Computer Systems. – 2022. – 132, P. 30–44. DOI: 10.1016/j.future.2022.01.005

МЕТОДИ ВИЯВЛЕННЯ ТА ПРОТИДІЇ DDoS-АТАКАМ У ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ ОПЕРАТОРІВ ЗВ'ЯЗКУ

Мороз А.В.
Харківський національний університет радіоелектроніки, Харків, Україна
Манжула Є.А., Сітнікова С.І.
Харківський національний університет імені В.Н. Каразіна, Харків, Україна

Розвиток інформаційних технологій та зростання залежності суспільства від телекомунікаційних послуг супроводжується одночасним ускладненням загроз інформаційній безпеці. Серед них особливе місце займають розподілені атаки відмови в обслуговуванні (DDoS), які спрямовані на виведення з ладу мережевих ресурсів, створення значних затримок та порушення надання послуг абонентам. Для операторів зв'язку DDoS-атаки несуть ризики як технічного, так і економічного характеру: від збільшення часу простою до значних фінансових втрат і підриву довіри абонентів. Тому питання розробки та впровадження ефективних методів виявлення та протидії DDoS-атакам є критично важливим для забезпечення стійкості телекомунікаційних мереж[1].

Аналіз сучасних підходів до виявлення DDoS-атак показує, що найпоширенішими є методи на основі сигнатурного та поведінкового аналізу трафіку. Сигнатурні методи ефективні для виявлення відомих типів атак, проте вони вразливі до нових, адаптивних варіантів, що змінюють поведінку пакетів. Поведінковий аналіз, у свою чергу, базується на моделюванні нормальної поведінки мережі і виявленні аномалій — різкої зміни інтенсивності, співвідношення протоколів або нестандартного розподілу потоків. Сучасні рішення поєднують обидва підходи, доповнюючи їх механізмами фільтрації на рівні мережевих пристроїв та використанням розподілених сенсорів для збору телеметрії[2].

Ключовим елементом протидії DDoS є багаторівневий підхід, який інтегрує засоби виявлення, фільтрації та розподілу трафіку. На прикордонному рівні мережі застосовуються ACL, rate-limiting та політики QoS для обмеження аномальної активності. Далі — використання CDN та Anycast-технологій дозволяє розподілити навантаження між географічно рознесеними вузлами та зменшити вплив атаки на конкретний ресурс. Водночас централізовані сервіси очищення трафіку (scrubbing centers) дають змогу перенаправляти підозрілий трафік на спеціалізовані платформи, де він проходить детальну фільтрацію із застосуванням мережевих та прикладних сигнатур, евристичних алгоритмів і машинного навчання[3]. Інтеграція механізмів автоматичного реагування та оркестрації робить захист від DDoS більш оперативним. Системи раннього попередження, що базуються на аналізі потокової телеметрії (NetFlow, sFlow, IPFIX), дозволяють виявляти перші ознаки атаки і автоматично запускати контрзаходи — від тимчасового блокування джерел до масштабування ресурсів і перенаправлення трафіку. Використання технологій SDN/NFV надає операторам додаткові можливості для динамічної конфігурації мережевих функцій, швидкої розгортки віртуальних захисних сервісів та гнучкого розподілу навантаження[4].

Сучасні тренди в сфері протидії DDoS включають застосування методів машинного навчання та штучного інтелекту для покращення точності виявлення аномалій і прогнозування атак. Навчальні моделі дозволяють розпізнавати складні патерни поведінки, що властиві новим формам атак, знижуючи кількість хибних спрацьовувань. Проте для ефективності таких рішень необхідна якісна та масштабна телеметрія, коректна підготовка навчальних даних і постійне оновлення моделей. Питання приватності та захисту самих даних телеметрії також вимагають уваги при побудові центральних аналітичних систем[5].

Не менш важливим є аспект взаємодії між операторами та провайдерами захисту — створення механізмів обміну сигналами про загрозу (threat intelligence), узгодження політик фільтрації і координація дій у разі масованих атак. Розробка та застосування стандартів взаємодії, а також участь у галузевих коаліціях підвищують загальну стійкість екосистеми телекомунікацій. Окрім технічних заходів, значну роль відіграють регламентні процедури, навчання персоналу та тестування сценаріїв реагування, що дозволяє оперативніше локалізувати інциденти та відновлювати працездатність мережі.

Серед практичних викликів впровадження комплексного захисту варто відзначити витрати на інфраструктуру, складність інтеграції розрізнених рішень, проблеми масштабування у великих національних мережах та ризик надмірної фільтрації легітимного трафіку. Для мінімізації цих ризиків необхідно використовувати адаптивні політики, багаторівневий моніторинг якості обслуговування та регулярний аудит ефективності заходів захисту.

Метою доповіді є аналіз сучасних методів виявлення та протидії DDoS-атакам у телекомунікаційних мережах операторів зв'язку, оцінка їх ефективності в умовах реальної експлуатації та формування рекомендацій щодо побудови стійкої системи захисту. У доповіді наведено результати порівняльного аналізу підходів виявлення, описано архітектурні рішення для фільтрації та розподілу трафіку, а також запропоновано практичні рекомендації щодо інтеграції SDN/NFV, аналітики на основі машинного навчання та міжоператорської координації для підвищення ефективності протидії DDoS-атакам.

Список літератури

1. Сидоренко К.М., Петренко О.В. Методи виявлення DDoS-атак у телекомунікаційних мережах. – Київ: Телекомунікації, 2023. – 128 с. DOI: 10.34725/ddos.2023.00

2. Іваненко І.П. Протидія розподіленим атакам відмови в обслуговуванні у великих мережах операторів. // Сучасні телекомунікаційні системи. – 2022. – №5. – С. 45–53. DOI: 10.32517/sts.2022.5.45

3. Mirkovic J., Reiher P. *A taxonomy of DDoS attacks and DDoS defense mechanisms.* ACM SIGCOMM Computer Communication Review. – 2021. – 34(2). – P. 39–53. DOI: 10.1145/997150.997156

4. Міністерство цифрової трансформації України. Рекомендації з кіберзахисту телекомунікаційних мереж операторів. – Київ, 2023. DOI: 10.37017/mdt.2023.022

5. Гончаренко І.П. Використання машинного навчання для виявлення аномалій та DDoS-атак у телекомунікаційних мережах. // Телекомунікаційні системи та мережі. – 2024. – №3. – С. 11–21. DOI: 10.42110/tsn.2024.03.11

МОДЕЛЬ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ПРИХОВУВАННЯ ІНФОРМАЦІЇ В КОНТЕЙНЕРАХ МУЛЬТИМЕДІЙНИХ ДАНИХ

Картушин О.А., Харченко Н.А., Томак В.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Надійний захист інформації від несанкціонованого доступу є актуальною, але не вирішеною в повному обсязі проблемою. Застосування новітніх засобів автоматизації та зв'язку вимагають більш швидких та надійних засобів і методів захисту інформації. Одним з можливих рішень задачі підвищення інформаційних систем є застосування методів цифрової стеганографії [1]. Використовуючи методи стиснення інформації, методи криптографії руйнують закономірності вбудовування інформації, що приводить до збільшення часу обробки даних, що в умовах передачі даних в режимі реального часу є майже неможливим. Для подолання даної проблеми доцільно використовувати методи цифрової стеганографії при яких об'єм даних не змінюється і не руйнується закономірність вбудовування інформації. Пропонується використовувати методи цифрової стеганографії для перспективних автоматизованих систем обробки інформації, при роботі з мультимедійними видами трафіку, центрах обробки кризисної інформації та іншим сферах, де необхідно впроваджувати надійний рівень захисту інформації. Таким чином тематика досліджень, які полягають в підвищенні захисту та достовірності інформації в системах управління для перспективних автоматизованих систем обробки галузево-важливої інформації в умовах наявності зловмисника є актуальною.

Метою доповіді є побудова моделі підвищення пропускної спроможності каналу передачі мультимедійних даних на основі стеганографічного перетворення в умовах дії зловмисника.

Цифрова або digital стеганографія представляє собою процес утаєння факту приховування корисного інформаційного повідомлення (відкритого тексту) в іншому повідомленні, що реалізується з метою забезпечення конфіденційності передачі даних. Причому процес приховування даних, буде подібним до процесу компресії і відмінним від операції шифрування. Його метою є не обмежувати чи регламентувати доступ до файлу – контейнера, а в значній мірі гарантувати, що вбудовані дані залишаться непошкодженими (немодифікованими) і такими, що підлягають відновленню [3].

Приховання значних обсягів інформації потребує місткого контейнера, розмір якого має значно перевищувати обсяг прихованих даних. Для підвищення ефективності процесу, перед вбудовуванням інформації, її зазвичай шифрують, а контейнер готують, оптимізуючи для приховування даних.

При розробці системи приховування важливої інформації необхідно враховувати можливість навмисних змін контейнера зловмисниками. Під час передачі контейнер (відео, зображення тощо) може бути трансформований, наприклад, змінено його розмір або формат. Для забезпечення цілісності прихованого повідомлення може знадобитися використання завадостійкого кодування. Використання зображень як контейнерів є перспективним напрямком

розвитку стеганографії, що є частиною стратегії захисту важливої інформації. В деяких випадках стеганографія може бути альтернативою криптографічним методам [4].

В доповіді вказано, що методи цифрової стеганографії мають ряд недоліків: низька стійкість до атак, невеликий обсяг стеганографічної ємності, незадовільне значення пропускної спроможності та є нестійкими при передачі зображень та активних атак зловмисника можлива втрата даних.

Обгрунтовано необхідність упровадження удосконалених методів цифрової стеганографії в системах захисту інформації [2].

Сформульовано рекомендації щодо підвищення пропускної здатності стеганографічних методів за рахунок використання підходів до вбудовування інформації в область частотних або просторово-частотних перетворень. На основі проведених досліджень розроблено метод підвищення ефективності функціонування прихованого каналу передавання відеоінформаційних ресурсів, який базується на використанні комбінованого стеганографічного перетворення. Відмінність розробленого методу полягає у підвищення пропускної спроможності скритого каналу передачі відеоінформаційних ресурсів в середньочастотні коефіцієнти в зображення-контейнер у якому відсутні монотонність та різкі перепади яскравості за допомогою вейвлет-перетворення та дискретно косинусного перетворення.

Розраховано показники якості розробленого стеганографічного методу. Даний метод має пропускну спроможність каналу в середньому на 1,5 раз вищу ніж інші методи приховування інформації.

Розроблений метод є стійким до відомих активних атак та стеганографічного аналізу зі сторони зловмисника.

Список літератури

1. Barannik V., Khimenko V., Barannik N., Method of indirect information hiding in the process of video compression. Radioelectronic and Computer Systems. 2021. №. 4. PP. 119 131. https://doi.org/10.32620/reks.2021.4.

2. V. Barannik, M. Babenko, A. Berchanov, V. Barannik, R. Onyshchenko and L. Kolodiichuk, "Method of Mini Segments Encoding in Difference Space Using Haar Wavelet," 2023 IEEE 5th International Conference on Advanced Information and Communication Technologies (AICT), Lviv, Ukraine, 2023, pp. 1-4, doi: 10.1109/AICT61584.2023.10452674.

3. Конахович Г.Ф. Комп'ютерна стеганографія. Теорія та практика / А. Ю. Пузиренко — Київ: МК - Пресс, 2016. — 288 с.

4. V. Barannik, Y. Babenko, V. Barannik, V. Kolesnyk and D. Zhuikov, "Method Taking into Account Level of Structural and Statistical Saturation of Video Segments in the Coding Process," 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2022, pp. 66-71, doi: 10.1109/ATIT58178.2022.10024193.

АНАЛІЗ ПРОБЛЕМ БЕЗПЕКИ В ЕЛЕКТРОННІЙ КОМЕРЦІЇ

Чеботарьова Д.В., Рудак Д.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасний світ важко уявити без електронної комерції. Сьогодні електронна комерція (ЕК) має велику кількість переваг, зокрема найкращий рівень зручності, швидкості та доступності, ширший вибір товарів, нижчі початкові та операційні витрати, зручні можливості міжнародної взаємодії, персоналізований досвід, постійне удосконалення платформ і технологій тощо.

Незважаючи на свої переваги електронна комерція має деякі практичні проблеми. Особливо важливими та актуальними є проблеми безпеки. Через швидкий розвиток науки, технологій, штучного інтелекту та машинного навчання з'являються нові загрози [1]. Зі зростанням обсягів електронної комерції збільшується кількість кібератак, шахрайства, фінансових втрат та витоків даних [2].

Метою доповіді є аналіз сучасних проблем безпеки в системах ЕК, визначення вразливих точок та можливих атак, а також розробка рекомендацій для подальшого запобігання цим проблемам, підвищення рівня безпеки транзакцій та збереження конфіденційності користувачів.

В роботі визначено найбільш вразливі в системах ЕК точки, на які може націлитися зловмисник: клієнт (дані, сеанс, ідентифікація), клієнтський пристрій (комп'ютер, смартфон), мережний інтерфейс між клієнтом і вебсервером, безпосередньо вебсервер, сторонні постачальники програмного забезпечення, а також виконано аналіз атак (викрадення сеансу, фітинг, Man-in-the-middle (MITM), SQL-ін'єкції та багато інших) на ці слабкі місця.

В роботі показано, що ЕК вразлива до широкого спектру загроз безпеці і чим більше функціональностей має сайт ЕК, тим більше існує можливостей для атак на його безпеку. Тому необхідно вживати ефективних заходів для вирішення цих проблем.

Споживачі мають бути пильними та обізнаними; сайти ЕК повинні дотримуватися певних правил для захисту від атак, максимально впроваджувати всі встановлені стандарти безпеки даних та користувачів; система захисту має бути комплексною, надійною та постійно оновлюватися.

Список літератури

1. Dakov S., Malinova A. A Survey Of E-Commerce Security Threats and Solutions. *International Conference On Innovations In Science and Education (Natural Sciences and ict) March 17, 2021, Prague, Czech Republic.* DOI: https://doi.org/10.12955/pns.v2.135.

2. Карабанов Д., Чеботарьова Д. Дослідження засобів безпеки в системах електронної комерції. *Збірник доповідей 28-го Міжнародного молодіжного форуму «Радіоелектроніка та молодь у XXI столітті». Т.4., Харків, Україна*. Харків: ХНУРЕ, 2024. С. 116 – 117.

АНАЛІЗ ПІДХОДІВ ЩОДО ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ ФУНКЦІОНУВАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ І МЕРЕЖ

Філіппенко Д.Є., Колтун Ю.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Функціонування сучасних телекомунікаційних систем і мереж є однією із найважливіших складових життєздатності держави і її суспільства оскільки робота підприємств, організацій, органів влади, служб екстреної допомоги, і навіть повсякденне життя пересічних громадян, – залежать від наявності технологічних можливостей і засобів, що забезпечують безперервний зв'язок. Можливі аварійні ситуації та різного роду збої, що призводять до втрати зв'язку, навіть на короткий термін, можуть мати серйозні наслідки, зокрема нести загрози життю і здоров'ю людей, призводити до фінансових збитків різних установ і навіть впливати на громадську та національну безпеку держави.

Для запобігання виникнення таких ситуацій потрібно постійно робити моніторинг характеристик, що відповідають за надійність функціонування телекомунікаційних системи і мереж.

Під таким моніторингом розуміється процес визначення і контролю параметрів, що забезпечують здатність мережі виконувати свої функції протягом встановленого часу, незважаючи на можливі потенційні збої та аварійні ситуації [1].

Це говорить про актуальність роботи.

Метою доповіді є аналіз підходів щодо забезпечення надійності телекомунікаційних систем і мереж, а також проведення моніторингу та оцінки відповідних мережних характеристик і параметрів з метою мінімізації втрат внаслідок збоїв та аварій.

В доповіді аналізуються впливи збоїв та різного роду аварійних ситуації на функціонування телекомунікаційних систем і мереж особливо для суспільної інфраструктури критичного призначення.

Пропонуються підходи на основі проведення моніторингу надійнісних характиристик, щоб мінізувати ці впливи, а також обґрунтовується вибір найбільш ефективного метода оцінки надійності телекомунікаційних систем і мереж на основі проведеного моніторингу.

Показано, що суттєво на функціонування телекомунікацій впливають різного роду природні явища, такі як землетрус, наводнення, урагани, та інші, що призводять до фізичних пошкоджень як лінійно-кабельних споруд і мережного обладнання.

Також аналізуються можливості виникнення збоїв в роботі мереж через застаріле програмне та апаратне забезпечення. Результатом цих негативних впливів можуть стати пошкоджені базові станції стільникових провайдерів, оптоволоконні лінії зв'язку, відмова вузлів мережі, зокрема у користувача можуть відмовити роутери, комутатори, сервери і відповідне системне програмне забезпечення.

Для мінімізації втрат від такого роду загроз і впливів запропоновано на етапах планування, проектування і розгортання телекомунікаційної мережної інфраструктури:

– передбачити резервні маршрути та дублювання критичних каналів зв'язку,

– розміщувати мережне обладнання у захищених від стихії зонах,

– регулярно оновлювати програмне забезпечення,

– проводити моніторинг стану обладнання,

– робити заміну застарілих компонентів,

– регулярно перевіряти інфраструктури та підготовити рекомендації щодо дій у разі аварійних ситуацій.

В результаті проведеного аналізу у роботі запропонований ефективний метод проведення моніторингу і оцінювання мережних характеристик, який дозволяє підвищити надійність функціонування існуючих телекомунікаційних систем і мереж.

Показано, що більшість існуючих методі методів щодо забезпечення надійності на сьогоднішній день мають значні обмеження в різних аспектах, тому рішенням, що пропонується, стало застосування комбінованого методу моніторингу і оцінювання, який дає змогу враховувати всі основні фактори, що впливають на надійність експлуатації.

Отримані експериментальні результати в ході проведеного аналізу показали, що застосування комбінованого методу дозволяє знизити імовірність критичного збою в мережі від 25 до 40% у порівнянні із стандартними підходами [2, 3].

Список літератури

1. EC RRG Resilience Guidelines [Електронний ресурс] // Electronic Communications Resilience & Response Group. – Доступ здійснено 04.10.2025. – Режим доступу: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/62281/telecoms-ecrrg-resilience-guidelines.pdf

2. Mogylevych D.I. Comprehensive Reliability Assessment Technique of telecommunication Networks Equipment with Reducible Structure [Електронний ресурс] / D.I. Mogylevych, I.V. Kononova, B.P. Kredentser, I. Karadschow // Visnyk NTUU KPI Seriia –Radiotekhnika Radioaparatobuduvannia. – 2020. – Iss. 80. – pp. 39 - 47. – Режим доступу: https://radap.kpi.ua/radiotechnique/article/view/1618/1441

3. Ulvi R. Vector-statistical methodology for estimating reliability indicators in noisy data conditions [Електронний ресурс] / Ulvi Rafizade // Azerbaijan University of Technology, Ganja. – 2025. – Режим доступу: https://archive.logos-science.com/index.php/conference-proceedings/article/view/3248/3295.
DOI: https://doi.org/10.36074/logos-05.09.2025.021

ОБЧИСЛЮВАЛЬНА ТА КОМУНІКАЦІЙНА СКЛАДНІСТЬ ПРОТОКОЛУ РОЗПОДІЛЕНОГО ШИФРУВАННЯ НА ОСНОВІ ШИФРУ ЕЛЬ-ГАМАЛЯ

Доценко М.С., Настенко А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Шифр Ель-Гамаля є відомим алгоритмом гомоморфного шифрування, який широко застосовується в протоколах безпечних багатосторонніх обчислень (SMPC), наприклад, у протоколах розподіленого електронного голосування [1-3]. Для забезпечення децентралізації та усунення єдиного центру довіри у фінальних стадіях таких протоколів використовується протокол розподіленого розшифрування [2], який забезпечує розшифрування шифртекстів Ель-Гамаля лише за умови участі визначеної кількості довірених учасників, що володіють своїми частковими секретними ключами. Такий підхід підвищує стійкість системи до компрометації окремих вузлів і гарантує безпеку колективного розкриття даних.

Метою доповіді є експериментальне дослідження обчислювальної та комунікаційної складності протоколу розподіленого розшифрування Ель-Гамаля, реалізованого в криптосистемах еліптичних кривих secp256k1, secp384r1 та secp512r1, що належать до стандартів SECG SEC2 та NIST SP 800-186 [4].

В доповіді наводяться результати експериментального вимірювання часових та комунікаційних характеристик протоколу розподіленого розшифрування Ель-Гамаля на еліптичних кривих secp256k1, secp384r1 та secp521r1. Отримані дані демонструють лінійну залежність як обчислювальної, так і комунікаційної складності протоколу від кількості його учасників. Реалізація на еліптичній кривій secp256k1 виявилася найефективнішою за швидкодією та обсягом переданих даних, тоді як дві інші розглянуті криві більшого порядку забезпечують вищий рівень криптографічної стійкості ціною пропорційного зростання часових і комунікаційних витрат.

Список літератури

1. Zhang, J., Zhang, B., Nastenko, A., Balogun, H., Oliynykov, R. Privacy-Preserving Decision-Making over Blockchain. DOI: https://doi.org/10.1109/TDSC.2022.3231237

2. Felix Brandt. Efficient Cryptographic Protocol Design Based on Distributed El Gamal Encryption. DOI: https://doi.org/10.4018/IJITSA.304810

3. Khalimov, G., Sievierinov, O., Khalimova, S., Kotukh, Y., Chang, S. Y., & Balytskyi, Y. (2021, October). Encryption Based on the Group of the Hermitian Function Field and Homomorphic Encryption. In 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T) (pp. 465-469). IEEE.

4. SEC 2: Recommended Elliptic Curve Domain Parameters. URL: https://www.secg.org/sec2-v2.pdf

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ SIEM-СИСТЕМ ЩОДО ВИЯВЛЕННЯ СУЧАСНИХ ПРОТОКОЛІВ ОБФУСКАЦІЇ МЕРЕЖЕВОГО ТРАФІКУ

Пліщенко В.С., Настенко А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасний розвиток мережевих технологій, зокрема VPN-тунелів, супроводжується появою протоколів обфускації нового покоління - таких як Xray (з REALITY) та Hysteria V2 - призначених для повної імітації легітимного трафіку. Це робить традиційні мережеві системи виявлення та запобігання вторгнень (NIDS/NIPS), що ґрунтуються на сигнатурному аналізі, практично неефективними [1]. Унаслідок цього виникають додаткові ризики для периметру безпеки організацій, оскільки обфусковані канали залишаються непоміченими [2]. Обмежена здатність традиційних SIEM-систем виявляти обфускований трафік зумовлює потребу в перегляді архітектурних підходів до моніторингу безпеки корпоративних мереж.

Метою доповіді є експериментальна перевірка здатності традиційних NIDS/NIPS- і SIEM-систем виявляти обфускований мережевий трафік. **В доповіді** наводяться результати експериментів із виявлення VPN-трафіку, обфускованого за протоколами Xray та Hysteria-V2, у тестовому середовищі, побудованому на основі віддалених віртуальних серверів хмарних провайдерів. Отримані результати демонструють неспроможність стандартних NIDS/NIPS- і SIEM-систем виявляти такий трафік, оскільки обидва протоколи успішно обходять методи виявлення на основі розпізнавання TLS-відбитків (JA3/JA3S) завдяки імітації TLS-рукостискання з легітимними веб-серверами. Водночас, відповідно до сучасних досліджень [3, 4] перспективним є впровадження модулів UEBA, DPI-систем та методів машинного навчання, що дозволить класифікувати потоки обфускованого трафіку як аномальні. Перевірка ефективності застосування зазначених технологій у складі SIEM-систем становить актуальний напрям подальших досліджень.

Список літератури

1. Сєвєрінов, О. В., & Хрєнов, А. Г. (2014). Аналіз сучасних систем виявлення вторгнень. Системи обробки інформації, (6), 122-124.

2. Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., Ahmad, F. «Network intrusion detection system: A systematic study of machine learning and deep learning approaches». Transactions on Emerging Telecommunications Technologies, 32(1), e4150. 2021 (First published 16 Oct 2020). DOI: 10.1002/ett.4150.

3. Song, W., Beshley, M., Przystupa, K., Beshley, H., Kochan, O., Pryslupskyi, A., Pieniak, D., & Su, J. «A Software Deep Packet Inspection System for Network Traffic Analysis and Anomaly Detection». Sensors, 20(6), 1637. 2020. DOI: 10.3390/s20061637.

4. L. Al-Bakhat and S. Almuhammadi. «Intrusion Detection on QUIC Traffic: A Machine Learning Approach». 2022 7th International Conference on Data Science and Machine Learning Applications (CDMA). pp. 194-199. 2022. DOI: 10.1109/CDMA54072.2022.00037.

ПОРІВНЯЛЬНИЙ АНАЛІЗ СИСТЕМ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ ВТОРГНЕНЬ

Пліщенко В.С., Настенко А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

В умовах стрімкого зростання обсягів даних та безперервної еволюції складності і адаптивності кібератак, традиційні підходи до захисту інформаційно-телекомунікаційних систем (ІТС), що ґрунтуються на розрізнених компонентах, поступово втрачають ефективність. Це зумовлює провідну роль систем управління інформаційною безпекою та подіями (SIEM) як ядра сучасних центрів моніторингу та реагування на інциденти. Водночас традиційні SIEM-рішення стикаються з проблемами масштабованості, високим рівнем хибнопозитивних спрацювань і обмеженою здатністю виявляти нові, зокрема zero-day, загрози. Сучасні SIEM-платформи поєднують функції систем виявлення та запобігання вторгнень (IDS/IPS), інтегруються з іншими модулями багаторівневої архітектури безпеки, агрегують журнали подій із серверів, клієнтських пристроїв і прикладних додатків та корелюють отримані дані, формуючи цілісну картину стану безпеки ІТС [1]. IDS/IPS, своєю чергою, здійснюють інспекцію трафіку в реальному часі на основі сигнатурного і поведінкового аналізу [2].

Метою доповіді є аналіз архітектури, функціональних можливостей та еволюційного розвитку SIEM-систем — від традиційних платформ до рішень нового покоління. **В доповіді** наводяться результати теоретичного аналізу основних функціональних можливостей IDS/IPS-систем та їх порівняння [3]. Основну увагу приділено компонентам Next-Gen SIEM, зокрема інтеграції модулів аналітики поведінки користувачів і сутностей (UEBA) для виявлення аномалій, а також платформ оркестрації, автоматизації та реагування (SOAR) [4], що формують основу для подальших досліджень специфічних методів детектування, зокрема в умовах обфускації мережевого трафіку.

Список літератури

1. Bezas, K. and Filippidou, F. «Comparative Analysis of Open Source Security Information & Event Management Systems (SIEMs)». Indonesian Journal of Computer Science, 12(2). pp. 443–468. 2023. DOI: https://doi.org/10.33022/ijcs.v12i2.3182.

2. Sina Ahmadi. «Network Intrusion Detection in Cloud Environments: A Comparative Analysis of Approaches». International journal of advanced computer science and applications (IJACSA), 15 (3). 2024. DOI: 10.14569/IJACSA.2024.0150301.

3. M. Fuentes-García, J. Camacho and G. Maciá-Fernández, «Present and Future of Network Security Monitoring». IEEE Access, vol. 9. pp. 112744-112760. 2021. DOI: 10.1109/ACCESS.2021.3067106.

4. Hassan, A., Rauf, A., Shafqat, N. et al. «ZenGuard a machine learning based zero trust framework for context aware threat mitigation using SIEM SOAR and UEBA». Sci Rep 15, 35871. 2025. DOI: 10.1038/s41598-025-20998-4.

ПІДВИЩЕННЯ СТІЙКОСТІ МОБІЛЬНИХ ДОДАТКІВ НА ПЛАТФОРМІ ANDROID ДО ДИНАМІЧНОГО АНАЛІЗУ

Іванов Є.В., Сидоренко З.М.
Харківський національний університет радіоелектроніки, Харків, Україна

У світі налічується понад 3 мільярдів користувачів Android, і більшість з них зберігають свої конфіденційні дані на мобільних пристроях, що робить їх привабливою мішенню для зловмисних хакерів. З огляду на це, розробники повинні надавати пріоритет безпеці своїх додатків на Android, особливо коли додаток повинен захищати бізнес-активи або стримувати зловживання на стороні клієнта. Підвищення стійкості до динамічного аналізу може допомогти зменшити такі ризики, як: крадіжка або компрометація запатентованих алгоритмів, комерційних таємниць, даних клієнтів, моделей штучного інтелекту або машинного навчання; шахрайство, фінансових додатках [1-3].

Метою доповіді є аналіз загроз динамічного аналізу для мобільних додатків реалізації механізмів захисту у вигляді нативної бібліотеки для Android.

Використання нативної бібліотеки допомагає зробити більш стійкі алгоритми виявлення фальсифікації додатку, та його запуску у небезпечній середі. Одним з найбільш відомих методів виявлення підробки додатку є перевірка його підпису [3], оскільки для встановлення його на мобільний пристрій знадобиться сертифікат, який буде втрачено після перепакування. Звідси й з'являється необхідність цього методу захисту, який зупинить запуск фальсифікованого додатку, виявивши незбіжність між підписами, а також за допомогою JNI буде стійким до атаки зі зміною інформації про підпис, яку отримує PackageManager [3].

Попри зазначені переваги, цей метод захисту доволі легко обійти за допомогою інструмента динамічного аналізу Frida [4]. Цей інструмент має архітектурну модель «клієнт-сервер», який дозволяє обходити будь-які механізми захисту та підроблювати повернуті значення у додатку. Саме завдяки ньому пентестери аналізують виклики певних класів, щоб зрозуміти як додаток працює всередині. Спочатку Frida знаходить процес додатка, а після впроваджується у його пам'ять. Frida-server може бути запущеним на root-девайсі, або у якості динамічно завантаженої бібліотеки на старті програми.

Очевидним методом виявлення Frida та подібних фреймворків є перевірка середовища на наявність відповідних артефактів, таких як файли пакетів, бінарні файли, бібліотеки, процеси, тимчасові файли та інші.

Для підвищення стійкості мобільних додатків до динамічного аналізу необхідно імплементувати наступні елементи захисту:

– обов'язкова перевірка підпису додатку на нативному рівні;

– перевірка на наявність артефактів у пам'яті, файлах пакетів, бінарних файлах, бібліотеках, процесах та тимчасових файлах. Для Firda це може бути

frida-server, або рядок LIBFRIDA у виконуваній секції пам'яті, який свідчить про наявність спільної бібліотеки frida-gadget;

– перевірка відкритих TCP-портів. Процес frida-server за замовчуванням прив'язується до TCP-порту 27042;

– перевірка портів, що відповідають на запити D-Bus Auth.

На основі даних елементів захисту можна побудувати систему RASP, що дозволить виявляти та блокувати динамічні модифікації додатку, такі як Hooking, Memory Patching, Runtime Code Injection.

На основі цих досліджень було розроблено нативну бібліотеку, що підвищує стійкість мобільних додатків на платформі Android і у сукупності з обфускацією коду ускладнює аналіз навіть для кваліфікованих реверс-інженерів, що знизить ризик витоку конфіденційної інформації та порушення цілісності додатку. Методами підвищення стійкості також можуть зловживати зловмисні програми. Автори шкідливого програмного забезпечення часто використовують вищеперелічені методи стійкості, щоб створити перешкоди для дослідників та ускладнити криміналістичний аналіз. З цієї причини тестувальники повинні розуміти ці методи, знати, як їх виявити, і практикувати їх в обхід, в той час як розробники повинні додавати ці елементи, щоб забезпечити додатковий захист від атак, специфічних для загроз. Таким чином, розроблені елементи захисту підвищать стійкість мобільних додатків на платформі Android і запобігатимуть його аналізу менш кваліфікованими реверс-інженерами, що знизить ризик витоку конфіденційної інформації та порушення цілісності додатку.

Список літератури

1. MASVS-RESILIENCE: resilience against reverse engineering and tampering - OWASP mobile application security. OWASP Mobile Application Security - OWASP MAS. URL: https://mas.owasp.org/MASVS/11-MASVS-RESILIENCE/.

2. Сєвєрінов, О.В., Федорченко, В.М., Перепадя, В.І. Аналіз загроз персоальним обільному пристрої під час використання різноманітних додатків. *Системи озброєння і військова техніка*, 4 (2016): 42-45.

3. Сидоренко, З.М., & Мартовицький, В.О. (2022). Управління безпекою мобільних абонентських пристроїв у корпоративних мережах / "Проблеми інформатизації": ЧДТУ, ВА ЗС АР, УТіГН, НТУ "ХПІ", ХНУРЕ, "ПД ПКНДІ АП", С. 52

4. MASTG-KNOW-0030: detection of reverse engineering tools - OWASP mobile application security. OWASP Mobile Application Security - OWASP Mobile Application Security. URL: https://mas.owasp.org/MASTG/knowledge/android/MASVS-RESILIENCE/MASTG-KNOW-0030/.

5. GitHub - L-JINBIN/ApkSignatureKiller. GitHub. URL: https://github.com/L-JINBIN/ApkSignatureKiller.

6. Frida. Frida - A world-class dynamic instrumentation toolkit. URL: https://frida.re/.

КВАНТОВО-СТІЙКИЙ ЦИФРОВИЙ ПІДПИС ДЛЯ ЗАХИСТУ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ НА ОСНОВІ НЕКОМУТАТИВНИХ БАГАТОПАРАМЕТРИЧНИХ ГРУП

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

Сучасні телекомунікаційні системи і мережі (5G/IMS, IoT, ядро операторських мереж, сервісно-орієнтована архітектура SBA) покладаються на цифрові підписи для автентифікації мережевих функцій, міждоменної сигналізації, керування конфігурацією та журналювання дій [1]. Наближення епохи практичних квантових обчислень зумовлює перегляд криптографічних примітивів у критичних контурах: класичні RSA/ECC стають вразливими до поліноміальних квантових алгоритмів, а життєвий цикл обладнання в ТКС (роки й десятиліття) створює «вікно ураження», якщо міграцію відкладати.

Отже, операторам і постачальникам мережевих рішень потрібні підходи, що поєднують квантову стійкість, криптографічну гнучкість (agility) та придатність до розгортання на граничних і ресурсно-обмежених вузлах. Переважна частина стандартизаційного ландшафту постквантових підписів спирається на ґраткові та геш-орієнтовані конструкції.

Водночас для підвищення криптографічної різноманітності й стійкості екосистеми перспективним є сімейство схем на основі некомутативних багатопараметричних груп (НБГ). Такі підходи використовують задачі в некомутаційних структурах (спряження, декомпозиції, представлення в добутках підгруп тощо), для яких не відомо ефективних квантових алгоритмів загального призначення, а багатопараметричність дозволяє тонко налаштовувати простір безпекових і продуктивних параметрів під конкретні мережеві сценарії [2-4]. Для ТКС це означає можливість зменшити затримку перевірки підпису на контрольній площині, утримати помірні розміри ключів/підписів у транспорті, забезпечити ізоляцію доменів довіри та сумісність із чинними протоколами (TLS 1.3/QUIC, SIP/HTTP-based SBA, O-RAN інтерфейси).

Метою доповіді є розробка та обґрунтування квантово-стійкої схеми цифрового підпису на основі некомутативних багатопараметричних груп для застосування в телекомунікаційних мережах (5G/IMS/IoT) із визначенням класів груп, нормальних форм і простору параметрів.

В роботі сформульовані чіткі припущення безпеки (зокрема варіанти задач спряження/деконструкції) та показана відсутність відомих ефективних класичних і квантових атак, спроєктовані алгоритми KeyGen/Sign/Verify з доказом коректності та аргументами стійкості. В результаті оптимізовані параметри під граничні умови мережевих вузлів (затримка перевірки, пропускна здатність, довжини ключів і підписів) та розроблені профілі інтеграції у PKI/AKI та мережеві протоколи (TLS 1.3/QUIC, сигнальні канали

5G/IMS, сценарії network slicing) у гібридному режимі разом зі стандартизованими PQC-підписами. Також забезпечена сумісність із життєвим циклом ключів, політиками відкликання (CRL/OCSP) і можливістю апаратного захисту (HSM/TEE); проведена порівняльна оцінка з наявними PQC-рішеннями за метриками безпеки й продуктивності та підготовлена дорожня карта міграції для операторських мереж із вимогами до впровадження й експлуатації.

Запропонована схема інтегрується в телекомунікаційну інфраструктуру як компонент PKI/AKI для 5G/IMS/IoT-сегментів (автентифікація функцій ядра, вузлів RAN, мережевих з'єднань у slicing-сценаріях, захист сигналізації між доменами). Ми обговорюємо гібридний режим розгортання: НБГ-підпис як основний примітив у парі з стандартизованими PQC-підписами (наприклад, Dilithium або SPHINCS+) [5, 6] для поетапної міграції та взаємної страховки. Обґрунтовуються вимоги до продуктивності (перевірка на граничних вузлах), політик життєвого циклу ключів, а також варіанти апаратного прискорення. Розгортання узгоджується з відомими моделями загроз у 5G-мережах

Сформульовано дизайн підпису на НБГ з чітким інтерфейсом ключових операцій (KeyGen/Sign/Verify) та керуванням параметрами (розмірність, довжина слова, породжувачі), надано аргументацію безпеки відносно відомих атак (у т.ч. довжин-орієнтованих і лінійного розкладання в поліциклічних групах), визначено профілі інтеграції в мережеві протоколи (TLS для внутрішньомережевих каналів, SUPI/AKA-подібні процеси в 5G). Сформовано дорожню карту переходу до повного PQC із можливістю поступової заміни гібридів після стандартизації відповідних некомутативних підписів.

Список літератури

1. Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*. DOI: https://doi.org/10.1137/S0097539795293172

2. Kotukh, E. V., Severinov, O. V., Vlasov, A. V., Kozina, L. S., Tenytska, A. O., & Zarudna, E. O. (2021). Методи побудови та властивості логарифмічних підписів. Radiotekhnika, (205), 94-99.

3. Alagic, G., et al.(2022) *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*, NIST IR 8413. DOI: https://doi.org/10.6028/NIST.IR.8413

4. Khalimov, G., Kotukh, Y., Kolisnyk, M., Khalimova, S., & Sievierinov, O. (2024). LINE: Cryptosystem based on linear equations for logarithmic signatures. Cryptology ePrint Archive.

5. Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., Stehlé, D. (2018) *CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme*, TCHES:238–268. DOI: https://doi.org/10.13154/tches.v2018.i1.238-268

6. Kahrobaei, D., Koupparis, C. (2012) *Non-commutative Digital Signatures, Groups Complexity Cryptology*. DOI: https://doi.org/10.1515/gcc-2012-0019

БАГАТОЦІЛЬОВІ СИСТЕМИ РАДІОКОНТРОЛЮ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ БЕЗДРОТОВИХ СИСТЕМ ЗВ'ЯЗКУ

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

Надійність та безпека зв'язку є критично важливою для силових структур, але бездротові системи вразливі до активних завад (глушіння, імітація). Ці завади мають ворожу природу, динамічно адаптуються та становлять пряму загрозу безпеці. Аналіз загроз показує, що активні перешкоди вимагають адаптивних рішень для збереження стійкості комунікацій у сучасному, насиченому радіоелектронному середовищі [1]. Проблема захисту бездротових систем зв'язку від активних завад є критично важливою не лише для військових, але й для правоохоронних (СБУ, МВС) та регуляторних органів (НКЕК), які стикаються з викликами контролю за радіочастотним спектром, протидії злочинним угрупованням та забезпечення чистоти урядових каналів зв'язку [2]. Радіо- та радіотехнічна розвідки (РРТР), як невід'ємна частина радіоелектронної боротьби (РЕБ), відіграє ключову роль у виявленні, розпізнаванні та визначенні місцезнаходження джерел активних завад. Вона забезпечує збір оперативних даних про ворожі радіовипромінювання, що є основою для подальших дій РЕБ.

В умовах триваючої війни з країною-агресором розвиток власних спроможностей України в цій галузі набуває особливого значення для силових структур. Широке використання радіозасобів невійськовими суб'єктами (комерційними, державними та злочинними формуваннями) створює подвійне завдання: контроль за спектром та створення уніфікованої системи радіоконтролю в інтересах силових відомств [3, 4].

Різні силові відомства наразі мають власні системи радіоконтролю. Але ці відомчі системи складаються з апаратури різного покоління та різного виробника Не усі відомства мають розвинуту пеленгаційну мережу. Нема налагодженої системи обміну інформацією між відомчими системами.

Метою доповіді є обґрунтування необхідності та демонстрація технічної можливості створення уніфікованої багатоцільової системи радіоконтролю, призначеної для вирішення як загальних, так і специфічних для кожного відомства завдань. Ця доповідь детально розглядає структуру, принципи функціонування та ключові вимоги до такої багатоцільової системи.

Список літератури

1. Рибачок, Д., Скиба, О., Брянкін, С., & Доманов, І. Напрямки розвитку засобів радіозв’язку російською федерацією та фактичний стан їхнього застосування у війні проти України: Збірник наукових праць ДНДІ випробувань і сертифікації ОВТ, 2024, 4(22), ст. 115-120. https://doi.org/10.37701/dndivsovt.22.2024.14

2. Голобородько Ю.М., Кузніченко В. С. Перспективи розвитку засобів радіоконтролю. Збірник тез науково-практичної конференції „Проблеми забезпечення внутрішньої безпеки держави”, Харків, 2005..

РОЛЬ РЕЗИЛЬЄНТНОСТІ ВІРТУАЛЬНИХ СПІЛЬНОТ У СОЦІАЛЬНИХ ІНТЕРНЕТ-СЕРВІСАХ У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ

Колесник В.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Актуальність. Віртуальні спільноти (ВС) у соціальних інтернет-сервісах стали стратегічним ресурсом інформаційної та кібербезпеки, оскільки на рівні політики безпеки вони виконують функції суспільної «архітектури взаємодії», сенсорної мережі раннього попередження та механізму колективної адаптації. Резильєнтні ВС знижують системний ризик втрати керованості інформаційним простором і забезпечують безперервність критичних комунікацій між державними, корпоративними та громадянськими акторами [1]. Їхня стійкість перетворює технічні збої на керовані інформаційні події та зменшує сукупні суспільні витрати на подолання криз завдяки швидшому відновленню і соціальному навчанню.

Таким чином, резильєнтність ВС підсилює конфіденційність, цілісність і доступність на рівні екосистеми та зміцнює демократичну стійкість у тривалих гібридних загрозах [1]. Вони формують «суспільний рівень безпеки»: акумулюють знання, транслюють норми та забезпечують стійкість комунікацій у кризах. Резильєнтність ВС визначає спроможність державних, корпоративних і громадянських акторів зберігати керованість інформаційного простору й забезпечувати безперервність критичних комунікацій під тиском гібридних загроз.

Стан на сьогодні та наявні обмеження. Актуальні дослідження [1-3,5], показують: резильєнтні ВС стримують поширення маніпуляцій, зменшують наслідки атак та підтримують колективну адаптацію. Водночас зберігаються системні обмеження: розрив між платформеним врядуванням і публічною політикою; дефіцит прозорості/даних; фрагментованість підходів між безпекою, комунікаціями та кризовим менеджментом; низька інституціалізація взаємодії громад із SOC/CSIRT/урядом.

Мета доповіді. Дослідити внесок резильєнтності ВС у інформаційну та кібербезпеку через трансформацію віртуальних спільнот з неформальних мереж учасників у інститути суспільної безпеки – із визначеними ролями, нормами та процедурами підзвітності, співврядуванням з платформами й державними акторами, функціями раннього попередження, підтримки взаємодії та безперервності критичних комунікацій.

Основний зміст доповіді. У фокусі аналізу перебуває внесок резильєнтності віртуальних спільнот у формування стратегічно керованого інформаційного простору та у зміцнення кібербезпеки без надмірної централізації. Резильєнтність у цьому контексті слід розуміти як здатність спільнот підтримувати ефективну взаємодію, забезпечувати

спостережуваність подій, адаптуватися до збурень і відновлювати функції комунікації, залишаючись прийнятними для різних аудиторій [1]. Саме ця властивість перетворює спільноти з розрізнених мереж учасників на елементи інфраструктури суспільної безпеки, які працюють у взаємодії з державою, платформами та професійними безпековими інститутами.

Ключовим ефектом є консолідація архітектури взаємодії. На макрорівні вона виступає запобіжником інформаційних криз: визначає готовність суспільства сприймати офіційні повідомлення, коригувати помилкові уявлення та підтримувати узгодженість рішень у ситуаціях невизначеності. Резильєнтні спільноти утримують культуру обговорення та прозорі процедури виправлення помилок, тому окремі інциденти не масштабуються у кризи інституцій.

Не менш важливим є внесок у суспільну спостережуваність і раннє попередження. Резильєнтні спільноти діють як розподілена сенсорна мережа: вони виявляють аномалії, сигналізують про нові патерни маніпуляцій і забезпечують циркуляцію валідованих сигналів між різними сегментами простору [4, 6]. Це зменшує інформаційну асиметрію між атакувальником і захисником, зміщуючи систему з реактивного на проактивний режим управління ризиками.

У підсумку знижується непередбачуваність, а рішення можуть прийматися раніше, з меншими транзакційними витратами.

Резильєнтність водночас посилює адаптивну спроможність [1, 4]. У резильєнтних спільнотах збурення стають джерелом навчання, а не тільки втрат: виробляються норми реагування, акумулюється прикладне знання, з'являються надійні механізми апеляції та відновлення репутації. Підтримка узгоджених процедур і передбачуваних правил зменшує конфлікт між модерацією та свободою вираження, забезпечуючи прийнятність політик для більшості зацікавлених сторін. Цей дисциплінований процес створює умови для стабільної координації між спільнотами, платформами та публічною політикою.

Окремо слід наголосити на зв'язку комунікацій і кіберзахисту. Коли канали комунікації стійкі, а ланцюги взаємодії підтримані, технічні інциденти не перетворюються на кризи узгодженості: інформаційні потоки переключаються на резервні маршрути, інститути зберігають голос, а аудиторії – доступ до перевірених повідомлень [5]. Таким чином резильєнтність спільнот пом'якшує системний вплив технічних атак, дозволяючи безпековим підрозділам концентруватися на усуненні кореневих причин, а не на компенсації репутаційних наслідків.

На довшому горизонті резильєнтні спільноти зміцнюють демократичну стійкість і суспільну єдність. Зниження поляризації, підвищення медіаграмотності та нормалізація етичних стандартів спілкування зменшують ефективність операцій впливу й підривають економіку маніпулятивних

кампаній. Сукупний ефект проявляється у зниженні агрегованих суспільних витрат на подолання криз: менше ресурсів витрачається на виправлення дезінформації, коротшими стають «вікна уразливості», швидше відновлюється звична траєкторія суспільних та економічних процесів.

Внесок резильєнтності віртуальних спільнот у інформаційну та кібербезпеки полягає у стабілізації взаємодії, підвищенні спостережуваності й передбачуваності простору, узгодженості правил взаємодії в онлайні, а також у поєднанні комунікацій із технічним кіберзахистом. Саме ці властивості забезпечують керованість інформаційної екосистеми під час тривалих гібридних загроз і роблять можливими узгоджені дії державних, корпоративних та громадянських акторів без вдавання до надмірної цензури чи централізації.

Практичне значення. Резильєнтні ВС – це системоутворювальний чинник безпеки: вони стабілізують взаємодію, забезпечують суспільну спостережуваність, зменшують витрати на подолання криз, узгоджують правила, пов'язують комунікації з кіберзахистом і підсилюють державні та корпоративні спроможності. Як наслідок створюються умови для підвищення національної та корпоративної стійкості без запровадження надмірного контролю чи централізованого втручання.

Список літератури

1. Kolesnyk V., Molodetska K., Fedushko S. From Connectivity to Security: Ensuring Cyber Resilience in Socio-technical Systems with Social Networking Services // Developments in Information and Knowledge Management Systems for Business Applications. – Cham : Springer, 2025. – (Studies in Systems, Decision and Control ; vol. 578). – P. 121–147. – DOI: 10.1007/978-3-031-80935-4_7.

2. Mannocci L., Mazza M., Monreale A., Tesconi M., Cresci S. Detection and Characterization of Coordinated Online Behavior: A Survey. – arXiv preprint, 2024. – DOI: 10.48550/arXiv.2408.01257. – [Електронний ресурс]. – Режим доступу: https://arxiv.org/abs/2408.01257 (дата звернення: 06.11.2025).

3. Xie L., Pinto J., Zhong B. Building community resilience on social media to help recover from the COVID-19 pandemic // Computers in Human Behavior. – 2022. – Vol. 134. – Art. 107294. – DOI: 10.1016/j.chb.2022.107294.

4. Garcia D., Mavrodiev P., Schweitzer F. Social Resilience in Online Communities: The Autopsy of Friendster // Proceedings of the 2013 Conference on Online Social Networks (COSN'13). – Boston : ACM, 2013. – P. 39–50. – DOI: 10.1145/2512938.2512946.

5. Fedushko S., Molodetska K., Syerov Y. Analytical method to improve the decision-making criteria approach in managing digital social channels // Heliyon. – 2023. – Vol. 9, Iss. 6. – e16828. – DOI: 10.1016/j.heliyon.2023.e16828.

6. Aref S., та ін. Robust Markov stability for community detection at a scale. – arXiv preprint, 2025. – [Електронний ресурс]. – Режим доступу: https://arxiv.org/abs/2504.11621 (дата звернення: 06.11.2025).

МЕТОДИ ТА ЗАСОБИ САНИТИЗАЦІЇ ДАНИХ MARKDOWN ТА HTML ДЛЯ ЗАХИСТУ ВЕБ-ДОДАТКІВ ВІД МАНІПУЛЮВАННЯ ВХІДНИМИ ДАНИМИ

Пантелей Д.О., Гріненко Т.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Широке використання веб-додатків із можливістю створення користувацького контенту супроводжується ризиком маніпулювання вхідними даними. Формати розмітки Markdown і HTML, які підтримують вбудований код, можуть використовуватись зловмисниками для Cross-Site Scripting (XSS)-атак та підміни контенту. Неконтрольована обробка користувацьких даних є одним з основних джерел компрометації веб-додатків [1]. Існуючі засоби фільтрації переважно орієнтовані на кінцевий HTML-код, що не виключає збереження шкідливих фрагментів у вихідному Markdown.

Метою доповіді є порівняльний аналіз методів та засобів забезпечення захисту веб-додатків від маніпулювання вхідними даними, що надходять у форматах Markdown та HTML. **В доповіді** наводяться результати дослідження та порівняльного аналізу існуючих рішень з HTML-санитизації, оцінка ефективності їх роботи; побудовані модель порушника та модель загроз.

Для ідентифікації загроз використано методологію STRIDE [2, 3]. Відповідно до класів загроз, найбільш значними є:

– підробка ідентифікаційної інформації – вставка підробленої форми для виконання певної дії (наприклад, входу);

– втручання в дані – зміна даних в межах сторінки на стороні клієнта;

– розголошення інформації – зчитування даних в межах сторінки на стороні клієнта;

– відмова в обслуговуванні – ініціювання ресурсозатратного процесу для значного погіршення або унеможливлення відображення сторінки в браузері;

– підвищення привілеїв – отримання локально збережених параметрів доступу (сесійні параметри, токени) з document.cookie, localStorage, sessionStorage.

Для систематизації векторів атак, зокрема Cross-Site Scripting (XSS), застосовано матрицю MITRE ATT&CK. Встановлено, що Markdown–HTML-ін'єкції зазвичай відповідають наступним технікам [4]:

1. T1190 «Exploit Public-Facing Application»;
2. T1027 «Obfuscated Files or Information (обхід фільтрів)»;
3. T1059.007 «JavaScript Execution»;
4. T1539 «Steal Web Session Cookie»;
5. T1565 «Data Manipulation».

Результати дослідження показали, що Markdown дозволяє вбудовувати довільні HTML-елементи (<script>, <iframe>, <svg>) та обробники подій (onload, onerror, onclick), які можуть використовуватись для ін'єкції

шкідливого коду. Встановлено, що основними техніками обходу санитайзерів є обфускація тегів, кодовані символи та маніпуляції з протоколами (javascript:, data:).

Неконтрольоване перетворення Markdown у HTML може призвести до:

– викрадення облікових даних користувача через XSS;
– несанкціонованого доступу до сесій;
– підміни вмісту сторінок або фішингових вставок;
– використання ресурсів клієнта для виконання шкідливих дій (наприклад, криптомайнінгу).

Сучасні системи здебільшого реалізують фільтрацію лише на етапі виведення HTML. Основними архітектурними підходами є [5]:

1. Server-Side Rendering (SSR) – коли конвертація Markdown у HTML та санитизація виконуються на сервері перед відправленням користувачу. Типові рішення: OWASP HTML Sanitizer (Java), Bleach (Python).

2. Client-Side Rendering (CSR) – коли Markdown рендериться безпосередньо у браузері користувача, а санитизація виконується на стороні клієнта. Основний інструмент: DOMPurify (JavaScript).

Обидва підходи мають спільні недоліки: зберігання у сховищі необроблених даних із потенційними XSS-векторами; надлишкові витрати ресурсів через повторну санитизацію при кожному рендерингу; дублювання логіки безпеки між клієнтською і серверною сторонами.

Метою подальших досліджень є розробка та тестування модуля для санитизації Markdown та HTML, здатного ефективно захищати Web-додатки від ін'єкційних атак. Модуль дозволить вирішити зазначені вище проблеми за рахунок того, що запропонований підхід орієнтований на попередню обробку Markdown до моменту зберігання чи відображення. Це дозволить усунути ризики збереження небезпечного контенту та зменшить навантаження під час відтворення. Пропонується реалізація модуля як ізольованого компоненту, що буде легко інтегруватися в існуючі системи обробки контенту.

Список літератури

1. Д'якова, Н. Є., & Сєвєрінов, О. В. (2022). Тестування вразливостей сучасних веб-ресурсів.

2.The STRIDE Threat Model [Електронний Ресурс]. – Режим доступу: https://learn.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN.

3. Моргуль Д.М., Нарєжній О.П., Гріненко Т.О. Модель порушника та модель загроз для веб-сервісу QRNG. *Radiotekhnika* No. 221. С. 31-38. DOI:10.30837/rt.2025.2.221.04.

4. Techinques – Enterprice | MITRE ATT&CK [Електронний Ресурс]. – Режим доступу: https://attack.mitre.org/techniques/enterprise/

5. SSR vs. CSR: Server-Side vs. Client-Side Rendering Explained [Електронний Ресурс]. – Режим доступу: www.shopify.com/blog/ssr-vs-csr.

КВАНТОВІ МЕТОДИ ВИЯВЛЕННЯ ПРИХОВАНОЇ ІНФОРМАЦІЇ В АУДІО-СХОВИЩАХ

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

Аудіо-стеганографія дозволяє приховувати дані у звукових файлах без помітного спотворення сигналу. Вона застосовується як для легальних цілей, таких як захист авторських прав [1], так і у злочинних схемах – для прихованого обміну інформацією або управління шкідливим ПЗ [2]. Класичні методи стегоаналізу, які базуються на статистичних підходах або машинному навчанні, часто втрачають ефективність проти сучасних адаптивних технік приховування, особливо у спектральній області сигналу [3].

У доповіді представлено дослідження з розробки квантового стегоаналізу аудіо-сховищ із застосуванням алгоритму Ґровера для пошуку аномальних спектральних ознак. Завдання виявлення аномалій у спектральних коефіцієнтах формалізовано як пошук у невпорядкованій множині, що дозволяє ефективно застосовувати квадратичне прискорення, притаманне алгоритму Ґровера [5]. Прототип квантового алгоритму реалізовано у середовищах IBM Qiskit та Google Cirq [6], а результати його роботи порівняно з класичними методами для оцінки точності, швидкості та масштабованості [3]. Запропонований підхід до квантового стегоаналізу, який дозволяє прискорити процес пошуку аномальних спектральних ознак у великих аудіо-базах та підвищує точність виявлення прихованої інформації порівняно з класичними методами [1]. Дослідження включає систематичний аналіз сучасних методів аудіо-стеганографії та оцінку їхніх слабких місць [2], а також критичний огляд класичних підходів стегоаналізу, що визначає, де квантові алгоритми можуть забезпечити найбільший приріст ефективності [4]. Розроблена концепція включає побудову оракула для алгоритму Ґровера, який “мітить” аномальні спектральні ознаки, та тестування прототипу на контрольованих наборах даних [3, 4]. Використання квантових алгоритмів забезпечує підвищену швидкодію і масштабованість процесу, що особливо важливо при аналізі великих масивів мультимедійних даних. Запропонований підхід відкриває перспективи практичного використання у системах захисту даних.

Список літератури

1. Маркус С. Ґровер і алгоритми квантового пошуку / пер. з англ. І. Петренко. – Київ: Наук. думка, 2004. – 256 с.

2. Chen M., Li H. Anomaly Detection in Audio Signals Using Machine Learning // Journal of Audio Engineering. – 2020. – Vol. 15, № 2. – P. 45-60.

3. О’Грейді К., Кемпбелл Л. Deep Learning for Audio Steganalysis: Toward Robust Detection // IEEE Transactions on Information Forensics and Security. – 2021. – Vol. 16, № 5. – P. 1234-1248.

4. Grover L. K. A fast quantum mechanical algorithm for database search // Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC).– Philadelphia, 1996. – P. 212-219.

ВПЛИВ BSI НА ЄВРОПЕЙСЬКУ СТРАТЕГІЮ ПОСТКВАНТОВОЇ КРИПТОГРАФІЇ

Мельникова О.А., Грасмік С.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Розвиток квантових обчислень є загрозою для сучасних криптографічних механізмів, що ґрунтуються на складності факторизації або обчислення дискретного логарифму. Квантові комп'ютери мають потенціал виконувати обчислення, які є практично недосяжними для класичних систем. Наприклад, алгоритм Шора за поліноміальний час факторизує великі числа або знаходить дискретний логарифм [1, 2]. Це потенційна вразливість для багатьох криптографічних алгоритмів — зокрема, для RSA та ECC, які використовуються у цифрових підписах, сертифікатах і протоколах безпеки TLS. Саме через це BSI (Федеральне відомство з безпеки інформаційних технологій Німеччини) визначає одним із пріоритетів розроблення та впровадження стандартів постквантової безпеки [3].

Метою доповіді є узагальнення підходів BSI щодо забезпечення постквантової стійкості інформаційних систем та аналіз впливу BSI на європейську політику стандартизації криптографії. **В доповіді** розглянуто особливості переходу від класичних до постквантових криптографічних рішень, визначені в сучасних технічних настановах і рекомендаціях BSI. Зокрема, в оновлених німецьких вимогах до криптографічних засобів запропоновано поетапне виведення з використання класичних алгоритмів (RSA, DSA, ECC) та впровадження квантово-стійких систем на основі решіткових перетворень, наприклад, FrodoKEM, Classic McEliece, ML-KEM (Kyber) і SPHINCS+ [1, 2]. Ці алгоритми були оцінені за показниками швидкодії, використання пам'яті та сумісності з чинними протоколами, що дає змогу забезпечити безпечний перехід до постквантових рішень без радикальної перебудови IT-інфраструктури. Впровадження цих алгоритмів забезпечує необхідний рівень безпеки для довготривалого збереження конфіденційних даних і сумісність із чинними протоколами безпеки. Основою для вибору цих алгоритмів є результати наукових досліджень, проведених для BSI у рамках проєкту [4], де обґрунтовано доцільність використання решіткових криптосистем як базових постквантових рішень.

Окрім решіткових криптосистем, BSI також розглядає кодові (code-based) та гібридні підходи як потенційно надійні варіанти для окремих сценаріїв застосування. Як зазначено в документі [2] (криптографічні методи: рекомендації та довжини ключів), жоден окремий алгоритм не є універсальним для всіх типів даних чи середовищ, тому рекомендується підтримувати кілька альтернативних постквантових рішень. Такий підхід підвищує стійкість національної інфраструктури до майбутніх технологічних ризиків і забезпечує гнучкість під час переходу до нових стандартів безпеки.

BSI особливо наголошує на принципі криптографічної гнучкості (crypto-agility) — здатності інформаційних систем швидко змінюватися відповідно до

нових криптографічних стандартів. Такий підхід дає змогу поєднувати класичні та постквантові механізми на перехідному етапі, зокрема у формі гібридних криптографічних систем. У них поєднуються класичні та постквантові підписи (наприклад, ECDSA зі SPHINCS+ або XMSS), що забезпечує перевірку достовірності даних двома незалежними алгоритмами та підвищує загальну стійкість системи на час перехідного періоду [1].

У межах європейської співпраці BSI активно бере участь у розробці спільних рішень щодо переходу до постквантової криптографії. Зокрема, німецькі рекомендації лягли в основу спільної позиції органів кібербезпеки ЄС [5], які координують впровадження нових стандартів після завершення процесу стандартизації постквантових алгоритмів, ініційованого NIST. Такий підхід забезпечує узгодженість національних стратегій і сприяє створенню єдиної безпекової інфраструктури в європейському цифровому просторі. BSI також проводить практичні тестування/оцінювання алгоритмів у середовищах із обмеженими ресурсами, зокрема для застосування в IoT-пристроях [2]. Їх результати підтвердили, що алгоритми Kyber і SPHINCS+ можуть ефективно працювати навіть на малопотужних вбудованих системах, що важливо для інтеграції в інфраструктуру “розумних” пристроїв.

Дослідження за підтримки BSI щодо ринку криптографії та квантових обчислень [6] свідчать: більшість німецьких підприємств вже відчувають потребу переходу на квантово-стійкі рішення, але впровадження поступове через високу складність міграції наявних систем.

Таким чином, діяльність BSI визначає як національний, так і європейський напрямок розвитку постквантової криптографії. Поєднання нормативного, технічного та практичного підходів дає можливість створювати цілісну стратегію переходу до нової моделі інформаційної безпеки в умовах квантових технологій.

Список літератури

1. Bundesamt für Sicherheit in der Informationstechnik. *Post-Quanten-Kryptografie. Handlungsempfehlungen des BSI.* — Bonn: BSI, 2020.

2. Bundesamt für Sicherheit in der Informationstechnik. *Kryptographische Verfahren: Empfehlungen und Schlüssellängen* (BSI TR-02102-1, Version 2025-01). — Bonn: BSI, 2025.

3. Bundesamt für Sicherheit in der Informationstechnik. *Kryptografie quantensicher gestalten.* — Bonn: BSI, 2023.

4. Buchmann J., Dahmen E., Hülsing A. *Gitterbasierte Verfahren.* — Darmstadt: TU Darmstadt, 2017. — (BSI-Studie).

5. European PQC Partnership. *Joint Statement on the Transition to Post-Quantum Cryptography.* — 2025. — URL: https://pqcpartnership.eu/joint-statement (дата звернення: 15.10.2025).

6. KPMG & Bundesamt für Sicherheit in der Informationstechnik. *Marktumfrage Kryptografie und Quantencomputing.* — Berlin: KPMG, 2023.

АНАЛІЗ ЗАХИЩЕНОСТІ END-TO-END ШИФРУВАННЯ АУДІО ТА ВІДЕО-ВИКЛИКІВ У СУЧАСНИХ МЕСЕНДЖЕРАХ

Мельникова О.А., Гузенко Н.В.
Харківський національний університет радіоелектроніки, Харків, Україна

У наш час існує багато месенджерів, які надають користувачам можливість спілкуватися у текстовому, відео або аудіо-форматі. Вони стали невід'ємною частиною нашого життя, адже забезпечують легкий обмін інформацією. З розвитком цифрових технологій все більшу актуальність набирають питання безпеки персональних даних та захищеності переданих повідомлень.

Метою доповіді є аналіз сучасних месенджерів щодо забезпечення безпеки під час аудіо та відео-викликів. У доповіді розглянуто реалізації end-to-end шифрування в різних месенджерах, що дає змогу проаналізувати їх захищеність. Були проаналізовані такі месенджери: Telegram, Signal, WhatsApp, Facebook Messenger та Viber.

В одному з найпопулярніших месенджерів, Telegram, end-to-end шифрування реалізовано лише для секретних чатів. Звичайні чати, групи та канали використовують шифрування типу "клієнт–сервер", тобто Telegram має доступ до всієї інформації з цих чатів. Секретні чати Telegram створюються лише між двома пристроями й доступні лише у мобільній версії застосунку. Дані для таких чатів, зокрема всі повідомлення, зберігаються локально та забезпечують справжнє E2EE (end-to-end encryption) на основі протоколу MTProto 2.0 [1].

Для всіх дзвінків, навіть у звичайних чатах, Telegram використовує E2EE шифрування [2]. Протокол MTProto 2.0, на якому базується Telegram, застосовує алгоритм Діффі-Геллмана для розподілу ключів, AES-256 для симетричного шифрування, RSA-2048 для ініціалізації обміну ключами та SHA-256 для ґешування.

Signal не є одним із найпопулярніших месенджерів, проте у всіх його чатах, дзвінках і викликах використовується end-to-end шифрування. Реалізацію його протоколу опубліковано на GitHub, тобто будь-який користувач може отримати доступ до повного вихідного коду, наприклад, для аудиту. Signal використовує дволанцюговий алгоритм шифрування, у якому кожне повідомлення має власний ключ. Це означає, що при розкритті одного ключа інші залишаються повністю захищеними. Для додаткового захисту та анонімності Signal приховує частину метаданих, зокрема інформацію про відправника, щоб навіть сервер не міг визначити, хто є ініціатором повідомлення або виклику. Для обміну ключами Signal застосовує алгоритм Extended Triple Diffie-Hellman [3], який дозволяє створювати сеанси навіть тоді, коли отримувач перебуває офлайн. Для шифрування повідомлень використовується AES-256-CBC, для ґешування – SHA-256, а для підпису – EdDSA. WhatsApp використовує Signal Protocol [4] для забезпечення end-to-end шифрування у всіх чатах, а також аудіо та відео-викликах. За заявою

компанії, всі ключі шифрування зберігаються лише на пристроях користувачів. Водночас WhatsApp збирає метадані та передає їх компанії Meta. Під час ініціалізації чату, якщо отримувач перебуває офлайн, WhatsApp використовує prekeys — одноразові ключі, що зберігаються на сервері та призначені для встановлення сесії, коли інша сторона знову з'явиться онлайн. Для шифрування повідомлень використовується AES-256, для ґешування — SHA-256.

Наступний популярний месенджер — Facebook Messenger, який також належить компанії Meta, використовує за основу Signal Protocol (протокол, розроблений Signal). Однак end-to-end шифрування, на відміну від Signal та WhatsApp, за замовчуванням вимкнене, хоча доступне у секретних чатах — подібно до Telegram. Для шифрування повідомлень застосовується [5] AES-256 у режимі CTR, SHA-256 для ґешування та EdDSA для підпису. Додатково він використовує Labyrinth Protocol для синхронізації E2EE між пристроями та вдосконалює механізм перевірки пристроїв.

Viber з 2016 року підтримує end-to-end шифрування у приватних і групових чатах, а також у дзвінках. Але застосовує власний протокол, принципи якого були оприлюднені. Viber збирає метадані про користувача та його пристрій, однак усі ключі шифрування зберігаються на пристроях користувачів. Сервіс використовує [6] алгоритм Діффі-Геллмана для розподілу ключів, AES-256-CFB для шифрування, SHA-256 для ґешування та EdDSA для підпису.

На основі проведеного аналізу сформовано критерії для порівняння з метою підвищення рівня безпеки. Отримані результати показують, що більшість сучасних месенджерів впроваджують достатньо надійні механізми захисту, але деякі месенджери обмежують E2EE шифрування, наприклад, для використання лише у захищених чатах. Загалом можна стверджувати, що EE2E шифрування поступово стає стандартом у сфері цифрових комунікацій та забезпечує захист приватного спілкування від несанкціонованого доступу.

Список літератури

1. MTProto. URL: https://core.telegram.org/mtproto (дата звернення 15.10.2025).
2. Security Analysis of End-to-End Encryption in Telegram. URL: https://caislab.kaist.ac.kr/publication/paper_files/2017/SCIS17_JU.pdf (дата звернення 15.10.2025).
3. The Double Ratchet Algorithm. URL: https://signal.org/docs/specifications/doubleratchet/ (дата звернення: 15.10.2025).
4. Prekey Pogo: Investigating Security and Privacy Issues in WhatsApp's Handshake Mechanismю URL: https://arxiv.org/pdf/2504.07323 (дата звернення 15.10.2025).
5. Messenger End-to-End Encryption Overview. URL: https://engineering.fb.com/wp-content/uploads/2023/12/MessengerEnd-to-EndEncryptionOverview_12-6-2023.pdf (дата звернення: 15.10.2025).
6. Viber Encryption Overview. URL: https://www.viber.com/app/uploads/viber-encryption-overview.pdf (дата звернення 15.10.2025).

КІЛЬЦЕВІ ПІДПИСИ У БЛОКЧЕЙН СИСТЕМАХ НА ОСНОВІ НЕКОМУТАТИВНИХ ГРУП

Фроленко В.О.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасних блокчейн системах питання забезпечення анонімності, цілісності та стійкості до квантових атак є одним з ключових напрямів розвитку криптографії. Традиційні методи цифрових підписів ґрунтуються на комутативних групах (RSA, ECDSA), які можуть бути вразливими до квантових алгоритмів. Одним із перспективних підходів є використання кільцевих підписів на основі некомутативних груп [1, 2], що відкриває нові можливості для реалізації постквантової безпеки у блокчейн-технологіях.

Метою доповіді є теоретичне обґрунтування моделі кільцевого підпису для блокчейн систем на основі некомутативних груп, що забезпечує анонімність підписанта та стійкість до квантових атак.

У зв'язку з інтенсивним розвитком квантових обчислень, виникає потреба у нових криптографічних механізмах, здатних протистояти квантовим атакам. На відміну від традиційних схем кільцевого підпису, що базуються на задачах дискретного логарифма або факторизації (у комутативних групах), дана модель використовує некомутативні структури, серед яких: групи кіс (braid groups), групи матриць над кільцями з невзаємозамінними елементами, або групи перетворень із некомутативними операціями. Кожна з них характеризується високим ступенем обчислювальної складності при виконанні операцій знаходження зворотного елементу, що є основою для побудови стійких криптографічних примітивів. Застосування цих структур у схемах кільцевого підпису забезпечує формування криптографічних систем нового покоління, здатних забезпечити постквантову стійкість, анонімність учасників і захист від криптоаналітичного розкриття навіть у разі появи потужних квантових обчислювальних засобів [3].

Основна ідея схеми полягає у забезпеченні можливості одному з учасників групи підписати повідомлення таким чином, щоб інші могли перевірити його достовірність, але не могли визначити, хто саме з учасників створив підпис. У запропонованій моделі, побудованій на некомутативних групах, кожен учасник володіє відкритим ключем, що формується на основі його секретного ключа та фіксованого елемента групи. Сукупність усіх відкритих ключів утворює «кільце» потенційних підписантів.

Учасник, що здійснює підписання, використовуючи свій секретний ключ, генерує підпис за допомогою комбінацій некомутативних операцій над елементами групи.

Перевірка підпису здійснюється через спільну перевірку групових співвідношень, без розкриття інформації про те, який саме ключ було використано [3]. Такий підхід гарантує анонімність підписанта, цілісність

повідомлення та незаперечність факту підпису від імені будь-якого члена кільця. На відміну від еліптичних кривих або RSA, задачі на некомутативних групах (зокрема спряження чи декомпозиції) не мають відомих ефективних квантових алгоритмів для їх розв'язання. Це робить модель перспективною в умовах появи квантових обчислень.

Через властивість некомутативності операцій результати навіть близьких ключів у групі виглядають статистично незалежними. Це знижує ризик атак деанонімізації у блокчейн-мережах. Модель може бути вбудована в механізми анонімних транзакцій або доказів знань без розкриття.

Використання некомутативних структур забезпечує високий рівень криптографічної ентропії та захист від квантового криптоаналізу, що робить таку модель придатною для інтеграції у децентралізовані блокчейн-мережі.

Реалізація кільцевих підписів на некомутативних групах може бути використана для побудови анонімних транзакцій, приватних голосувань або конфіденційних смартконтрактів у децентралізованих мережах.

Запропонована модель кільцевого підпису на основі некомутативних груп розглядається як перспективний напрям розвитку постквантової блокчейн-криптографії [4, 5]. Її доцільність полягає у здатності забезпечувати квантову стійкість криптографічних механізмів, підвищувати рівень анонімності транзакцій, зменшувати ризик криптоаналітичного розкриття підписів, а також у можливості інтеграції в сучасні блокчейн-платформи без необхідності суттєвих структурних змін.

Список літератури

5. Kotukh, Y., Khalimov, G., & Dzhura, I. (2025). Cryptographic competitiveness of cryptosystems based on noncommutative groups. Radiotekhnika, (221), 72–82. https://doi.org/10.30837/rt.2025.2.221.10

6. Kotukh, E., Severinov, O., Vlasov, A., Kozina, L., Tenytska, A., & Zarudna , E. (2021). Methods of construction and properties of logariphmic signatures. Radiotekhnika, 2(205), 94–99. https://doi.org/10.30837/rt.2021.2.205.09

7. Easttom, C. (2022). Quantum computing and cryptography. In Modern Cryptography: Applied Mathematics for Encryption and Information Security (pp. 397-407). Cham: Springer International Publishing.

8. Поддубний В.О., Гвоздьов Р.Ю., Сєвєрінов О.В. Методи електронного підпису на основі некомутативних груп // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: 12-та міжнародна науково-технічна конференція, 27-28 квітня 2022 р. – Баку – Харків – Жиліна, 2022. - Т. 1, С. 149.

9. G.Khalimov, Y.Kotukh, S.Khalimova, O.Sievierinov, A.Vlasov. "Towards advance encryption based on a Generalized Suzuki 2-groups". International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME) 2021.

10. G.Khalimov, Y.Kotukh, I.Didmanidze, O.Sievierinov. "Towards three-parameter group encryption scheme for MST3 cryptosystem improvement". Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4) 2021.

MITM-АТАКИ ТА ЇХ ВИЯВЛЕННЯ ЗАСОБАМИ SECURITY OPERATIONS CENTER (SOC)

Федюшин О.І., Федосенко А.М.
Харківський національний університет радіоелектроніки, Харків, Україна
Сухотеплий В.М.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба, Харків, Україна

В епоху тотальної цифровізації, коли особисті та корпоративні дані стали найціннішим активом, питання захисту інформації від несанкціонованого доступу набуває вищого рівня. Кожна людина повинна критично оцінювати ситуації, коли її просять надати конфіденційні дані, і бути впевненою, що взаємодіє з легітимною системою, а не зі зловмисником.

Саме тому виникає гостра необхідність у потужних, централізованих системах моніторингу, здатних виявляти приховані атаки на рівні мережевого трафіку та аномалій у поведінці систем. Це і визначає критичну роль Security Operations Center (SOC) [1, 2], який виступає як технологічний захист, що аналізує потоки даних і виявляє ознаки компрометації, непомітні для звичайного користувача. Дослідження методів виявлення MITM-атак [3] засобами SOC є не просто актуальним, а життєво необхідним для побудови надійної системи кіберзахисту в сучасних умовах. Традиційно модель SOC є централізованою, всі ресурси та персонал розташовані в одному місці, що забезпечує фізичний захист даних та оптимізоване управління. Однак сучасні SOC також можуть бути розподілені між географічно розрізненими локаціями, що забезпечує глобальне розповсюдження ресурсів та цілодобовий аналіз загроз безпеки в режимі реального часу. SOC служать центральним вузлом для оцінки ситуації з безпекою в режимі реального часу, а їх основні функції включають постійний моніторинг, виявлення загроз, аналіз інцидентів та скоординовану реакцію на події, пов'язані з безпекою. Вони отримують різноманітні дані, інформацію та розвіддані, які надходять до сховища, яке використовується аналітиками для інтерпретації, кореляції, відображення, зберігання, архівування та прийняття рішень. Ключова роль у протидії загрозам MITM належить Security Operations Center. Як показав аналіз, SOC є не просто набором інструментів, а цілісним процесом, що поєднує технології та експертизу. За допомогою таких інструментів, як SIEM та IDS/IPS аналітики можуть ідентифікувати аномалії, що свідчать про MITM-атаку.

Список літератури

1.What is a security operations center (SOC)? [Електронний ресурс] / Режим доступу: https://www.ibm.com/think/topics/security-operations-center.

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

3. What is a Man-in-the-Middle Attack (MitM)? Definition and Prevention. [Електронний ресурс] / Режим доступу: https://jetpack.com/blog/what-is-a-man-in-the-middle-attack/.

ЗАБЕЗПЕЧЕННЯ ПРИНЦИПУ НАЙМЕНШИХ ПРИВІЛЕЇВ У ДИНАМІЧНИХ ХМАРНИХ СЕРЕДОВИЩАХ

Федюшин О.І., Ткачук І.К.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасних хмарних інфраструктурах принцип найменших привілеїв є одним із фундаментальних принципів кібербезпеки. Постійне масштабування мікросервісних архітектур, автоматизоване розгортання компонентів і динамічне призначення доступів формують складну систему керування правами, де надлишкові дозволи стають джерелом потенційних атак. Недотримання цього принципу створює ризики ескалації привілеїв, компрометації облікових даних і несанкціонованого доступу до критичних ресурсів. Статичні політики доступу в умовах динамічного середовища не здатні своєчасно відображати реальні потреби сервісів.

Проблематика забезпечення мінімально необхідних дозволів полягає у визначенні реального обсягу прав, необхідних кожному суб'єкту для виконання своїх функцій [1]. Поведінка мікросервісів змінюється залежно від контексту виконання, тому статичні правила швидко втрачають актуальність. Одним із ефективних підходів є поведінковий аналіз активності компонентів системи – це впровадження процесу відстеження запитів до ресурсів, порівняння їх із діючими політиками та виявлення надлишкових привілеїв. Такий підхід дозволяє автоматично оптимізувати політики доступу та підтримувати їх у відповідності до реального використання.

Додатково ефективність підвищують моделі контекстно-залежного контролю доступу, які враховують середовище виконання, часові параметри, рівень довіри до суб'єкта та тип взаємодії між компонентами системи. Такі моделі дозволяють коригувати дозволи відповідно до поточного стану системи, наприклад, зменшувати обсяг привілеїв під час зниження рівня довіри або при виявленні аномальної активності. Інтеграція поведінкового аналізу з контекстними механізмами створює основу для самоналаштовного управління доступами, що забезпечує баланс між безпекою, гнучкістю та безперервністю роботи мікросервісної інфраструктури [2].

Метою доповіді є представлення підходів до реалізації принципу найменших привілеїв у динамічних хмарних середовищах шляхом поведінкового аналізу та адаптивного оновлення політик доступу. Це сприяє зменшенню поверхні атак, підвищенню стійкості інфраструктури й формуванню автоматизованих систем захисту сучасних хмарних сервісів.

Список літератури

1. Least Privilege and More [Електронний ресурс] / Режим доступу: https://www.cs.cornell.edu/fbs/publications/leastPrivNeedham.pdf

2. A Systematic Review of Identity and Access Management Requirements in Enterprises and Potential Contributions of Self-Sovereign Identity [Електронний ресурс] / Режим доступу: https://link.springer.com/article/10.1007/s12599-023-00830-x

ЗАХИЩЕНИЙ МЕСЕНДЖЕР ІЗ ЛОКАЛЬНИМ ЗБЕРІГАННЯМ КРИПТОГРАФІЧНИХ КЛЮЧІВ НА КЛІЄНТСЬКОМУ ПРИСТРОЇ

Федюшин О.І., Корсун А.Д.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасних комунікаційних системах безпека даних значною мірою залежить не лише від алгоритмів шифрування, а насамперед від способу зберігання та керування криптографічними ключами. Більшість популярних месенджерів покладаються на серверну інфраструктуру для управління ключами, що створює ризики компрометації через витік даних, зловмисний доступ або помилки конфігурації. Проблема централізованого зберігання ключів є одним із ключових викликів у сфері захисту інформації.

Метою даної роботи є розроблення архітектури підсистеми локального зберігання криптографічних ключів у межах захищеного месенджера, де ключі користувача ніколи не покидають меж клієнтського пристрою. Запропонований підхід використовує вбудовані системні сховища: Windows DPAPI, macOS Keychain, Android Keystore та Linux Secret Service – для створення уніфікованого інтерфейсу керування ключами (Key Storage API) [1, 2]. **Предметом дослідження** є архітектура, алгоритми і засоби захисту локального зберігання ключів у клієнтських застосунках, а об'єктом – процеси безпечного управління криптографічними ключами у середовищах користувацьких пристроїв. У роботі проведено дослідження механізмів апаратно-захищеного зберігання, алгоритмів zeroization, шифрування резервних копій ключів із використанням PBKDF2 та Argon2id, а також методів ізоляції ключового матеріалу від додатків і процесів операційної системи. Розроблений модуль інтегровано у клієнтський застосунок на базі Electron/React, що забезпечує взаємодію з бекендом (Spring Boot, PostgreSQL, WebSocket) без передачі ключів через мережу. Проведено статичний і динамічний аналіз безпеки (SAST, DAST) та ручне пентестування, які підтвердили надійність реалізації і відсутність витоків секретного матеріалу під час роботи програми. Отримані результати можуть бути використані для створення систем безпечного зберігання криптографічних даних у застосунках нового покоління, що дотримуються принципу «Zero Trust», коли користувач повністю контролює свої ключі та доступ до них [3].

Список літератури

1. Marlinspike M., Perrin T. The Signal Protocol (X3DH and Double Ratchet) Technical Overview. – Open Whisper Systems, 2016.

2. NIST SP 800-57. Recommendation for Key Management. – Part 1: General. – National Institute of Standards and Technology, 2020.

3. Moskvin, K., & Sievierinov, O. (2025). Zero Trust Architecture in Corporate Cybersecurity Systems // Computer and Information Systems and Technologies Kharkiv, September 2024. P. - 54-55.

АРХІТЕКТУРА ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ХМАРНОГО МЕНЕДЖЕРА ПАРОЛІВ ІЗ НАСКРІЗНИМ ШИФРУВАННЯМ

Федюшин О.І., Міллер К.З.
Харківський національний університет радіоелектроніки, Харків, Україна

Швидке зростання кількості веб-сервісів та хмарних платформ призводить до використання користувачами десятків паролів. На практиці це часто завершується використанням слабких або повторюваних даних, що значно підвищує ризик компрометації облікових записів. Хмарні менеджери паролів дозволяють централізовано зберігати та синхронізувати облікові дані між пристроями, проте у традиційних рішеннях питання безпеки часто обмежуються лише використанням TLS-шифрування каналу та базовим хешуванням паролів на сервері. Компрометація серверної інфраструктури або внутрішні зловмисники в таких моделях можуть призвести до витоку конфіденційної інформації. Одним із сучасних підходів до мінімізації довіри до сервера є застосування концепції наскрізного шифрування (end-to-end encryption, E2EE). У цій моделі всі критично важливі криптографічні операції виконуються виключно на стороні клієнта, а на сервер передаються та зберігаються лише зашифровані дані. Сервер виступає транспортним рівнем та сховищем і не має доступу до відкритого вмісту сховища паролів. Додатково використовується принцип «zero-knowledge»: постачальник сервісу не володіє інформацією, яка дозволила б відновити ключі шифрування користувача.

Метою доповіді є розробка та дослідження архітектури безпечного хмарного менеджера паролів із наскрізним шифруванням та автентифікацією користувача, у якому серверна частина не має доступу до відкритих облікових даних, а компрометація сервера не призводить до розкриття вмісту сховища. Для досягнення цієї мети запропоновано поєднання криптографічних механізмів на стороні клієнта з захищеною серверною інфраструктурою, яка відповідає за автентифікацію, авторизацію та синхронізацію. **Об'єктом дослідження** є процес зберігання та синхронізації облікових даних користувачів у хмарному середовищі. **Предметом дослідження** є методи організації наскрізного шифрування, керування ключами та автентифікації користувача в архітектурі хмарного менеджера паролів [1]. У запропонованій архітектурі користувацькі секрети (логіни, паролі, нотатки, дані двофакторної автентифікації) [2] зберігаються у вигляді зашифрованого сховища, ключ до якого генерується локально з майстер-пароля. Для формування криптографічних ключів використовується стійка функція похідних від пароля, наприклад Argon2id або PBKDF2 з індивідуальною сіллю та високою обчислювальною складністю. Отриманий ключ розділяється на принаймні два логічні компоненти: ключ шифрування сховища та ключ автентифікації, що знижує ризики у разі часткової компрометації.

Для симетричного шифрування вмісту сховища доцільно застосовувати сучасні режими автентифікованого шифрування, такі як AES-GCM [3], які

одночасно забезпечують конфіденційність і цілісність даних. Кожен запис у сховищі має власний унікальний вектор ініціалізації (IV/nonce), а метадані (мітки часу, тип запису, ідентифікатор запису) включаються до додаткових автентифікованих даних (AAD). Це ускладнює маніпуляції з зашифрованим вмістом без знання ключа.

Автентифікація користувача на сервері відділяється від механізму шифрування сховища. Додатково може використовуватися двофакторна автентифікація, що зменшує ризик захоплення облікового запису при витоку пароля [4, 5]. Серверна частина реалізує REST- або GraphQL-API для роботи з зашифрованими сховищами, а також механізм черги змін для синхронізації між кількома пристроями.

У роботі проведено формалізацію моделі загроз для хмарного менеджера паролів та аналіз основних сценаріїв атак: компрометація серверної БД, пасивне перехоплення трафіку, атаки грубої сили на майстер-пароль, спроби підміни клієнтського застосунку. Показано, що у разі компрометації серверного сховища зловмисник отримує доступ лише до зашифрованих даних; їхнє успішне розшифрування потребує підбору майстер-пароля з урахуванням параметрів KDF, що при правильному виборі параметрів робить атаку економічно невигідною. На основі запропонованої архітектури розроблено прототип хмарного менеджера паролів, у якому криптографічні операції на клієнті реалізовано із застосуванням стандартних засобів платформи, а серверна частина побудована як веб-служба з використанням сучасного фреймворку та реляційної бази даних. Проведені експериментальні дослідження показали, що вибрані параметри KDF забезпечують прийнятний час обробки на користувацьких пристроях при значному підвищенні стійкості до атак перебору. Отримані результати демонструють, що застосування наскрізного шифрування, розділення ключів та посилених механізмів автентифікації дозволяє суттєво підвищити рівень безпеки хмарних менеджерів паролів без критичного погіршення зручності користування. Подальші дослідження можуть бути спрямовані на інтеграцію апаратних модулів безпеки, побудову формальних доказів стійкості окремих компонентів системи та впровадження додаткових механізмів захисту від фішингових атак і компрометації клієнтських пристроїв.

Список літератури

1. Bonneau J., Herley C., Van Oorschot P., Stajano F. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes // 2012 IEEE Symposium on Security and Privacy. – 2012. – P. 553–567.

2. Biryukov A., Dinu D., Khovratovich D. Argon2: The Memory-Hard Function for Password Hashing and Other Applications // Proc. of IEEE EuroS&P. – 2016. – P. 289–302.

3. Dworkin M. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. NIST Special Publication 800-38D. – 2007.

4. Grassi P. et al. Digital Identity Guidelines. NIST Special Publication 800-63B. – 2017.

5. FIDO Alliance. FIDO2: Client to Authenticator Protocol (CTAP) and Web Authentication (WebAuthn). Technical Specifications. – 2019.

МОДЕЛЮВАННЯ ВПЛИВУ ІНТЕГРАЦІЇ THREAT INTELLIGENCE НА ТОЧНІСТЬ ВИЯВЛЕННЯ АТАК У SOC-СЕРЕДОВИЩІ

Федюшин О.І., Вербицький А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасних умовах постійно зростаючої кількості кіберзагроз і складності атак ефективна діяльність Центрів оперативного реагування на інциденти безпеки (SOC) неможлива без використання систем Threat Intelligence (TI). Розвідка кіберзагроз виступає стратегічним компонентом кіберзахисту, який забезпечує не лише виявлення відомих індикаторів компрометації (IoC), але й формування контексту, необхідного для глибокого розуміння тактик, технік і процедур зловмисників (TTP) [1, 2].

Важливу роль відіграють також комерційні постачальники TI-фідів, які формують високоякісну, перевірену інформацію про актуальні загрози. Серед них виділяються Mandiant, Recorded Future, CrowdStrike Falcon Intelligence і Flashpoint. Ці сервіси надають глибокі аналітичні звіти про діяльність APT-груп, досліджують темні сегменти мережі (Dark Web), виявляють нові індикатори атак і забезпечують прогнозування ризиків. Отримані дані дозволяють SOC не лише реагувати на відомі інциденти, але й передбачати майбутні сценарії атак, що є важливим кроком у побудові адаптивної оборони.

Не менш значущою є роль інтегрованих сервісів і фреймворків, які підтримують застосування TI у повсякденних процесах SOC. Зокрема, MITRE ATT&CK Framework забезпечує методологічну основу для класифікації дій зловмисників і моделювання атак, допомагаючи аналітикам співвідносити реальні інциденти з відомими техніками. SIEM-системи, такі як Splunk чи Microsoft Sentinel, завдяки підтримці форматів STIX/TAXII, автоматично збагачують журнали подій TI-даними, що підвищує точність кореляції та зменшує кількість хибних спрацьовувань [3]. Крім того, сучасні EDR/XDR-рішення використовують TI для автоматичного пошуку загроз (Threat Hunting) у реальному часі, дозволяючи виявляти компрометації на ранніх етапах.

Отже, використання TI у діяльності SOC стає ключовим чинником підвищення ефективності кіберзахисту. Це дозволяє не лише виявляти відомі загрози, але й передбачати нові, забезпечуючи комплексну ситуаційну обізнаність і стійкість інформаційної інфраструктури до сучасних кібератак.

Список літератури

1. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). Information and cyber security of the enterprise. Textbook. Lviv: Publisher Marchenko T. V.

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

3. Li, X., Wang, Z., Leung, V. C. M., Ji, H., Liu, Y., & Zhang, H. (2021). Blockchain-empowered data-driven networks. ACM Computing Surveys, 54(3), 1-38.

ОЦІНКА ЕФЕКТИВНОСТІ СТЕГАНОАНАЛІЗУ НА ОСНОВІ 2D-ЗОБРАЖЕНЬ АУДІО

Федюшин О.І., Безсонов М.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Метод найменш значущого біта (LSB) залишається найпростішим і найпоширенішим способом приховування даних у зображеннях. Водночас його практичне застосування різко обмежується крихкістю до будь-яких змін контейнера: стискання з втратами (JPEG/WebP), масштабування, фільтрація та інші дії призводять до суттєвої або повної втрати прихованої інформації; додатково LSB легко детектується статистичними тестами, має низьку місткість і не забезпечує належної безпеки без криптозахисту [1, 2].

Саме ця крихкість LSB та подібних простих методів змушує зловмисників переходити до значно складніших, адаптивних та робастних алгоритмів (наприклад, у частотній області), які здатні витримувати стиснення та обробку. Це, у свою чергу, створює гостру проблему для кібербезпеки: класичні статистичні детектори виявляються безсилими проти таких загроз. Таким чином, розробка нових методів виявлення, здатних ідентифікувати навіть найсучасніші техніки приховування, є надзвичайно актуальною задачею.

Метою доповіді є оцінка ефективності **методів стеганоаналізу аудіо-повідомлень** у 2D-представленнях та виявлення факту приховування даних за різних типів вбудовування та постобробки контейнера.

У роботі досліджується застосування 2D-представлень аудіосигналів (STFT-спектрограма, мел-спектрограма, CQT) та глибинних моделей зору (CNN/ViT) для стеганоаналізу зображень, що містять проєкції аудіо.

Запропоновано узагальнений підхід до виявлення прихованих повідомлень із підвищеною стійкістю до постобробки (стиснення, масштабування, фільтрація) та обґрунтовано інформативність різних 2D-перетворень для виявлення «мікрошрамів» вбудовування [3].

Використання ResNet/EfficientNet/Vision Transformer (через transfer learning з ImageNet) дозволяє виявляти «мікрошрами» стеганографії у зображеннях значно надійніше, ніж ручні ознаки. Вибір оптимального 2D-представлення для конкретних класів приховування (LSB, частотні методи, методи у стиснених форматах) є відкритим дослідницьким питанням.

Список літератури

1. Mustafa Sabah. Combination of Steganography and Cryptography. URL:https://iopscience.iop.org/article/10.1088/1757-899X/518/5/052003/pdf.

2. Поддубний, В., & Сєвєрінов, О. (2025). Дослідження ефективності алгоритмів оброблення зображень у схемах нульового водяного знака. Сучасний стан наукових досліджень та технологій в промисловості, (1 (31)), 102-114.

3. Kodlubovskyi D. Data hiding in images using combined steganography and cryptography. URL: http://journals.dut.edu.ua/index.php/dataprotect/article/view/688.

РОЗРОБКА ЗАХИСНИХ МЕХАНІЗМІВ XDR ЧЕРЕЗ ПРАКТИЧНІ СЦЕНАРІЇ ПЕНТЕСТІВ ТА МОДЕЛЮВАННЯ АТАК

Топіха Т.Б., Смірнов А.О., Городецький С.Л.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасних умовах стрімкої цифровізації бізнес-процесів, державного управління та критичних інфраструктур питання забезпечення кібербезпеки набуває стратегічного значення. Кожного року зростає кількість інцидентів, спричинених не лише типовими вірусами чи шкідливими вкладеннями, а й складними багатоступеневими атаками, які використовують соціотехнічні методи, викрадення облікових даних, горизонтальне переміщення в мережі та ексфільтрацію конфіденційної інформації. За даними звітів IBM X-Force Threat Intelligence та Verizon DBIR (2024 р.) [1, 2], понад половину виявлених інцидентів відносяться саме до багатокрокових атак, які важко виявити традиційними засобами [3]. У таких умовах центри операцій безпеки (SOC) змушені працювати у режимі постійного навантаження, обробляючи величезну кількість подій і сповіщень. Це, своєю чергою, збільшує ймовірність пропуску критичних загроз та уповільнює реагування на інциденти.

Традиційні засоби захисту системи IDS/IPS, SIEM та EDR безумовно залишаються важливими елементами сучасної кібербезпеки. Вони дозволяють здійснювати моніторинг мережевого трафіку, централізовано збирати логи, аналізувати події на кінцевих точках та формувати базові правила реагування. Проте їхня фрагментарність, різнорідність форматів даних та відсутність контекстної взаємодії між різними джерелами суттєво обмежують можливості комплексного аналізу. Як наслідок, для аналітиків SOC залишається великий обсяг ручної роботи, що збільшує час ухвалення рішень і ризики людського фактору [3]. Вирішенням цих проблем є впровадження інтегрованих систем XDR (Extended Detection and Response), які поєднують телеметрію з різних кінцевих точок, мережі, хмарних сервісів, пошти, ідентичностей у єдину аналітичну екосистему [4]. XDR не лише централізує збір даних, але й забезпечує автоматичну кореляцію подій, створюючи повний контекст інциденту від початкового проникнення до фінальної дії зловмисника. Таким чином, система дозволяє значно скоротити час виявлення, підвищити точність детекцій та автоматизувати ключові етапи реагування.

Метою даного дослідження стало створення лабораторної XDR-платформи, яка дозволяє перевірити ефективність механізмів виявлення та реагування шляхом практичного моделювання атак і пентест-емуляції. У роботі зроблено акцент на практичне підтвердження теоретичних положень, тобто не лише описано архітектуру, а й реалізовано її в умовах контрольованого середовища з подальшим тестуванням.

У межах дослідження було спроєктовано й розгорнуто лабораторну інфраструктуру в середовищі Microsoft Azure, яка максимально наближена до реальної корпоративної екосистеми. До її складу входить публічний веб-сервер (Nginx), внутрішній файловий сервер, поштовий сервіс (Exchange Online),

кілька користувацьких станцій із агентами Defender for Endpoint, а також аналітична платформа Microsoft Sentinel, що виконує функції SIEM/SOAR [5]. Усі джерела телеметрії передавали дані до Log Analytics Workspace, де вони нормалізувались, аналізувались і корелювались за єдиною схемою. Основою методології став фреймворк MITRE ATT&CK, який забезпечив систематизацію тактик і технік супротивників (TTP) та слугував базою для створення сценаріїв моделювання атак [6]. У рамках експериментів реалізовано сценарії початкового доступу через фішинг (T1566), викрадення облікових даних (T1003), горизонтального переміщення (T1021), ескалації привілеїв (T1068) та ексфільтрації даних (T1041).

Для безпечної емуляції поведінки зловмисників використано інструменти які дозволили відтворити реалістичні техніки без ризику для продуктивних систем. Усі події фіксувалися XDR-агентами, передавалися до Sentinel, де автоматично створювалися інциденти з побудовою ланцюгів подій і подальшою активацією сценаріїв реагування (Logic Apps). Реалізовані плейбуки передбачали ізоляцію хостів, блокування користувачів, надсилання повідомлень аналітикам SOC і автоматичне оновлення списків контролю доступу. Результати практичного етапу дослідження підтвердили, що впроваджене XDR-рішення забезпечує більш глибоку видимість подій, швидшу ідентифікацію інцидентів і зниження кількості хибних сповіщень. Автоматизація процесів реагування дала змогу оптимізувати навантаження на аналітиків SOC, підвищити стабільність роботи команди та скоротити час на обробку подій. Також було продемонстровано можливість інтеграції XDR із різними джерелами даних, що створює передумови для масштабування рішення в умовах реального підприємства.

Отримані результати свідчать, що використання підходу XDR у поєднанні з фреймворком MITRE ATT&CK і практичним моделюванням атак є ефективним шляхом підвищення рівня кіберстійкості організацій. Такий підхід не лише покращує якість виявлення загроз, а й забезпечує комплексне бачення безпекових подій, скорочуючи час реагування та зменшуючи залежність від людського чинника. Проведене дослідження підтвердило доцільність упровадження інтегрованих систем XDR як основи сучасної архітектури кіберзахисту.

Список літератури

1. IBM Security. X-Force Threat Intelligence Index 2024. — IBM Corporation, 2024. — 64 p. URL: https://www.ibm.com/reports/threat-intelligence.
2. Verizon Communications Inc. Data Breach Investigations Report 2024. — Verizon, 2024. — 120 p. URL: https://www.verizon.com/business/resources/reports/dbir/.
3. Ушатов, В., Сєвєрінов, О.В. (2019). Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки.
4. Gartner Research. Market Guide for Extended Detection and Response (XDR). — Gartner, 2023. — 22 p.
5. Microsoft Corporation. Microsoft Defender XDR Documentation. — Microsoft Learn, 2024. URL: https://learn.microsoft.com/en-us/defender-xdr/.
6. MITRE Corporation. MITRE ATT&CK Framework. — 2024. URL: https://attack.mitre.org.

МЕТОДИ КВАНТОВОЇ СТЕГАНОГРАФІЇ ЗОБРАЖЕНЬ ТА ЇХ ЗАСТОСУВАННЯ В СИСТЕМАХ ЗАХИСТУ

Головко Є.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні інформаційні системи потребують високого рівня захисту, особливо коли дані передаються відкритими каналами зв'язку. Але традиційні криптографічні підходи не приховують факт існування секретного повідомлення. Поєднання стеганографії з квантовими обчисленнями створює новий рівень безпеки, оскільки квантові стани дозволяють здійснювати операції паралельно, забезпечують високу непомітність і ускладнюють виконання стеганоаналізу [1]. Саме тому виникає необхідність наукового дослідження моделей квантового подання зображень та алгоритмів квантової стеганографії, орієнтованих на ефективне та надійне приховування даних.

Метою доповіді є дослідження моделей квантових зображень та стеганографічних методів на основі LSB, що забезпечують підвищений рівень захищеності інформації.

Квантові комп'ютери відкривають доступ до нових принципів представлення та обробки зображень, що забезпечує значні переваги порівняно з класичними системами. Моделювання зображень у квантових станах дозволяє реалізувати операції над усіма пікселями одночасно, що підвищує ефективність і розширює можливості забезпечення безпеки. Крім того, існуючі класичні стеганографічні методи є дедалі вразливішими до сучасних атак, тоді як квантові стани дозволяють мінімізувати спотворення та ускладнюють виявлення вбудованого повідомлення [2]. Актуальність зумовлена потребою у захищеній передачі зображень у таких сферах, як телемедицина, оборона, супутникова розвідка й системи спостереження, де конфіденційність і непомітність мають вирішальне значення.

Моделі зображень у квантових станах формують основу для побудови стеганографічних алгоритмів. Модель квантової решітки передбачає пряме відображення пікселів у кубіти, що робить її концептуально простою, але практично складною через потребу у великій кількості кубітів. Модель Real Ket базується на багаторівневому поділі зображення та використанні заплутування, що дозволяє виконати стиснення, однак випадковість структури зображення обмежує її ефективність у реальних застосуваннях.

Розвиток моделей призвів до створення FRQI, де координати та інтенсивність зображення зберігаються у суперпозиційних станах. Ця модель забезпечує компактність представлення та можливість паралельної обробки, але має значну обчислювальну складність і застосовується лише до квадратних зображень. На відміну від неї, модель NEQR кодує інтенсивність у базисних станах кубітів і дозволяє зменшити складність формування зображення у квантовому вигляді, що робить її технологічно зручною та придатною для використання в схемах стеганографії [3]. Усі ці моделі демонструють різний баланс між точністю представлення, кількістю необхідних кубітів та обчислювальною ефективністю,

проте саме NEQR найкраще відповідає вимогам стеганографії з огляду на простоту побудови та зручність інтеграції зі схемами вбудовування.

Квантова стеганографія зображень у контексті LSB-методів ґрунтується на заміні найменш значущих бітів інтенсивності пікселів на біти повідомлення. Простий LSB-алгоритм виконує таку заміну без додаткових структурних операцій, тому є легким у реалізації, але має низьку стійкість до атак, оскільки зміни на рівні окремих пікселів легко ідентифікувати за допомогою стеганоаналізу. Через це його практичне застосування обмежене.

Зовсім інші властивості демонструє блоковий LSB-алгоритм. Він передбачає розбиття квантового зображення на блоки, у межах яких формується агреговане значення LSB, і саме воно використовується для приховування одного кубіта повідомлення. Задля реалізації такої схеми необхідні додаткові квантові компоненти - лічильник і компаратор, які дозволяють виконувати підсумовування та порівняння значень у межах блоку. Вбудовування здійснюється лише для тих блоків, що відповідають позиції повідомлення, тоді як попереднє скремблювання зображення за методом кривої Гільберта забезпечує додаткову непомітність. Під час вилучення повідомлення блоки аналізуються з урахуванням порогового значення, що дозволяє відновити правильний кубіт навіть у разі часткового спотворення. Таким чином, блоковий LSB забезпечує значно вищу стійкість порівняно з простим методом, оскільки зміна одиничного LSB уже не впливає на точність вилучення інформації, а операції з блоками формують природний захист від випадкових або цілеспрямованих атак. Дослідження методів квантової стеганографії зображень демонструє перспективність їх використання у сучасних системах захисту інформації. Моделі представлення квантових зображень мають суттєві відмінності, і вибір конкретної моделі визначає ефективність побудови стеганографічної схеми. Найбільш збалансованим за складністю та продуктивністю є підхід NEQR, що дозволяє оптимально організувати приховування даних у квантових зображеннях. Аналіз алгоритмів LSB показує, що хоча простий метод має низьку стійкість, блоковий LSB забезпечує високу непомітність і можливість адаптації під різні вимоги. Обидва алгоритми базуються на сліпому вилученні, що робить їх практичними у використанні. Результати дослідження підтверджують значний потенціал квантової стеганографії та окреслюють напрям подальших робіт, пов’язаних із підвищенням стійкості, оптимізацією обчислювальних ресурсів і моделюванням реальних систем квантового приховування інформації.

Список літератури

1. Конахович Г. Ф., Шевченко О. В., Кінзеревий В. М., Хохлачова Ю. Е. Сучасні методи квантової стеганографії. Захист інформації. 2011. № 2 (51). С. 5–9.

2. Шпикуляк , І.С. 2024. Роль стенографії як засобу запису інформації. Інформаційні технології і системи в документознавчій сфері. (Бер 2024), 13-14.

3. Методи захисту інформації на основі квантової стеганографії зображень / О. Федюшин, Є. Головко, А. Смірнов, В. Сухотеплий, О. Чечуй // Радіотехніка. – 2024. – Вип. 218. – С. 44–55. – DOI : https://doi.org/10.30837/rt.2024.3.218.03

ЗАСТОСУВАННЯ ГЛИБИННОГО НАВЧАННЯ У ВИЯВЛЕННІ АНОМАЛІЙ МЕРЕЖЕВОГО ТРАФІКУ

Зінченко Є.Ю., Балагура Д.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні інформаційні мережі передають великий обсяг даних і мають високу швидкість обміну та високу комунікаційну складність, що робить виявлення кіберзагроз і несанкціонованих дій складним. Традиційні методи аналізу мережевого трафіку, що засновані на сигнатурному виявленні, не забезпечують достатнього захисту від нових або невідомих типів загроз. Це означає, що для виявлення загроз в сучасних інформаційних мережах необхідно використовувати інтелектуальні методи обробки даних, і глибоке навчання має важливе значення [1].

Метою роботи є вивчення можливостей використання методів глибинного навчання для виявлення аномалій у трафіку мережі, порівняння ефективності різних архітектур нейронних мереж (CNN, RNN і автоенкодерів) і визначення перспективи їх інтеграції у сучасні системи інформаційної безпеки. Багатошарові нейронні мережі є основою глибокого навчання, підмножини машинного навчання. Ці мережі можуть автоматично визначати важливі ознаки в даних і виявити приховані закономірності. Автоенкодери, згорткові (CNN), рекурентні (RNN) та LSTM-архітектури дозволяють ефективно аналізувати неструктуровані потоки мережевого трафіку та класифікувати відхилення, які можуть свідчити про атаки чи аномалії [2, 3]. У дослідженні використовувалися набори даних CICIDS2017 і UNSW-NB15, які містять приклади нормального та шкідливого трафіку. Результати експерименту показали, що моделі глибинного навчання перевершують традиційні методи машинного навчання щодо швидкості та точності виявлення аномалій. Результати підтверджують, що впровадження глибинних моделей у системи SIEM та UEBA є доцільним для підвищення ефективності моніторингу та управління інцидентом інформаційної безпеки в умовах зростаючих обсягів даних, швидкісних характеристик мереж та кіберзагроз [2, 3]. Таким чином, використання глибинного навчання в системах виявлення аномалій підвищує точність, адаптивність і надійність захисту інформаційних мереж, що робить цей напрям одним із ключових у розвитку інтелектуальних систем кібербезпеки.

Список літератури

1. Chawla, S., Chalapathy, R. *Deep Learning for Anomaly Detection: A Survey*. arXiv preprint, 2019. Посилання: https://arxiv.org/abs/1901.03407?

2. The UNSW-NB15 Dataset, The University of New South Wales. Посилання: https://research.unsw.edu.au/projects/unsw-nb15-dataset

3. Moustafa N., Slay J. *UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems*. – MilCIS Conference, 2015. Посилання: https://researchdata.edu.au/the-unsw-nb15-dataset/1957529?

РОЗРОБКА СИСТЕМИ ФІЛЬТРАЦІЇ ЕЛЕКТРОННОЇ ПОШТИ НА ОСНОВІ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ

Даншин В.В., Балагура Д.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасне інформаційне суспільство характеризується стрімким розвитком цифрових технологій і зростанням обсягів електронного листування. Електронна пошта є одним із найпоширеніших засобів комунікації в бізнесі, державному секторі та повсякденному житті [1]. Разом із цим різко зростає кількість кіберзагроз, пов'язаних із поштовими повідомленнями - спам, фішингові атаки, шкідливі вкладення, соціальна інженерія тощо [2]. Традиційні системи фільтрації електронної пошти, що базуються на фіксованих правилах або простих статистичних моделях, уже не здатні ефективно протидіяти сучасним атакам, які постійно змінюють структуру та зміст повідомлень. У цих умовах актуальним стає використання технологій штучного інтелекту (ШІ), зокрема великих мовних моделей (LLM) [3], які можуть здійснювати семантичний аналіз, розуміти контекст і логіку тексту, а також самонавчатися на основі нових прикладів.

Метою роботи є розроблення інтелектуальної системи фільтрації електронної пошти із застосуванням сучасних моделей машинного навчання та архітектури Retrieval-Augmented Generation [4]. У роботі розглядаються актуальні загрози електронній пошті, такі як спам, фішинг, spear-phishing, шкідливі вкладення та автоматизовані ШІ-згенеровані повідомлення. Аналізуються класичні методи фільтрації black/white списки, rule-based, баєсів фільтр та порівнюються з підходами на основі трансформер-моделей і векторного пошуку. Реалізується прототип системи, що поєднує нейронні мережі, динамічне формування правил і гібридну обробку даних з елементами RAG-архітектури. Результатом дослідження є створення адаптивної системи, здатної виявляти спам і фішингові повідомлення з високою точністю, пояснювати свої рішення та динамічно оновлювати правила класифікації. Створення UI дизайну для користувача та адміністратора для коригування роботи системи і аналізу роботи ШІ. Отримані результати підтверджують доцільність впровадження ШІ у сферу кіберзахисту електронної пошти.

Список літератури

1. Cloudflare. Email Security Threat Report, 2024. [Електронний ресурс]. – Режим доступу: https://blog.cloudflare.com/radar-2024-year-in-review/
2. Голубничий, Д.Ю., Сєвєрінов, О.В., Коломійцев, О.В., та інш. (2021). Аналіз сучасних загроз в інформаційних системах за складовими загроз: кібербезпеки, інформаційної безпеки та безпеки інформації.
3. Large language models [Електронний ресурс]. – Режим доступу: https://link.springer.com/article/10.1007/s10462-024-10888-y
4. Retrieval-Augmented Generation [Електронний ресурс]. – Режим доступу: https://www.sciencedirect.com/science/article/pii/S1877050924021860

МЕТОДИ АНАЛІЗУ СТІЙКОСТІ АЛГОРИТМУ ASCON ДО АЛГЕБРАЇЧНИХ АТАКА

Руженцев В.І., Куценко Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Розвиток сучасних стандартів легковагової криптографії зумовлює необхідність глибокого дослідження їхньої стійкості до алгебраїчних атак, які базуються на поданні криптографічних перетворень у вигляді систем булевих рівнянь над полем GF(2). Одним із таких алгоритмів є Ascon [1], що у 2023 році був обраний Національним інститутом стандартів і технологій США (NIST), як базовий стандарт легковагової криптографії для захисту даних у пристроях з обмеженими обчислювальними ресурсами.

Ascon ґрунтується на губчастій конструкції (sponge construction), використовує 5-бітні S-блоки, подібні до SHA-3, та лінійний шар, споріднений з SHA-2. Така структура забезпечує високу продуктивність і компактність, проте потенційно може бути вразливою до алгебраїчних і кубічних атак [2], що експлуатують низький алгебраїчний ступінь окремих компонентів алгоритму.

Доповідь присвячена методам аналізу криптостійкості алгоритму Ascon до алгебраїчних атак, а також до куб-атаки. Представлені в [3] результати демонструють, відомі оцінки криптостійкості можуть бути завищені і реальна криптостійкість алгоритму може бути нижче. Саме тому необхідно провести власний експеримент з імітації куб атаки на алгоритм Ascon та порівняти отримані характеристики з існуючими.

Метою доповіді є аналіз та оцінка стійкості багатораундового криптографічного алгоритму Ascon до алгебраїчних атак, зокрема до кубічної атаки, шляхом моделювання внутрішніх перетворень у вигляді систем булевих багаточленів, дослідження алгебраїчних властивостей S-блоків і лінійного шару, а також оцінювання алгебраїчного ступеня перетворень на різних етапах роботи алгоритму. Для досягнення поставленої мети передбачено: побудову математичної моделі криптоалгоритму Ascon, аналіз зміни алгебраїчного ступеня при різній кількості раундів, практичну реалізацію скороченого варіанту Ascon для перевірки ефективності куб-атаки та формування рекомендацій щодо підвищення його криптостійкості.

Список літератури

1. Lightweight cryptography project of the American National Institute of Standards and Technology, 2015. URL: https://csrc.nist.gov/projects/lightweight-cryptography.

2. Lars R. Knudsen. Truncated and higher order differentials. In Bart Preneel, editor, Fast Software Encryption, pp. 196–211, Berlin, Heidelberg, 1995. Springer Berlin Heidelberg. / Режим доступу: https://doi.org/10.1007/3-540-60590-8_16

3. V. Ruzhentsev. Nonlinear degree of Ascon permutation. INTERNATIONAL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, Poland, Warsaw, 2025, VOL. 71, № 2, PP. 477-482, doi: 10.24425/ijet.2025.153594.

МЕТОДИ ВИЯВЛЕННЯ ТА ПРОТИДІЇ MEV-АТАКАМ ЧЕРЕЗ МІЖЛАНЦЮГОВІ ПРОТОКОЛИ У ДЕЦЕНТРАЛІЗОВАНИХ СИСТЕМАХ

Антіпін В.С., Олійников Р.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Розвиток децентралізованих фінансових систем (DeFi) та поширення міжланцюгових протоколів створили нові вектори кібератак, серед яких особливе місце займають MEV-експлойти (Maximal Extractable Value). Ці атаки дозволяють валідаторам, пошуковикам або операторам вузлів маніпулювати порядком транзакцій для отримання додаткового прибутку за рахунок звичайних користувачів. У контексті міжланцюгової взаємодії проблема набуває особливої гостроти через асинхронність підтверджень транзакцій, різну швидкість фіналізації блоків і відсутність єдиного механізму консенсусу між блокчейнами.

За результатами дослідження Lyu та ін. (2022) [1], системи приватних транзакцій у Ethereum продемонстрували суттєвий ризик централізації та уразливість до повторного впорядкування операцій, що безпосередньо пов'язано з феноменом MEV. Паралельно Öz та ін. (2025) [2] показали, що частка міжланцюгових арбітражних транзакцій у загальному обсязі MEV-активності зросла з 7,8% до 21% упродовж двох років, що вказує на стрімке поширення кросчейн-маніпуляцій. У звіті Європейського управління з цінних паперів і ринків (ESMA, 2022) [3] зазначено, що швидке зростання обсягів транзакцій у DeFi без належних механізмів контролю створює ризики для стабільності фінансової системи, включно з ринковими викривленнями, спричиненими MEV.

Метою дослідження є постановка задачі розроблення комплексного підходу до виявлення та протидії MEV-атакам у міжланцюговому середовищі з урахуванням відмінностей у механізмах консенсусу, затримках підтвердження транзакцій та топології мереж. Робота спрямована на формування методологічної основи для побудови системи захисту децентралізованих фінансових протоколів від нового класу кіберзагроз.

Аналіз наукових джерел показує, що проблематика MEV-атак активно вивчається, однак більшість робіт фокусується на внутрішньоланцюгових сценаріях.

Daian та ін. (2020) [4] уперше формалізували концепцію MEV і довели, що валідатори можуть отримувати додатковий прибуток шляхом переупорядкування, вставки або цензурування транзакцій, що порушує принцип справедливості системи. Qin, Zhou і Gervais (2022) [6] провели кількісну оцінку вилученої вартості та визначили понад 600 млн доларів збитків у період 2020–2021 років. Mazor і Rottenstreich (2024) [5] експериментально підтвердили наявність значних арбітражних можливостей у міжланцюговому обміні, які можуть бути використані для скоординованих MEV-експлойтів.

Водночас існуючі рішення не враховують асинхронність підтверджень між різними ланцюгами, різницю у протоколах фіналізації блоків і специфіку кросчейн-мостів. Öz та ін. (2025) [2] наголошують, що саме затримка між станами ланцюгів і неузгодженість їхніх фіналізацій створюють основу для появи міжланцюгових MEV.

У цьому дослідженні міжланцюгова екосистема розглядається як розподілена система з асинхронною взаємодією компонентів, де кожен блокчейн представлено як окремий процес із власним механізмом консенсусу та правилами фіналізації. Для формалізації моделі загроз вводиться поняття системи

$$S = (C, B, M, T, F),$$

де C – множина блокчейнів;

B – множина міжланцюгових мостів;

M – функція маршрутизації повідомлень між ланцюгами;

T – множина транзакцій;

F – функція фіналізації для кожного ланцюга, що визначає часові вікна та гарантії підтвердження.

MEV-атака в такій системі визначається як послідовність дій

$$A = \langle a_1, a_2, \dots, a_k \rangle,$$

де a_i – вставка, видалення або переупорядкування транзакції в межах одного чи кількох ланцюгів.

Атака вважається успішною, якщо

$$\Pi(A) = profit(A) - [cost(A) + risk(A)] > 0,$$

де $profit(A)$ – отриманий прибуток;

$cost(A)$ – витрати на виконання атаки;

$risk(A)$ – очікувані втрати через санкції або невдачу.

Основна складність виявлення таких атак полягає в необхідності кореляції подій у різних блокчейнах з урахуванням затримок фіналізації.

Для встановлення причинно-наслідкових зв'язків між подіями пропонується використовувати годинники Лампорта (для встановлення часткового порядку подій) у поєднанні з векторними годинниками Fidge–Mattern, що дозволяє визначати послідовність транзакцій між різними ланцюгами. Це дає змогу виявляти скоординовані атаки, у яких зловмисник використовує декілька адрес у різних блокчейнах для маскування маніпуляцій. Для оцінки рівня підозрілості транзакційного патерну визначається функція

$$S(p) = \alpha \cdot temporal(p) + \beta \cdot volume(p) + \gamma \cdot frequency(p) + \delta \cdot identity(p),$$

де $temporal(p)$ – часові аномалії;

$volume(p)$ – обсяг операцій;

$frequency(p)$ – частоту появи подібних дій;

$identity(p)$ – повторюваність або кореляцію між адресами вузлів.

На практичному рівні пропонується архітектура розподіленої системи моніторингу, що складається з трьох модулів. Перший – модуль збору даних, який отримує транзакційні події з публічних мемпулів у мережах типу Ethereum [1], а також через подієві стріми Geyser/Block Engine у Solana та журнали relay-повідомлень у протоколах Axelar, IBC або LayerZero [2]. Другий – модуль кореляційного аналізу, що синхронізує часові ряди та застосовує модифіковану метрику подібності Жаккара з часовим вікном для визначення відповідності транзакцій між ланцюгами. Третій – модуль виявлення аномалій, який використовує комбінацію статистичного аналізу та алгоритмів машинного навчання (Isolation Forest, DBSCAN) для класифікації підозрілих шаблонів поведінки.

Серед запропонованих механізмів протидії передбачається застосування протоколів commit-reveal для міжланцюгових транзакцій, введення випадкових часових вікон у роботі мостів, багатоджерельна агрегація цінових даних для оракулів і впровадження схем MEV-refund, що частково компенсують користувачам негативний ефект маніпуляцій [4, 6]. Особлива увага приділяється інтеграції з системами Web3-SOC та SIEM, що дозволяє перетворювати виявлені події на сигнали кіберзахисту для провайдерів ліквідності та операторів мостів.

Реалізація запропонованого підходу сприятиме підвищенню рівня захисту децентралізованих фінансових систем від MEV-атак у міжланцюговому середовищі та створить основу для подальших досліджень і розроблення стандартів кібербезпеки.

Список літератури

1. An empirical study on Ethereum private transactions and the security implications / X. Lyu та ін. 2022. URL: https://doi.org/10.48550/arXiv.2208.02858.

2. Cross-chain arbitrage: the next frontier of MEV in decentralized finance / B. Öz та ін. URL: https://arxiv.org/abs/2501.17335.

3. European Securities and Markets Authority. Crypto-assets and their risks for financial stability. 2022. URL: https://www.esma.europa.eu/sites/default/files/library/esma50-165-2251_crypto_assets_and_financial_stability.pdf.

4. Flash boys 2.0: frontrunning in decentralized exchanges, miner extractable value, and consensus instability / P. Daian та ін. *2020 IEEE symposium on security and privacy (SP)*, м. San Francisco, CA, USA, 18–21 трав. 2020 р. 2020. URL: https://doi.org/10.1109/sp40000.2020.00040.

5. Mazor O., Rottenstreich O. An empirical study of cross-chain arbitrage in decentralized exchanges. *2024 16th international conference on communication systems & networks (COMSNETS)*, м. Bengaluru, India, 3–7 січ. 2024 р. 2024. URL: https://doi.org/10.1109/comsnets59351.2024.10426894.

6. Qin K., Zhou L., Gervais A. Quantifying blockchain extractable value: how dark is the forest?. *2022 IEEE symposium on security and privacy (SP)*, м. San Francisco, CA, USA, 22–26 трав. 2022 р. 2022. URL: https://doi.org/10.1109/sp46214.2022.9833734.

МЕТОДОЛОГІЯ ПРОВЕДЕННЯ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ВЕБ-ДОДАТКІВ

Дорофєєва К.І., Сєвєрінов О.В., Сидоренко З.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Забезпечення інформаційної безпеки веб-додатків залишається критично важливим завданням для організацій різного масштабу. Одним із прийнятних підходів для систематичної оцінки безпеки є тестування на проникнення, яке дозволяє імітувати дії зловмисника з метою виявлення слабких місць у захисті додатка. Аналіз актуальних загроз, що постають перед сучасними веб-додатками в умовах стрімкого розвитку технологій показує постійне зростання кількості кібератак. Основні категорії з них - ін'єкційні атаки (SQL/NoSQL Injection), міжсайтовий скриптинг (XSS), підробка запитів (CSRF), атаки на автентифікацію та управління сесіями, зокрема brute force, credential stuffing та викрадення токенів. Особлива увага необхідно приділяти вразливостям у контролі доступу, сучасним атакам на API та ризикам, пов'язаним із використанням сторонніх бібліотек і компонентів у ланцюгах постачання [1, 2].

Метою доповіді є дослідження та формалізація методології проведення тестування на проникнення веб-додатків, а також формування чіткої послідовності дій, метрик і шаблонів звітності для етичних тестувань на проникнення.

Послідовність проведення тестування на проникнення передбачає такі етапи [3, 4].

1. Підготовчий етап. Визначення об'єкта тестування, меж і правил, отримання письмового дозволу від власника системи і узгодження часових вікон для виконання активних перевірок;

2. Планування та конфігурація інструментів. Налаштування проксі, визначення політик сканування, імпорт сценаріїв аутентифікації, підготовка довірених сертифікатів для HTTPS-трафіку та інтеграція із засобами автоматизації;

3. Збір інформації. Реєстрація всіх HTTP/HTTPS-запитів і відповідей, ідентифікація точок введення даних, карта сторінок і перечислення функціональних API. Пасивний збір дозволяє мінімізувати ризик впливу на продуктивне середовище; активний – застосовується тільки в узгоджені вікна й за наявності дозволу;

4. Аналіз вразливостей. Застосування правил виявлення OWASP ZAP та власних тестів для виявлення класичних категорій вразливостей. Тут описується як проводити верифікацію виявлень вручну або із застосуванням скриптів, щоб уникнути хибнопозитивних спрацьовувань;

5. Перевірка експлуатації. Документоване відтворення виявлених пробілів у безпеці з максимально обережними діями, що не завдають шкоди системі;

6. Формування звіту та рекомендацій. Стандартизований шаблон звіту: опис вразливості, кроки відтворення, рівень критичності, можливі наслідки,

короткострокові та довгострокові рекомендації, пріоритети усунення та запропоновані заходи з моніторингу;

7. Післятестові дії. Перевірка усунення вразливостей, оновлення документації з безпеки, передача знань команді розробки та налаштування автоматичного моніторингу для виявлення регресій.

У доповіді представлено структурований підхід до реалізації кожного з етапів методології. Акцент зроблено на узгодженні меж перевірки, документуванні дій та стандартизації процесу звітування, що забезпечує відтворюваність результатів і можливість інтеграції методології в корпоративні процеси управління безпекою. Описано методику збору метрик, умови експериментів і вимоги до середовища для забезпечення достовірності результатів.

Завдяки запропонованій методології забезпечується не лише систематичний і формалізований підхід до виявлення та аналізу вразливостей веб-додатків, але й створюється основа для побудови комплексного процесу управління безпекою веб-додатків [1]. Розроблена послідовність дій дозволяє поєднати теоретичні принципи тестування на проникнення з практичними аспектами його реалізації в реальних умовах експлуатації. Це забезпечує відтворюваність результатів, точність виявлення вразливостей і можливість їх подальшого усунення без шкоди для продуктивного середовища [5].

Отже, розроблена методологія проведення тестування на проникнення веб-додатків є гнучким, масштабованим і практично орієнтованим інструментом, який може бути впроваджений як у невеликих організаціях, так і у великих корпоративних середовищах. Її застосування сприяє формуванню культури безпечної розробки (SDLC), підвищенню рівня обізнаності персоналу щодо сучасних загроз і створює основу для побудови стійкої та адаптивної системи захисту, здатної ефективно реагувати на динамічні зміни кіберсередовища.

Список літератури

1. OWASP Top Ten | OWASP Foundation. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. URL: https://owasp.org/www-project-top-ten/ (date of access: 21.10.2025).

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

3. Qiu, X.; Wang, S.; Jia, Q.; Xia, C.; Xia, Q. An automated method of penetration testing. In Proceedings of the 2014 IEEE Computers, Communications and IT Applications Conference, Beijing, China, 20–22 October 2014; pp. 211–216.

4. Д'якова, Н. Є., & Сєвєрінов, О. В. (2022). Тестування вразливостей сучасних веб-ресурсів.

5. Zhou, T.-Y.; Zang, Y.-C.; Zhu, J.-H.; Wang, Q.-X. NIG-AP: A new method for automated penetration testing. Front. Inf. Technol. Electron. Eng. 2019, 20, 1277–1288.

ВИКОРИСТАННЯ SPLUNK SOAR PHANTOM ДЛЯ ОПТИМІЗАЦІЇ ТА АВТОМАТИЗАЦІЇ РЕАГУВАННЯ НА ІНЦИДЕНТИ В SOC

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

Центри операцій безпеки SOC щоденно отримують та обробляють велику кількість кіберінцидентів, що часто може подовжити час реагування та підвищити ймовірність пропуску загроз, які можуть спричинити значні наслідки для організації. За результатами SANS Institute, приблизно 79% центрів операцій безпеки функціонують у режимі 24/7, що свідчить про потребу у постійному моніторингу інформаційної інфраструктури та миттєвому реагуванні на інциденти безпеки [1]. Співробітники SOC формують звіти власноруч, витрачаючи на це значну частину робочого дня. У той час автоматизація залишається обмеженою, що створює потенціал для впровадження платформ типу SOAR для підвищення ефективності [2, 3].

Метою доповіді є дослідження можливостей платформи Splunk SOAR Phantom для автоматизації процесу реагування на інциденти в SOC та оцінки ефективності її використання з метою оптимізації часу та ресурсів обробки інцидентів.

Згідно зі звітом Gartner Market Guide for Security Orchestration, Automation and Response Solutions [4] ринок SOAR рішень нині перебуває у фазі активного злиття з SIEM-платформами, формуючи єдині системи управління та реагування на інциденти. Такий підхід забезпечує підвищення ефективності роботи SOC шляхом об’єднання процесів моніторингу, аналітики та автоматизації реагування. У переліку провідних продуктів ринку Gartner [4] виокремлює Splunk SOAR, який демонструє інтеграційні можливості та розширену взаємодію з джерелами загроз і зовнішніми API.

Саме тому у ході було реалізовано інтеграцію між Splunk SOAR Phantom [5] та SIEM-системою Splunk Enterprise Security [6], що робить їхню взаємодію ефективним інструментом для оптимізації та автоматизації реагування на інциденти у середовищі SOC. Така взаємодія забезпечує автоматичне отримання повідомлень алертів із SIEM і подальшу обробку інцидентів за допомогою заздалегідь впроваджених сценаріїв плейбуків.

Крім того, значним напрямом розвитку є покращення здатності Splunk SOAR працювати разом з іншими аналітичними платформами та хмарними сервісами. Це дасть змогу об’єднати всі системи безпеки в одну узгоджену екосистему, де дані аналізуватимуться централізовано, а реагування на загрози відбуватиметься швидше та ефективніше. Наприклад, у дослідженні було обрано API-платформу AbuseIPDB, яка дозволяє виконувати перевірку статусів і репутації IP-адрес. Після надходження оповіщення про підозрілу IP-адресу з SIEM, система SOAR автоматично витягує цю адресу з події, надсилає запит до AbuseIPDB API та отримує звіт про репутацію. У разі виявлення підозрілої активності SOAR додатково перевіряє наявність цієї IP-адреси у внутрішньому “чорному списку” організації. Якщо збігів не виявлено, плейбук

автоматично формує повідомлення для працівників SOC із рекомендацією щодо блокування IP-адреси.

Доцільно використовувати технології машинного навчання для підвищення точності автоматичного визначення рівня важливості інцидентів і вдосконалення механізмів кореляції подій між різними джерелами даних, що дозволить ще більше скоротити час реагування та зменшити кількість хибних спрацювань. Впровадження інтелектуальних алгоритмів аналізу загроз дозволить автоматично виявляти складні атаки, що часто залишаються непоміченими при традиційних методах моніторингу.

У доповіді наводяться результати вимірювань ефективності впровадження автоматизованого реагування на інциденти за допомогою Splunk SOAR Phantom. Спираючись на них, можна стверджувати, що реалізована інтеграція дозволяє працівникам SOC-центрів мінімізувати обсяг ручної обробки подій, яка інколи може призводити до затримок у реагуванні більш серйозних подій. Згідно з результатами дослідження компанії Exaforce [2], впровадження автоматизації реагування дає змогу скоротити час розслідування інцидентів більш ніж на 60 %. Тож, подальший розвиток таких систем передбачає вдосконалення взаємодії між людиною та автоматизованими механізмами реагування. Це дає змогу зменшити навантаження на аналітиків SOC, скоротити час ухвалення рішень і мінімізувати вплив людського фактора на процес реагування.

Отже, інтеграція Splunk SOAR Phantom із Splunk Enterprise Security на практиці показує, як можна автоматизувати та узгодити процеси кіберзахисту. Використання SOAR-рішень є ефективним способом створення сучасної та гнучкої системи реагування на інциденти безпеки, яка відповідає поточним вимогам і тенденціям розвитку кібербезпеки.

Список літератури

1. *Elastic – The Search AI Company | Elastic*. URL: https://www.elastic.co/pdf/sans-soc-survey-2025.pdf (дата звернення: 05.11.2025).

2. Exaforce Learning Center | Automating incident response in the SOC: Machine-speed defense for modern threats. *Exaforce*. URL: https://www.exaforce.com/learning-center/automating-incident-response-in-the-soc-machine-speed-defense-for-modern-threats?utm_source=chatgpt.com (дата звернення: 05.11.2025).

3. Ушатов, В., Сєвєрінов, О.В. (2019). Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки.

4. Security Orchestration, Automation and Response Solutions Reviews and Ratings. *www.gartner.com*. URL: https://www.gartner.com/reviews/market/security-orchestration-automation-and-response-solutions (дата звернення: 05.11.2025).

5. *Splunk SOAR Validated Architectures Version 2.0| The Key to Enterprise Resilience*. URL: https://www.splunk.com/en_us/pdfs/tech-brief/splunk-phantom-validated-architectures.pdf (дата звернення: 05.11.2025).

6. Splunk® Enterprise Security Analytics Driven Security and Continuous Monitoring for Modern Threats. *Winncom Technologies | Головна*. URL: https://winncom.ua/wp-content/uploads/2018/07/Splunk-Enterprise-Security.pdf (дата звернення: 05.11.2025).

МЕТОД ПОБУДОВИ ГРАФУ АТАКИ В SIEM-СИСТЕМАХ НА ОСНОВІ КОНТЕКСТУ ІДЕНТИЧНОСТІ

Москвін К.С., Балагура Д.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні центри моніторингу безпеки (SOC) стикаються з експоненційним зростанням обсягів даних. Впровадження ешелонованого захисту, що включає системи EDR, NGFW та IAM, генерує мільйони окремих подій. Це створює фундаментальну проблему: традиційні SIEM-системи, хоч і агрегують ці дані, часто не здатні автоматично зв'язати їх у єдиний, зрозумілий ланцюжок інциденту. Як наслідок, аналітики перевантажені сповіщеннями, що призводить до "втоми від сповіщень" та збільшення часу виявлення загроз [1, 2]. Зі збільшенням складності атак зростає і їхня прихованість. Зловмисники активно використовують вкрадені облікові дані для легітимного, на перший погляд, просування всередині мережі. Існуючі механізми кореляції, що покладаються на зіставлення IP-адрес, хешів або статичних сигнатур, виявляються неефективними. Вони не можуть надійно відрізнити легітимну дію привілейованого користувача від дій зловмисника, що заволодів його акаунтом [3].

Тема даної доповіді присвячена розробці методу, що вирішує цю проблему шляхом використання контексту ідентичності як центрального вузла для кореляції подій. На відміну від підходів, де IAM є лише одним із джерел логів, запропонований метод використовує дані про користувачів, їхні ролі, привілеї та поведінкові патерни для автоматичного зв'язування розрізнених подій з EDR та NGFW. Це дозволяє в режимі реального часу формувати динамічний, орієнтований на користувача граф атаки, що є ключовим для реалізації сучасних стратегій безпеки, таких як Zero Trust [4].

Метою доповіді є дослідження та обґрунтування методу побудови графу атаки, який автоматично корелює події з різних систем захисту навколо сутності користувача. Такий підхід дозволяє миттєво візуалізувати повний ланцюжок атаки (Kill Chain), об'єднуючи мережеву активність, запуски процесів на хостах та спроби доступу. У рамках доповіді буде розглянуто запропоновану архітектуру інтеграції, алгоритм збагачення подій та побудови графу кореляції, а також представлено результати тестування методу на змодельованих сценаріях багатоетапних атак.

Список літератури

1. Cissec, J. The Challenge of Alert Overload in Modern Security Operations [Електронний ресурс] / Режим доповідей: https://securityboulevard.com
2. Sievierinov, O., Ovcharenko, M., & Vlasov, A. (2021). Enterprise Security Operations Center. Computer and information systems and technologies.
3. Microsoft. Identity is the new security perimeter [Електронний ресурс] / Режим доступу: https://www.microsoft.com
4. NIST. Special Publication 800-207: Zero Trust Architecture [Електронний ресурс] / Режим доступу: https://csrc.nist.gov/publications/detail/sp/800-207/final

ЗАСТОСУВАННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ ДЛЯ ЗАХИСТУ МЕРЕЖ ІНТЕРНЕТУ РЕЧЕЙ

Хруслов Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Стрімкий розвиток Інтернету речей (IoT) та експоненціальне зростання кількості підключених пристроїв, що, за прогнозами, значно збільшиться в найближчі роки, створюють фундаментальні виклики для кібербезпеки. Традиційні, переважно централізовані, моделі управління IoT-мережами демонструють значні архітектурні вразливості. Вони покладаються на централізовані сервери для зберігання та обробки даних, що робить їх вразливими до єдиних точок відмови (SPOF), а також до атак типу «відмова в обслуговуванні» (DoS) та «людина посередині» (MITM). Ця проблема значно посилюється через апаратні обмеження та програмну різноманітність мільярдів IoT-пристроїв. Багато сенсорів та виконавчих пристроїв не мають достатньої обчислювальної потужності, пам'яті та енергоресурсів для імплементації складних криптографічних протоколів, що ускладнює впровадження уніфікованих та надійних механізмів захисту [1, 2].

У цьому контексті технологія блокчейн пропонує трансформаційне рішення, здатне кардинально підвищити рівень захищеності розподілених IoT-систем. Впровадження децентралізованого, незмінного та криптографічно захищеного розподіленого реєстру дозволяє вирішити ключові проблеми вразливості, притаманні централізованим підходам. Основні переваги полягають у забезпеченні надійної цілісності даних, оскільки будь-яка спроба модифікації інформації у ланцюгу блоків буде миттєво виявлена. Крім того, децентралізована природа технології усуває єдину точку відмови, підвищуючи загальну відмовостійкість. Важливим аспектом є можливість реалізації новітніх методів управління доступом та ідентифікацією, наприклад, через децентралізовані ідентифікатори та смарт-контракти для автоматизації правил взаємодії пристроїв [3].

Однак, незважаючи на очевидні переваги, практична інтеграція блокчейну в IoT стикається з серйозними викликами, які випливають із фундаментальної невідповідності між ресурсоємною природою блокчейну та апаратними обмеженнями IoT. Для подолання цих суперечностей активно розробляються та досліджуються нові методи та гібридні архітектури. Одним з найбільш перспективних рішень є побудова багаторівневих систем, де кінцеві малопотужні сенсори об'єднуються в локальні «IoT-кластери». У таких архітектурах смарт-контракти можуть використовуватися для автоматизації процесів та управління правилами доступу на рівні кластера, тоді як для обміну даними з кінцевими пристроями застосовуються оптимізовані для мікроконтролерів криптографічні протоколи та бібліотеки [4]. Незважаючи на ефективність гібридних моделей, критичними проблемами залишаються фундаментальні виклики масштабованості. По-перше, це низька пропускна здатність (кількість транзакцій на секунду, TPS). Класичні блокчейни не

розраховані на обробку масивних потоків даних у реальному часі, які генерують IoT-системи. По-друге, це вимоги до зберігання даних: реєстр має тенденцію до постійного зростання, оскільки зберігає повну історію транзакцій. Це унеможливлює розміщення повних вузлів на пристроях з обмеженою пам'яттю, змушуючи їх покладатися на менш безпечні «легкі вузли». По-третє, це висока затримка при підтвердженні транзакцій, що виникає через час, необхідний для генерації та валідації блоків, і є неприйнятною для систем реального часу. Нарешті, високе енергоспоживання традиційних консенсус-алгоритмів, як-от Proof-of-Work, робить їх використання неможливим для пристроїв, що живляться від батарей. Це змушує дослідників звертати увагу на енергоефективні альтернативи, як-от Proof-of-Stake або безблокові структури DAG (Tangle). Крім того, існує проблема початкової довіри до даних: блокчейн гарантує незмінність даних, але не їхню початкову правдивість. Якщо скомпрометований сенсор, через апаратний збій або зловмисну дію, передасть некоректні дані, блокчейн лише надійно зафіксує цю дезінформацію [5]. **Метою доповіді** є проведення аналізу ключових переваг та фундаментальних технічних викликів при інтеграції блокчейн-технологій в розподілені системи Інтернету речей. **В доповіді** наводяться результати огляду сучасних методів, що пропонуються для вирішення конфлікту між вимогами безпеки блокчейну та апаратними обмеженнями IoT-пристроїв. Особлива увага приділяється розгляду гібридних багаторівневих архітектур та легковагих криптографічних протоколів. Наведені дані показують, що хоча технологія блокчейн пропонує потужні механізми для забезпечення цілісності даних та децентралізації, її практична реалізація вимагає вирішення складних проблем масштабованості, вибору енергоефективних механізмів консенсусу та розробки методів верифікації даних на етапі їх початкового збору.

Список літератури

1. Obaidat M. A., Rawashdeh M., Alja'afreh M., Abouali M., Thakur K., Karime A. Exploring IoT and Blockchain: A Comprehensive Survey on Security, Integration Strategies, Applications and Future Research Directions. *Big Data and Cognitive Computing*. 2024. Vol. 8, Art. 174. DOI: https://doi.org/10.3390/bdcc8120174

2. Yevheniev, A. M., Sydorenko, Z. M., & Sievierinov, O. V. (2025). Забезпечення цілісності даних у системах промислового інтернету речей на основі використання завадостійких кодів. Radiotekhnika, (221), 46-50.

3. Enaya A., Fernando X., Kashef R. Survey of Blockchain-Based Applications for IoT. *Applied Sciences*. 2025. Vol. 15, Art. 4562. DOI: https://doi.org/10.3390/app15084562

4. Чепель Л. В., Бойко Ю. В. Підхід до безпеки та організації мереж IoT з використанням блокчейн технології. *Вісник Вінницького політехнічного інституту*. 2024. № 4. С. 129–138. DOI: https://doi.org/10.31649/1997-9266-2024-175-4-129-138

5. Mezquita Y., Casado R., Gonzalez-Briones A., Prieto J., Corchado J. M. Blockchain Technology in IoT Systems: Review of the Challenges. *Annals of Emerging Technologies in Computing (AETIC)*. 2019. Vol. 3, No. 5. DOI: https://doi.org/10.33166/AETIC.2019.05.003

МЕТОДИ ПРОТИДІЇ НЕСАНКЦІОНОВАНОМУ ДОКУМЕНТУВАННЮ МОВИ

Шкопотко П.М., Олейніков А.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Актуальність захисту мовної інформації від несанкціонованого документування зростає через поширення високотехнологічних засобів акустичної розвідки, таких як мініатюрні диктофони, радіозакладки та лазерні системи [1, 2].

Метою дослідження є систематизація та аналіз ефективності сучасних методів протидії несанкціонованому документуванню мови. В доповіді розглядається класифікація методів за принципом впливу на засіб документування: фізичне придушення, функціональне придушення, виявлення та нейтралізація.

До акустичних методів належить створення маскуючих звукових завад, таких як білий шум, рожевий шум та найефективніша – мовоподібна завада («багатомовний гомін»).

Ефективність визначається зниженням індексу артикуляції та співвідношенням сигнал/шум (С/Ш) на вході мікрофона. Критичним параметром є відстань між джерелом завади та потенційним диктофоном, оскільки за законом зворотних квадратів наближення джерела завади до цілі дозволяє значно підвищити рівень завади при зменшенні загальної потужності [2, 3].

Електромагнітні методи спрямовані на придушення радіоканалів передачі даних шляхом постановки завад (jamming). Ефект досягається за рахунок детектування модульованого ВЧ-сигналу на нелінійних елементах схеми пристрою, що генерує низькочастотну заваду безпосередньо в аудіотракті, знижуючи співвідношення С/Ш [1]. Ефективність цих методів різко падає для добре екранованих пристроїв.

Ультразвукові методи поділяються на два типи. Одночастотний метод полягає у випромінюванні потужного ультразвукового сигналу, який сприймається мікрофоном та призводить до спрацьовування системи автоматичного регулювання підсилення (АРП) диктофона. АРП, сприймаючи потужний сигнал як перевантаження, знижує коефіцієнт підсилення всього тракту, тим самим приглушуючи корисний мовний сигнал. Двочастотний метод ґрунтується на одночасному випромінюванні двох ультразвукових сигналів з близькими частотами.

Внаслідок нелінійних властивостей вхідних каскадів підсилювача відбувається нелінійне перетворення цих частот із виділенням різницевої частоти, яка потрапляє в аудіодіапазон і створює ефективну заваду, що накладається на корисний сигнал [1, 4].

Найперспективнішим є модифікований акустичний метод, що поєднує адаптивне керування, спектральний аналіз та активний компенсувальний вплив. Він аналізує акустичну обстановку в реальному часі, виявляє активність

мови за допомогою VAD (Voice Activity Detection) та формує цільову заваду, спектр якої зосереджений на формантних частотах поточної мови. Це забезпечує високу ефективність при мінімальній потужності та психологічному дискомфорті, а також ускладнює роботу систем автоматичного розпізнавання мови (ASR) [1, 5].

Для оцінки ефективності методів запропоновано використовувати комплекс об'єктивних метрик, зокрема PESQ (Perceptual Evaluation of Speech Quality) для прогнозування суб'єктивної якості та STOI (Short-Time Objective Intelligibility) для оцінки розбірливості. Експериментальні дослідження, проведені для різних дистанцій між джерелом завади та диктофоном, підтверджують, що зменшення відстані значно підвищує ефективність придушення.

Зокрема, на відстані 0,5 м розбірливість мови, оцінена за STOI, падала до рівня неприйнятного для розуміння (менше 0,3), тоді як на відстані 2 м цей показник був значно вищим. Це підтверджує важливість мінімізації відстані "джерело завади - ціль" для підвищення енергетичної ефективності комплексних систем захисту.[5]

Найбільш ефективним є комплексний захист, що поєднує методи різної фізичної природи.

Серед активних методів адаптивні акустичні методи, такі як модифікований акустичний та цільові ультразвукові, демонструють найкращі результати щодо зниження якості та розбірливості несанкціонованого запису, особливо при забезпеченні мінімальної відстані до захищуваної зони.

Подальші дослідження перспективні у напрямку розвитку інтелектуальних систем, здатних адаптивно формувати заваду на основі аналізу параметрів мовного сигналу та характеристик середовища.

Список літератури

1. І.Є. Антіпов, А.М. Олейніков, Ю.В. Ликов, В.Д. Кукуш, І.О. Милютченко. Засоби та системи технічного захисту інформації: Навчальний посібник для студентів ЗВО / Харків: ХНУРЕ, 2019. – 216 с.

2. Олейніков, А. М. Математичне моделювання акустичного каналу витоку мовної інформації / А. М. Олейніков, О. М. Широкий // Радіотехніка: Всеукр. міжвід. наук.-техн. зб. – Харків, 2014. – Вип. 177. - С. 161 - 171.

3. Fielder, G. D. Acoustical and Vibrational Methods of Information Protection / G. D. Fielder // Journal of the Audio Engineering Society. – 1998. – Vol. 46, No. 7/8. – P. 652–665.

4. Гоков О.М. Фізичні основи технічних засобів розвідки: навчальний посібник / О.М. Гоков. – Харків: ХНЕУ ім. С. Кузнеця, 2022. – 255 с.

5. ITU-T Recommendation P.862: Perceptual evaluation of speech quality (PESQ): An objective method for end-to-end speech quality assessment of narrow-band telephone networks and speech codecs. – International Telecommunication Union, 2001.

ЗАХИЩЕНІСТЬ ОБ'ЄКТА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ВІД ДИСТАНЦІЙНИХ ЗАСОБІВ АКУСТИЧНОЇ РОЗВІДКИ

Олейніков А.М., Пономаренко Є.Д.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасних умовах розвитку технічних засобів спостереження виникає потреба у комплексному захисті об'єктів інформаційної діяльності від несанкціонованого зняття акустичної інформації. Сучасні засоби дистанційної акустичної розвідки здатні фіксувати коливання поверхонь або повітряних мас, спричинені мовленням людини, навіть на значній відстані від об'єкта [1]. Тому забезпечення належного рівня акустичної безпеки є критично важливим для організацій, які працюють з конфіденційною або державною інформацією.

Метою доповіді є аналіз технічних каналів витоку мовної інформації на об'єкті інформаційної діяльності (ОІД) від дистанційних засобів акустичної розвідки та розробка комплексу технічного захисту інформації на ОІД для забезпечення безпеки мовної інформації. До основних видів технічних загроз дистанційного акустичного знімання інформації належать використання вузькоспрямованих мікрофонів, які здатні приймати звукові сигнали на відстані до 100–150 м залежно від конкретного стану акустичного фону середовища поширення акустичних коливань, лазерні системи акустичної розвідки, які реєструють мікроколивання скла вікон на відстані декілька сотень метрів, а також деякі види пасивних радіоакустичних закладних пристроїв, в основі яких лежать методи високочастотного нав'язування при використанны високочастотних резонаторів [2]. У доповіді розглядаються питання створення комплексу технічного захисту інформації ОІД на основі використання звукопоглинальних матеріалів у конструкціях стін, підлоги, стелі застосування вікон із багатошаровими склопакетами, встановлення генераторів акустичних або вібраційних завад («маскувальних шумів»), використання плівок або фільтрів на скляних поверхнях, що знижують відбиття лазерного променя, створення звукоізольованих переговорних приміщень, забезпечення цілодобового радіомоніторингу та інше. Рекомендовано використовувати пасивні (звукоізоляційні) та активні (генератори шуму) методи захисту, а також проводити регулярні перевірки приміщень на наявність технічних засобів розвідки.

Список літератури

1. Засоби та системи технічного захисту інформації: Навчальний посібник для студентів ЗВО. / І.Є. Антіпов, А.М. Олейніков, Ю.В. Ликов, В.Д. Кукуш, І.О. Милютченко. 2-е вид., перероб. і доп. – Харків: ХНУРЕ, 2024. – 266 с.

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

ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА ПОТЕНЦІЙНИХ МОЖЛИВОСТЕЙ ВУЗЬКОСПРЯМОВАНИХ МІКРОФОНІВ

Машура А.П., Олейніков А.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Спрямованість мікрофонів є однією з ключових характеристик, що визначає їх ефективність у застосуваннях, пов'язаних із записом, передаванням і обробкою акустичних сигналів. Вузькоспрямовані мікрофони (ВНМ) використовуються в системах акустичної розвідки, моніторингу навколишнього середовища та спеціалізованих технічних засобах контролю. Їхні характеристики істотно залежать від геометричних параметрів конструкції – кількості елементів, їх взаємного розташування та співвідношення розмірів із довжиною звукової хвилі [1-3]. У роботі досліджено три основні типи ВНМ: лінійні групи мікрофонів, трубчасті мікрофони та рефлекторні системи. Для кожного типу розглянуто аналітичні залежності, що описують характеристику спрямованості $R(\theta)$, та розраховано коефіцієнт спрямованості Ω за інтегральною формулою $\Omega = \frac{2}{\int_0^{\pi} R^2(\theta)\sin\theta\, d\theta}$. Для лінійної групи мікрофонів характеристика спрямованості визначається як $R(\theta) = \frac{\sin\left(n\pi\frac{d}{\lambda}\sin\theta\right)}{n\sin\left(\pi\frac{d}{\lambda}\sin\theta\right)} \times R_1(\theta)$, де n – кількість мікрофонів; d – відстань між ними; λ – довжина хвилі; $R_1(\theta)$ – характеристика спрямованості окремого мікрофона. Аналіз показав, що збільшення довжини лінійної системи підвищує коефіцієнт спрямованості.

Трубчасті мікрофони описуються функцією $R(\theta) = \frac{\sin\left(n\pi\frac{d}{\lambda}(1-\cos\theta)\right)}{n\sin\left(\pi\frac{d}{\lambda}(1-\cos\theta)\right)}$ і мають простішу конструкцію, але нижчу вибірковість у низькочастотній області. Їх перевага полягає у компактності, проте вони поступаються лінійним групам за енергетичною ефективністю. Характеристика рефлекторних мікрофонівх описується функцією Бесселя $J_1(\psi)$: $R(\theta) = \frac{J_1(\psi)}{\psi/2}, \psi = \frac{2\pi\rho_0}{\lambda}\sin\theta,$ де ρ_0 – радіус параболи відбивача, забезпечують найкращу просторову вибірковість у високочастотному діапазоні. Вони не мають обмежень за максимальною частотою й демонструють найвищий рівень фокусування звукової енергії.

Моделювання характеристик проводилося засобами Python із використанням бібліотек NumPy, SciPy та Matplotlib. Це дозволило автоматизувати обчислення, побудувати діаграми спрямованості для різних частот і визначити залежність індексу спрямованості від геометричних параметрів. Результати показали, що при збільшенні діаметра рефлектора з 0,3 до 0,6 м головний пелюсток звужується майже на 40 %, а коефіцієнт спрямованості зростає у 2,5 рази. Отже, геометричні параметри визначають потенційні можливості ВНМ і повинні враховуватись при проектуванні. Під час аналізу індексу напрямленості при однакових лінійних розмірах мікрофонів, було виявлено що, для високочастотних застосувань найкраще використовувати

рефлекторні системи, для низько- та середньо-частотних — лінійні групи, а трубчасті мікрофони мають найгірші характеристики з цих трьох типів мікрофонів, що розглядаються.. Використання Python у процесі аналізу дозволяє створювати інтерактивні моделі та інтегрувати їх із системами ЦОС.

Список літератури

1. Олейніков А. М., Бородавка А. В. Основні напрямки вдосконалення засобів акустичної розвідки // *Радіотехніка*. – 2017. – Вип. 189. – С. 189–194.
2. Jespersen C. T., Kirkwood B. C., Groth J. Increasing the Effectiveness of Hearing Aid Directional Microphones. *Seminars in Hearing*. 2021. Т. 42, № 03. С. 224–236. URL: https://doi.org/10.1055/s-0041-1735131 (дата звернення: 02.11.2025).
3. Zhang X. Benefits and Limitations of Common Directional Microphones in Real-World Sounds. *Clinical Medicine Research*. 2018. Т. 7, № 5. С. 103. URL: https://doi.org/10.11648/j.cmr.20180705.12 (дата звернення: 02.11.2025).

АНАЛІЗ СУЧАСНИХ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ

Голобородько Д.В., Олейніков А.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Захист мовної інформації є актуальною проблемою сучасних телекомунікаційних систем, оскільки мовні канали зв'язку залишаються вразливими до різноманітних загроз інформаційній безпеці. Розвиток цифрових технологій обробки мовних сигналів створює нові виклики для забезпечення конфіденційності та автентичності голосових даних, особливо в контексті критичної інфраструктури [1, 2]. Метою роботи є аналіз сучасних методів захисту мовної інформації в телекомунікаційних системах та розробка рекомендацій щодо побудови багаторівневих систем захисту голосових комунікацій з урахуванням вимог до якості передачі мовлення в реальному часі. Основні загрози включають пасивне прослуховування каналів, активні атаки з модифікацією голосових даних, підміну голосу користувача та несанкціонований аналіз мовних записів із застосуванням методів машинного навчання. Зростання обчислювальних потужностей дозволяє атакуючим застосовувати складні алгоритми розпізнавання мовлення, що підвищує ризики витоку конфіденційної інформації [3].

У роботі розглядаються криптографічні методи, що базуються на математичних перетвореннях мовних потоків з використанням симетричних та асиметричних алгоритмів шифрування. Симетричні алгоритми забезпечують високу швидкість обробки та низькі затримки, що критично важливо для голосових комунікацій. Критичною особливістю є дотримання обмежень на затримки обробки, оскільки затримки понад 150 мілісекунд призводять до помітного погіршення якості інтерактивного спілкування.

Стеганографічні методи дозволяють вбудовувати додаткові дані в мовний сигнал через модифікацію його параметрів з мінімальним впливом на сприйняття

якості мовлення. Це досягається використанням психоакустичних моделей людського слуху. Стеганографічні підходи ефективно застосовуються для передачі службової інформації про стан захищеності каналу або додаткових ключових даних [4]. Методи скремблювання забезпечують захист через трансформацію часової або частотної структури сигналу. Часове скремблювання здійснює перестановку коротких сегментів мовного сигналу, тоді як частотне скремблювання інвертує спектральні компоненти. Проте ці методи забезпечують обмежений рівень захисту і використовуються як додатковий рівень безпеки. У доповіді також розглядаються методи запобігання несанкціонованому документуванню мови з використанням акустичного ультразвукового та електромагнітних методів подавлення. Біометричні методи верифікації базуються на аналізі унікальних характеристик голосу диктора з використанням статистичних моделей на основі мел-частотних кепстральних коефіцієнтів. Ці методи дозволяють аутентифікувати користувача та здійснювати періодичну верифікацію протягом розмови. Розвиток технологій синтезу мовлення вимагає вдосконалення методів виявлення спуфінгу та атак з використанням штучно згенерованого голосу [4]. Найбільш ефективним є побудова багаторівневої системи безпеки, що включає криптографічне шифрування каналу, біометричну аутентифікацію учасників та стеганографічне приховування службової інформації. Важливою є реалізація механізмів адаптивного управління рівнем захисту залежно від поточної оцінки загроз та доступних обчислювальних ресурсів [5]. Перспективні напрямки досліджень пов'язані з використанням квантових технологій для генерації криптографічних ключів, застосуванням методів глибокого навчання для виявлення аномалій у голосовому трафіку та розробкою захисту від атак з використанням синтезованого голосу та дипфейків. Забезпечення надійного захисту мовної інформації вимагає комплексного застосування методів різної природи. Вибір засобів має базуватися на аналізі специфічних загроз та врахуванні вимог до якості передачі мовлення. Подальший розвиток систем захисту має спрямовуватися на створення адаптивних рішень з автоматичним підбором конфігурації захисту.

Список літератури

1. Засоби та системи технічного захисту інформації: Навчальний посібник для студентів ЗВО / І. Є. Антіпов, А. М. Олейніков, Ю. В. Ликов, В. Д. Кукуш, І. О. Милютченко. 2-е вид., перероб. і доп. Харків: ХНУРЕ, 2024. 266 с.

2. Рубан І. В., Міхаль О. П. Методи захисту інформації в телекомунікаційних мережах критичного застосування. *Системи обробки інформації*. 2024. № 3. С. 45-52.

3. Сєвєрінов О. В., Ляшенко О. С. Біометричні методи ідентифікації в системах захисту інформації. *Радіоелектронні і комп'ютерні системи*. 2024. № 2. С. 118-125.

4. Kuchuk N., Kovalenko A. Approaches to synthesis of informational and technical structures of critical application object's control system. *Advanced Information Systems*. 2024. Vol. 8, No. 3. P. 34-40.

5. Ruban I., Sievierinov O. Method of voice information protection in telecommunication systems. *Telecommunications and Radio Engineering*. 2024. Vol. 83, No. 2. P. 15-24.

АНАЛІЗ ЕФЕКТИВНОСТІ ПОВНІСТЮ ГОМОМОРФНОГО ШИФРУВАННЯ ШЛЯХОМ ВИКОРИСТАННЯ МАТРИЧНИХ ПОЛІНОМІВ

Гущин Б.-Д.І.
Харківський національний університет радіоелектроніки, Харків, Україна

Зі зростанням обсягів хмарних обчислень актуальним стає питання забезпечення конфіденційності даних, що зберігаються та обробляються на зовнішніх серверах. Незважаючи на розвиток засобів доступу та безпеки, провайдери хмарних сервісів не гарантують повної відсутності ризику несанкціонованого доступу [1]. Тому виникає потреба в таких криптосистемах, які дозволяють здійснювати обчислення над інформацією, не розшифровуючи її.

Інструментом, що забезпечує таку властивість, є повністю гомоморфне шифрування, однак більшість відомих реалізацій страждають на надмірну обчислювальну складність. Одним із перспективних шляхів підвищення продуктивності є використання матричних поліномів та пакетного SIMD-кодування, що дозволяє одночасно виконувати операції над групами даних.

Метою доповіді є аналіз підходу до підвищення ефективності повністю гомоморфного шифрування (ПГШ) шляхом використання матричних поліномів і пакетного кодування, що дозволяє об’єднувати кілька відкритих текстів в один шифротекст для їх комплексної обробки у зашифрованому вигляді.

Гомоморфне шифрування є криптографічним примітивом, що викликає значний інтерес як у прикладному, так і в теоретико-математичному аспектах. Попри тривалу історію досліджень, низка ключових проблем цієї галузі досі лишається невирішеною. Гомоморфне шифрування має великий потенціал для застосування в сучасній криптографії та, ширше, у розробці математичних моделей і методів захисту інформації. Особливу практичну цінність становить можливість виконання обчислень безпосередньо над зашифрованими даними. У традиційних підходах конфіденційні дані шифруються перед зберіганням, а для виконання обчислень їх необхідно тимчасово розшифрувати, що створює потребу у використанні захищеного апаратного середовища та надійної інфраструктури керування секретними ключами. Натомість гомоморфне шифрування, за умови підтримки відповідних операцій, дозволяє здійснювати обчислення без розкриття даних, повністю усуваючи ризики, пов’язані з процесом їх розшифрування.

Основною сферою застосування повністю гомоморфних криптосистем є хмарні обчислення та інфраструктури аутсорсингу. Застосування ПГШ дозволяє зберігати дані на віддалених серверах виключно у зашифрованому вигляді та отримувати результати запитів також у зашифрованій формі, без потреби у проміжному розшифруванні інформації на стороні сервера.

Існує значна кількість протоколів взаємодії з базами даних, які забезпечують не лише конфіденційне отримання записів, а й приховане

отримання індексів елементів, що відповідають певним критеріям вибірки. Поряд із протоколами, що покладаються на повністю гомоморфне шифрування для виконання довільних операцій над зашифрованими даними, розробляються й інші схеми, у яких ПГШ використовується як інструмент для розв'язання специфічних криптографічних задач. До таких задач належать, перевірка делегованих обчислень та побудова стислих неінтерактивних доказів із нульовим розголошенням.

Можливість переставляти окремі слоти всередині одного шифротексту без його розшифрування суттєво розширює функціональні можливості гомоморфних систем [2]. Це уможливлює реалізацію стандартних машинних операцій у бітовому поданні, включаючи додавання, множення та логічний оператор XOR.

Практична значущість пакетного шифрування стала підґрунтям для включення його процедур до бібліотеки HElib, розробленої компанією IBM, яка є однією з найпоширеніших платформ для гомоморфних обчислень. У розглянутій криптосхемі відкриті тексти подаються у вигляді елементів кільця, тоді як шифротексти представляються матричними поліномами над цим самим кільцем. Шифрування передбачає кодування повідомлення у матрицю та формування матричного полінома із додаванням випадкової компоненти, що забезпечує семантичну криптостійкість.

Реалізація SIMD-шифрування може здійснюватися різними методами: на основі китайської теореми про залишки, [3] через використання множини різних власних значень або за допомогою інтерполяції матричних поліномів. Такий підхід є одним із найбільш гнучких, оскільки дає змогу контролювати ефективні SIMD-структури для гомоморфної обробки даних, зберігаючи можливість паралельного виконання операцій над векторами відкритих текстів.

Підходи до побудови пакетних повністю гомоморфних схем на основі матричних поліномів є перспективними для створення ефективних криптографічних механізмів.

Гомоморфне шифрування підтверджує свою актуальність як один із найбільш перспективних інструментів захисту інформації в умовах хмарних обчислень.

Список літератури

1. Рудий, С.В., Сєвєрінов, О.В. Дослідження моделі безпеки при використанні хмарних сервісів // ЧДТУ, ВА ЗС АР, УТіГН, НТУ "ХПІ", ХНУРЕ, "ПД ПКНДІ АП", 2022.

2. Белей, О. І. (2018) «Гомоморфне шифрування даних у хмарних сховищах методом матричних поліномів», Сучасний стан наукових досліджень та технологій в промисловості, (4 (6), с. 5–14. doi: 10.30837/2522-9818.2018.6.005.

3. Xun Yi, Russell Paulet, and Elisa Bertino, "Homomorphic Encryption and Applications", Springer, 2014, pp. 1-213.

МЕТОДИ ВЕРИФІКАЦІЇ БЕЗПЕКИ СМАРТ-КОНТРАКТІВ

Мокрій В.С., В'юхін Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Смарт-контракти є одним з найбільш поширених застосувань технології блокчейн на сьогоднішній день. Вони дозволяють виконувати угоди між сторонами автоматично, без посередників, роблячи процес швидким, прозорим і дешевшим. Саме завдяки цим перевагам смарт-контракти використовуються в широкому спектрі додатків у фінансовому секторі, страхуванні, торгівлі та системах DeFi. Але є важливий мінус: як тільки контракт поміщений на блокчейн, його вже неможливо змінити. В результаті будь-які помилки в коді залишаться назавжди і можуть призвести до значних втрат. Це пояснює, чому питання безпеки смарт-контрактів є такими важливими в наші дні.

Статистика підтверджує необхідність такого аналізу. За даними SlowMist, у 2024 році сталося 99 атак смарт-контрактів, що призвело до збитків на суму понад 214 мільйонів доларів [1]. У першій половині 2025 року ситуація погіршилася. Загалом у Web3 сталося 35 нових інцидентів із загальними збитками, що перевищили 3, 1 мільярда доларів США, більшість із яких були спричинені помилками коду [2]. Крім того, звіт Hacken показує, що лише в першій половині 2025 року недоліки в смарт-контрактах спричинили збитки на суму понад 6 мільярдів доларів [3]. Ці цифри говорять самі за себе: передчасне ігнорування автентифікації коду має катастрофічні наслідки.

Метою доповіді є розгляд статичного аналізу як одного з основних методів перевірки безпеки смарт-контрактів.

Цей метод набагато дешевше і безпечніше, ніж вирішення проблеми після завантаження системи. Статичний аналіз дозволяє виявити помилки, які найчастіше призводять до атаки: дублікати викликів функцій, цифрові переповнення або скорочення, неправильний контроль доступу, помилки в логіці виконання.

Існують спеціалізовані інструменти для реалізації цього підходу на практиці. Наприклад, Slither може швидко перевіряти контракти, написані в Solidity, і створювати докладні звіти для розробників. MythX - це комерційна хмарна платформа, інтегрована в середовище розробки, яка поєднує в собі можливості статичного та динамічного аналізу, що робить її універсальним інструментом для повної перевірки. Один із найперших інструментів – Oyente, довів, що навіть базовий аналіз коду може своєчасно виявляти критичні вразливості, включаючи атаки повторного входу [4].

Досліджуючи тестовий смарт-контракт з можливостями переказу коштів, усі три інструменти виявили різні вразливості. Slither визначив, що функція transferFunds() не перевіряє обмеження доступу, тобто будь-який користувач може її викликати, а також виявив можливість повторного виклику функції (re-entrancy) у методі withdraw(), коли зовнішні контракти можуть повторно викликати контракт до завершення виконання транзакції. MythX підтвердив ці

вразливості і додатково виявив ризик переповнення чисельної змінної у змінній balance, що може призвести до некоректного оновлення балансу користувача при великих сумах переказу. Oyente особливо акцентував на атаку повторного входу (Re-Entry) у функції withdraw(), відтворивши сценарій, коли зовнішній контракт може повторно викликати withdraw() і витягти кошти кілька разів до оновлення стану балансу.

Цей приклад показує, що інструменти статичного аналізу можуть доповнювати один одного: Slither швидко виявляє загальні помилки доступу та повторного виклику, MythX аналізує потенційні чисельні проблеми, а Oyente дозволяє моделювати конкретні сценарії атаки. Комбіноване використання цих інструментів може забезпечити більш комплексну та надійну автентифікацію для смарт-контрактів, дозволяючи розробникам закривати критичні вразливості ще до розгортання блокчейну.

Незважаючи на те що статичний аналіз не моделює фактичне виконання контракту, а складні логічні помилки можуть залишатися непоміченими та іноді створювати помилкові спрацьовування, він залишається основою для безпечної автентифікації коду. Його застосування дозволяє закрити вразливість до того, як контракт буде розгорнуто в блокчейні.

Щоб підвищити безпеку блокчейн-додатків, технології запобігання, особливо статичний аналіз, формують основу довіри до блокчейн-рішень і покращують рівень безпеки цифрових активів [5]. Статичний аналіз - це більш доступний, швидший і практичний метод, який можна застосовувати безперервно під час розробки, а не динамічне тестування та ресурсомісткі формальні перевірки. Тому його використання є необхідним етапом у створенні надійних смарт-контрактів і невід'ємною частиною комплексної стратегії захисту блокчейн-систем.

Список літератури

1. SlowMist. 2025 Mid-Year Blockchain Security and AML Report. URL: https://slowmist.medium.com/slowmist-2025-mid-year-blockchain-security-and-aml-report-3dfc535971fb

2. SlowMist. Annual Blockchain Security & AML Report 2024. URL: https://www.slowmist.com/report/2024-Blockchain-Security-and-AML-Annual-Report(EN).pdf

3. Tsankov, P., Dan, A., Drachsler-Cohen, D., Gervais, A., Buenzli, F., & Vechev, M. (2018, October). Securify: Practical security analysis of smart contracts. In Proceedings of the 2018 ACM SIGSAC conference on computer and communications security (pp. 67-82)..

4. Hacken. H1-2025 Web3 Security Report. URL: https://hacken.io/insights/q1-2025-security-report/

5. Терещенко Г. Ю., Кириченко І. В. Аналіз і обґрунтування використання наявних блокчейн-рішень для захисту цифрових активів. ХНУРЕ, 2024.

АНАЛІЗ МЕТОДІВ ПЕРЕВІРКИ ЦІЛІСНОСТІ ТА АВТЕНТИЧНОСТІ ФАЙЛІВ ЗА ДОПОМОГОЮ ГЕШ-ФУНКЦІЙ

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

У сучасних умовах, коли обсяг цифрових даних стрімко зростає, а також відбувається інтенсивний обмін файлами в інформаційних системах, важливим є забезпечення довіри до цифрових даних. Перевірка контрольних сум є одним з найпоширеніших методів підтвердження цілісності та автентичності файлів, що дозволяє швидко виявляти спроби несанкціонованої модифікації, втрати або підміни даних [1, 2].

Метою доповіді є аналіз методів перевірки цілісності та автентичності файлів за допомогою геш-функцій. Вибір алгоритму для розрахування контрольної суми залежить від мети користувача. Швидкі алгоритми – xxHash або Adler32, підходять для виявлення випадкових пошкоджень, а криптографічно стійкі алгоритми, такі як SHA256, SHA512 та новітній BLAKE3 доцільно використовувати для підтвердження автентичності [3]. Дослідження, наведені у [4], показали, що BLAKE3 підтримує багатопотокову обробку, має у 2-3 рази більшу швидкість роботи та потребує у 10 разів меншу кількість оперативної пам'яті для роботи в порівнянні з перерахованими криптостійкими алгоритмами.

Запропонований підхід полягає у першочерговому використанні високошвидкісного алгоритму xxHash для попередньої перевірки даних, а після – криптографічно стійкого BLAKE3 для верифікації критичної частки інформації. У змодельованому експерименті для масиву даних розміром 6 GB використання лише BLAKE3 зайняло близько 1.5 с, тоді як комбінована схема скоротила час до 1.23 с при застосуванні BLAKE3 до 75% даних (економія 18%) та до 0.85 с при застосуванні BLAKE3 до 50% даних (економія 43%). Таким чином, цей метод дає змогу скоротити час перевірки у порівнянні з використанням BLAKE3 для всього об'єму даних.

Проведений огляд підтверджує доцільність застосування каскадних методів, де швидкий алгоритм виконує попередню перевірку, а надійний криптографічний хеш застосовується лише до окремих критичних даних.

Список літератури

1. Моруга Д. І. Методи та алгоритми хешування паролів на платформі .NET: кваліфікаційна робота, пояснювальна записка; М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. – Харків, 2022. – 65 с.

2. Голубничий, Д.Ю., Сєвєрінов, О., Коломійцев, О.В., та інш. (2021). Аналіз сучасних загроз в інформаційних системах за складовими загроз: кібербезпеки, інформаційної безпеки та безпеки інформації.

3. Addis M. Which checksum algorithm should I use?. *DPC technology watch guidance note*. 2020. P. 1–5.

4. Pandya M. Performance evaluation of hashing algorithms on commodity hardware. *arXiv.org e-Print archive*. URL: https://arxiv.org/html/2407.08284v1.3.

АНАЛІЗ МЕТОДІВ ЗАХИСТУ ВІД ФІШИНГ-АТАКИ BRATA

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

У сучасних умовах, коли кількість мобільних користувачів та обсяг переданих даних стрімко зростають, зловмисники активно використовують вразливості у популярних застосунках для реалізації фішингових атак [1, 2]. Це створює додаткові ризики для фінансових установ і кінцевих користувачів, оскільки атака може відбутися без їхньої активної участі. Прикладом є BRATA (Brazilian Remote Access Tool for Android), яке використовувало критичну вразливість віддаленого виконання коду (RCE) CVE-2019-3568 у WhatsApp та у подальшому інтегрувало інші функції зловмисного контролю над пристроями [3].

Метою дослідження є аналіз використання CVE-2019-3568 у рамках атак BRATA та оцінка ефективності методів захисту шляхом моніторингу VoIP-трафіку і системних журналів, а також визначення можливостей прогнозування подібних атак.

Вразливість CVE-2019-3568 у VoIP-стеку WhatsApp являла собою переповнення буфера, що дозволяло віддалене виконання коду через спеціально сформовані RTCP-пакети.

Вона охоплювала кілька платформ, включаючи Android, iOS, Windows Phone та Tizen. За даними NVD, її рівень небезпеки становив 9.8 (CVSS 3.x, критичний) та 7.5 (CVSS 2.0, високий) [4].

Проведені дослідження підтвердили, що аналіз часових рядів є ефективним для вивчення динаміки фішингових атак. Виявлена наявність довготривалої пам'яті у поведінці атак відкриває можливість прогнозування пікових періодів їх активності.

Встановлено, що середнє добове зростання кількості підтверджених атак становить 3–5%, тоді як у фазах підвищеної активності сплески сягали понад 20% від середнього рівня.

Такі результати свідчать про циклічність та кореляцію у часових інтервалах і створюють підґрунтя для побудови адекватних прогнозних моделей.

На основі цих висновків вводяться практичні заходи протидії: своєчасне оновлення ПЗ до захищених версій та застосування систем аналізу VoIP-трафіку із журналами подій.

Сучасні наукові підходи демонструють ефективність поєднання методів аналізу трафіку з алгоритмами машинного навчання для створення багаторівневих систем захисту.

Щоб зменшити навантаження на сервери, інференс організують каскадно: легкі правила/моделі працюють на всьому потоці, а ресурсоємні CNN або XGBoost застосовуються лише до підозрілих подій (орієнтовно 5–15% у звичайному режимі та 30–40% під час піків завдяки автоскейлінгу). Такий підхід зберігає точність понад 99% і знижує рівень хибнопозитивних

спрацювань до 1–2%, скорочуючи середній час виявлення на 30–40% порівняно з класичними сигнатурними методами.

Додаткову економію забезпечують батчинг і черги для важких перевірок та адаптивне підвищення частоти семплювання на основі журналів VoIP-трафіку.

У тестових середовищах це підвищувало ймовірність раннього виявлення атак до 95% і знижувало ризик компрометації критичних систем на 40–50% [5].

Отримані результати свідчать, що вразливість CVE-2019-3568 є прикладом критичної проблеми безпеки, яка трансформує природу фішингових атак. Запропонований підхід, що базується на поєднанні оновлення ПЗ, моніторингу журналів, прогнозних моделей та гнучких механізмів захисту (каскадні ML-системи та інспекції «рухомого заслону»), одночасно підвищують рівень кіберзахисту та оптимізує використання серверних ресурсів.

Одночасна реєстрація аномальних RTCP-пакетів, відхилень у структурі викликів чи спроб несанкціонованих з'єднань у журналах дозволяє виявляти атаку на ранніх етапах та своєчасно реагувати.

Відповідно до проведених досліджень можна зробити висновок, що з міркувань економії серверних ресурсів доцільно реалізувати не «монолітну стіну», а «рухомий заслін» перевірок: динамічно змінювати глибину інспекції й частку вибіркового аналізу залежно від прогнозованої активності (наприклад, 5–10% семплювання у між-пікові години та 60–80% — у «вікна ризику»), автоматично масштабуючи модулі аналізу і вмикаючи повну перевірку лише під час очікуваних сплесків.

Це доводить доцільність комплексної багаторівневої стратегії, яка поєднує превентивні й реактивні заходи та дозволяє ефективніше протидіяти новітнім фішинговим атакам.

Список літератури

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

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

3. McAfee. Beware of BRATA: How to Avoid Android Malware Attack. – 2023. – URL: https://www.mcafee.com/learn/beware-of-brata-how-to-avoid-android-malware-attack/

4. NVD. CVE-2019-3568. - URL: https://nvd.nist.gov/vuln/detail/CVE-2019-3568

5. Дейнеко Ж., Драз Д. Дослідження динаміки фішингових атак методом вейвлет-аналізу // Тези доповідей 4-ї Міжнародної науково-технічної конференції «Інформаційні системи та технології» (ICT-2018), Харків, ХНУРЕ, 2018. - Секція «Захист інформації. Інформаційна безпека». - С. 396–397.

ДЕТЕКТУВАННЯ КОНЦЕПТУАЛЬНОГО ДРЕЙФУ У РЕКОНСТРУКТИВНИХ МЕТОДАХ ВИЯВЛЕННЯ ВІДХИЛЕНЬ В ПОТОКОВИХ ДАНИХ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Чала О.В., Алфьоров М.Є., Шендрик О.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Обробка потокових даних для прийняття управлінських рішень в інформаційних системах виконується в умовах суттєвих часових обмежень і тому потребує постійного моніторингу відхилень у даних [1]. Внаслідок темпоральних обмежень процедура моніторингу має виявляти відхилення патернів даних у автоматизованому режимі [2]. На сьогодні для такого виявлення використовуються реконструктивні методи, які застосовують архітектури кодувач-декодувач для відтворення нормальних патернів. Реконструктивний підхід передбачає навчання моделі відновленню вхідних даних після їх стиснення у компактне представлення. Кодувач перетворює багатовимірні вектори ознак у стислий латентний простір меншої розмірності, фіксуючи найсуттєвіші характеристики нормального функціонування системи. Декодувач виконує зворотне перетворення, намагаючись відновити оригінальні дані з латентного представлення [3]. Аномалії виявляються через аналіз помилки реконструкції: нормальні дані відновлюються з високою точністю, тоді як аномальні патерни, що не відповідають навчальній вибірці, призводять до значного зростання помилки відновлення. Застосування реконструктивних підходів обмежується такими їх особливостями: інверсією реконструкції, недиференційованістю дрейфу концепцій від справжніх аномалій та відсутністю механізмів пояснення [4]. Інверсія реконструкції полягає в тому, що автокодувальники відновлюють як нормальні, так і аномальні дані внаслідок надмірної узагальнювальної здатності латентного простору. Неможливість відрізнити дрейф концепцій призводить до високої частоти хибних спрацювань. Відсутність пояснень ускладнює підтримку ситуаційної обізнаності операторів. Таким чином, детектування концептуального дрейфу і подальше виявлення аномалій на основі реконструкції патернів вхідних потокових даних інформаційної системи є актуальною задачею.

Метою доповіді є розробка моделі, що відрізняє концептуальний дрейф від аномалій при виявленні відхилень у потокових вхідних даних інформаційної системи. Модель доповнює реконструктивні методи виявлення відхилень і використовує декомпозицію помилки відновлення даних на дві компоненти: складова систематичного концептуального дрейфу та складову локального відхилення.

Представлена в доповіді модель має такі відмінності: подвійну реконструктивну архітектуру, механізм обчислення метрики диференціації та адаптивний алгоритм встановлення порогу.

Подвійна реконструктивна архітектура складається з глобального та локального кодувачів-декодувачів. Перший навчається на повних векторах

ознак потокових даних за тривалий період спостереження, виявляє довгострокові статистичні характеристики розподілу даних та відтворює загальні патерни, включаючи систематичні зміни їх властивостей (дрейф концепцій).

Локальний кодувач-декодувач опрацьовує дані у обмежених часових вікнах для ідентифікації короткострокових відхилень.

Механізм обчислення метрики диференціації передбачає розрахунок відносної різниці помилок відновлення двох розглянутих архітектур. Глобальна помилка реконструкції розраховується як середньоквадратичне відхилення між вхідним вектором та виходом глобального декодувача. Локальна помилка визначається аналогічно для локального декодувача. Нормалізована різниця цих величин утворює індекс диференціації: значення близьке до нуля свідчить про узгодженість помилок обох архітектур, що інтерпретується як поступова зміна розподілу (концептуальний дрейф), тоді як високе значення індексу вказує на локальну аномалію.

Третя компонента реалізує адаптивне визначення порогу виявлення концептуального дрейфу з використанням експоненціального ковзного середнього з коефіцієнтом згладжування. Останній обчислюється на основі оцінки швидкості зміни розподілу даних.

Таким чином, розроблена модель забезпечує можливість розділення систематичних та випадкових компонентів помилки реконструкції у потокових даних.

Різниця між дрейфом концепцій та аномаліями визначається шляхом аналізу темпоральних характеристик похибки відновлення на різних масштабах спостереження.

Практичне значення отриманих результатів полягає у можливості виділення концептуального дрейфу і подальшого виявлення аномальних патернів даних у системах моніторингу телекомунікаційних мереж, кібербезпеки та промислового управління, що створює умови для підвищення точності детекції відхилень у режимі реального часу.

Список літератури

1. Gaber M. M., Zaslavsky A., Krishnaswamy S. Mining data streams: A review. ACM SIGMOD Record. 2005. Vol. 34, No. 2. P. 18–26. DOI: https://doi.org/10.1145/1083784.1083789

2. Lu J., Liu A., Dong F., Gu F., Gama J., Zhang G. Learning under concept drift: A review. IEEE Transactions on Knowledge and Data Engineering. 2019. Vol. 31, No. 12. P. 2346–2363. DOI: https://doi.org/10.1109/TKDE.2018.2876857

3. Hawkins S., He H., Williams G., Baxter R. Outlier detection using replicator neural networks. DaWaK 2002: Data Warehousing and Knowledge Discovery. 2002. P. 170–180. DOI: https://doi.org/10.1007/3-540-46145-0_17

4. Zhou C., Paffenroth R. C. Anomaly detection with robust deep autoencoders. Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. 2017. P. 665–674. DOI: https://doi.org/10.1145/3097983.3098052

МЕТОДИКА ОЦІНЮВАННЯ ДОСТОВІРНОСТІ ВІДПОВІДЕЙ МОВНИХ МОДЕЛЕЙ У КОНТЕКСТІ ВЕКТОРНОГО ПОШУКУ

Альошин Я.М.
Національний аерокосмічний університет
«Харківський авіаційний інститут», Харків, Україна

Сучасні мовні моделі, зокрема ті, що лежать в основі GPT-архітектури, значно розширили можливості інформаційного пошуку, аналітики та підтримки прийняття рішень. Вони забезпечують високу швидкість і гнучкість обробки текстових даних, однак водночас створюють ризик появи недостовірних або «галюцинованих» відповідей, що виглядають логічно, але не відповідають фактам.

Проблема достовірності особливо загострюється в умовах векторного пошуку, де релевантність формується не лише за ключовими словами, а за семантичною подібністю між запитом і текстом. Хоча векторні моделі надають змогу віднаходити глибокі змістові зв'язки, вони не забезпечують перевірку фактичної точності.

Векторний пошук базується на векторних поданнях текстів у багатовимірному семантичному просторі, де кожен документ або запит перетворюється на числовий вектор.

Для визначення схожості між об'єктами використовують метрики, найчастіше косинусну, євклідову, або мангеттенську відстань, що дозволяють встановлювати смислову спорідненість навіть без точного збігу термінів. Проте, висока семантична подібність не гарантує фактологічної коректності, тому доцільно поєднувати векторні методи з системами автоматизованої перевірки фактів.

Достовірність відповідей мовних моделей визначається низкою факторів: якістю навчального корпусу, рівнем контекстуалізації даних, наявністю механізмів перевірки фактів та інтерпретаційних помилок користувача під час формування запиту (prompt engineering).

Основними типами порушень достовірності є фактологічні помилки, логічні суперечності, хибні узагальнення та неповні висновки. У контексті векторного пошуку ці помилки ускладнюють автоматичне оцінювання якості відповіді, оскільки навіть високі показники семантичної відповідності не гарантують фактологічної правдивості [1, с. 324].

У доповіді викладено методику комплексного оцінювання відповіді, а саме: семантичної відповідності, що визначається за векторною близькістю між запитом і відповіддю; шляхом фактологічної перевірки, тобто зіставленням тверджень із достовірними джерелами або базами знань; логічною узгодженістю, що передбачає аналіз відсутності суперечностей і збереження причинно-наслідкових зв'язків [2, с. 526].

При цьому на кожному етапі методики формується часткова оцінка, а згодом розраховується інтегральний показник достовірності (Confidence Index, CI) за формулою:

$$CI=\alpha S+\beta F+\gamma L,$$

де S – семантична близькість, F – фактологічна точність, L – логічна узгодженість, а коефіцієнти α,β,γ визначають вагу кожного критерію (оптимальне співвідношення – 0.4 : 0.4 : 0.2).

Технологія оцінювання достовірності відповідей мовних моделей на основі зазначеної методики складається з трьох етапів. На етапі пошуку запит перетворюється у векторну форму, після чого виконується пошук релевантних документів у базі знань.

На етапі генерації модель формує відповідь на основі знайденого контенту за принципом Retrieval-Augmented Generation. На етапі верифікації відбувається обчислення векторної схожості між відповіддю та джерелами, автоматична перевірка фактів через бази даних (Wikidata, DBpedia, CrossRef) й логіко-семантичний аналіз із використанням моделей Natural Language Inference (NLI). Далі усі результати інтегруються в єдиний показник, що дозволяє ідентифікувати відповіді як достовірні, частково достовірні або недостовірні.

Апробація методики на корпусі понад 10 тисяч запитів показала середній індекс достовірності (CI): GPT-4 – 0,87, GPT-3.5 – 0,74, LLaMA-3 – 0,69. Найбільше похибок виникало у запитах з нечітким контекстом. Поєднання автоматичного фактчекінгу з експертною оцінкою підвищило точність результатів на 10–12 %, що підтвердило ефективність підходу [3, с. 96].

Подальші дослідження варто зосередити на гібридних системах перевірки, які поєднують векторний пошук із динамічними базами знань, а також на використанні нейросемантичних моделей і контрастивного навчання для точнішої оцінки достовірності.

Важливо дотримуватись принципів прозорості, відтворюваності та підзвітності, що забезпечить застосування методики у сферах, критичних до точності – освіті, медицині, праві та аналітиці [4].

Список літератури

1. Рудніцький Я. Е. Штучний інтелект в освіті: ChatGPT як ключовий інструмент для покращення навчання здобувачів освіти. Українські студії в європейському контексті, 2023. № 7. С. 324–327.

2. Сікора Я. Б., Марчук Н. А., Нестеров В. Ф. Технології майбутнього: роль штучного інтелекту у персоналізованому навчанні. Наука і техніка, 2024. № 1. С. 526–537.

3. Ткаченко К. Використання методів NLP в інтелектуальних навчальних системах. Цифрова платформа: інформаційні технології в соціокультурній сфері, 2024. Т. 7, № 1. С. 80-96.

4. Ashish V., Noam S., Niki P., Jakob U., Llion J., Aidan N. G., Lukasz K., Illia P. Attention Is All You Need, 2017. URL: https://arxiv.org/abs/1706.03762 (дата звернення: 22.05.2025.)

АГРЕГАЦІЯ ПОЯСНЮВАНИХ МЕТОДІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ ІНТЕРПРЕТАЦІЙ ШТУЧНОГО ІНТЕЛЕКТУ

Хміль О.С., Феоктистова О.І.
Національний аерокосмічний університет
«Харківський авіаційний інститут», Харків, Україна

Використання штучного інтелекту (ШІ) у програмних додатках потребує впевненості та довіри до його роботи з технічної точки зору. Галузь пояснюваного штучного інтелекту покликана вирішити цю проблему шляхом створення інтерпретацій процесу розмірковування у складних моделях. Однак питання надійності таких пояснень часто залишається поза увагою під час розроблення систем штучного інтелекту. На практиці ж необхідно забезпечити надійність використовуваних методів і технік, одним із ключових факторів якої є стійкість.

У доповіді розглянуто можливість підвищення стійкості пояснюваних методів за допомогою агрегації результатів застосування кількох підходів. Такий підхід спрямований на усунення проблеми розбіжностей між поясненнями, отриманими різними методами. При цьому є можливість врахування ситуацій, коли одночасно аналізується кілька процесів прийняття рішень.

Перевірку достовірності агрегованих пояснень проведено для трьох моделей: методу k-найближчих сусідів, випадкового лісу та нейронних мереж.

Результати свідчать про доцільність використання багатомодельної агрегації для підвищення надійності пояснень.

Стійкість пояснюваного методу визначається як здатність відтворювати однакові або подібні результати за незмінних вхідних даних. Варто зазначити, що популярні методи, такі як LIME і SHAP, продемонстрували низький рівень надійності у роботі [1].

Слід розрізняти стійкість до зміни розподілу вхідних даних та стійкість до атак, тобто здатність моделі протистояти навмисним зловмисним змінам без спотворення прогнозів [2].

В рамках проведеного дослідження розглядається лише перший тип стійкості.

Додатковою проблемою при використанні кількох методів одночасно є розбіжність пояснень − ситуація, коли різні методи, застосовані до однієї й тієї ж моделі, повертають суттєво відмінні результати [3].

Запропонований підхід складається з таких етапів:

1. Оцінка важливості ознак для кожної моделі.
2. Створення єдиної інтерпретації через нормалізацію та об’єднання векторів атрибуції ознак за допомогою арифметичного середнього.
3. Оцінка стійкості кожного пояснення (індивідуального та агрегованого) шляхом порівняння атрибуцій ознак за методом, описаним у роботі [4].

Для методу k-найближчих сусідів важливість ознак обчислювалася як різниця середніх відстаней за ознаками між точкою інтересу та об'єктами з того самого і протилежного класів (після нормалізації).

Для методу випадкового лісу оцінювалося, наскільки кожна ознака сприяє зменшенню невизначеності на кожному розбитті дерева, з урахуванням вагування за ймовірностями прогнозу для різних класів.

Для нейронної мережі атрибуції ознак були отримані за допомогою методу DeepLIFT [5].

Запропонований підхід протестовано на чотирьох відкритих наборах даних для задач класифікації.

Попередня обробка даних включала стандартизацію числових змінних, кодування категоріальних, а також видалення ознак із високою кореляцією.

Кожен набір даних було розділено на тренувальну, валідаційну та тестову вибірки.

Результати дослідження показали, що застосування нейронних мережі та метод випадкового лісу для організації пояснень надають змогу досягти більш високої точності та стабільності.

Причому нейронні мережі краще працюють на складних наборах даних, а метод випадкового лісу – на простіших.

При поєднанні пояснень з усіх трьох моделей агрегований підхід дає показники стійкості, які знаходяться між окремими моделями, але загалом залишаються більш послідовними.

Аналіз показав, що прогнози узгоджуються у тих областях даних, де пояснення є найбільш стійкими.

Список літератури

1. D. Alvarez-Melis, T. Jaakkola, On the robustness of interpretability methods, 2018. 10.48550/arXiv.1806.08049.

2. Reyes-Amezcua, Ivan & Ochoa-Ruiz, Gilberto & Mendez-Vazquez, Andres. (2023). Adversarial Robustness on Artificial Intelligence. 10.1201/b23345-24.

3. S. Krishna, T. Han, A. Gu, S. Wu, S. Jabbari, H. Lakkaraju, The disagreement problem in explainable machine learning: A practitioner's perspective, Transactions on Machine Learning Research (2024) 10.21203/rs.3.rs-2963888/v1.

4. I. Vascotto, A. Rodriguez, A. Bonaita, L. Bortolussi, When can you trust your explanations? A robustness analysis on feature importances, 2025. arXiv:2406.14349.

5. A. Shrikumar, P. Greenside, A. Kundaje, Learning important features through propagating activation differences, 34th International Conference on Machine Learning, ICML 2017 7 (2017) 4844–4866. https://dl.acm.org/doi/10.5555/3305890.3306006.

БЛОКЧЕЙН-ОРІЄНТОВАНІ МОДЕЛІ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ У КОРПОРАТИВНИХ СИСТЕМАХ СОФТВЕРНИХ ФІРМ

Єрьоменко А.Д., Феоктистова О.І.
Національний аерокосмічний університет
«Харківський авіаційний інститут», Харків, Україна

У доповіді розглянуто застосування технології блокчейн як сучасного інструмента забезпечення конфіденційності даних у корпоративних інформаційних системах софтверних компаній. Показано, що традиційні централізовані моделі контролю доступу характеризуються низкою обмежень, особливо в умовах високої динаміки ролей, розподіленості бізнес-процесів та зростання внутрішніх загроз.

Класичні моделі, зокрема Белла-ЛаПадули, Брюера-Наша та Кларка-Вілсона, не повною мірою відповідають вимогам гнучкості та прозорості у багатокористувацьких середовищах [1, 2].

Запропоновано концепцію інтеграції блокчейн-технологій у механізми управління доступом, яка передбачає поєднання трьох ключових складових: permissioned-блокчейну, токенізації доступу та розподіленого зберігання криптографічних ключів.

При цьому Permissioned-мережі забезпечують контрольований доступ до даних, незмінність записів та аудит дій користувачів у режимі реального часу, токенізація дозволяє впровадити персоналізоване, контекстно-залежне й часово обмежене надання прав доступу, а розподілене управління ключами мінімізує ризики одноосібного контролю і суттєво знижує вразливість до компрометації ключової інформації. Організація функціонування корпоративних систем на основі зазначеної концепції підвищить ефективність бізнес процесів за рахунок підвищення рівню довіри між учасниками внутрішніх та міжорганізаційних взаємодій, забезпечить прозорість процесів діловодства і знизить ризик зловживань.

Інтеграція блокчейну у корпоративну інфраструктуру породжує низку прикладних проблем, пов’язаних, зокрема, з масштабованістю, затримками підтвердження транзакцій, енергоспоживанням окремих консенсус-алгоритмів та необхідністю адаптації до правових обмежень (зокрема вимог GDPR щодо «права на забуття»).

Список літератури

1. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. – 2nd ed. – New York : John Wiley & Sons, 1996. – 758 c.

2. Carbo D. Don’t Just Rely On Data Privacy Laws to Protect Information [Електронний ресурс]. – 2020. – Режим доступу: https://www.securitymagazine.com/articles/91775-dont-just-rely-on-data-privacy-laws-to-protect-information (дата звернення: 15.08.2025).

СЕКЦІЯ 7
СУЧАСНІ ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНІ СИСТЕМИ

Керівник секції: д.т.н. проф. О. В. Коломійцев, НТУ «ХПІ», Харків
Секретар секції: к.т.н. доц. А. О. Подорожняк, НТУ «ХПІ», Харків

MULTIMODAL FUSION METHODOLOGY FOR DETECTING VISUALLY INVISIBLE TARGETS ON UAV PLATFORMS

Atayev S.U.
Lankaran State University, Lankaran, Azerbaijan
Hasanov A.H., Hashimov E.G.
National Defense University, Baku, Azerbaijan

The problem of detecting targets that are invisible in the visual band on UAV platforms is not reliably solvable by classical optical methods due to camouflage, poor illumination, dust and smoke. The proposed methodology relies on multimodal sensor fusion and aims to form dependable situational awareness under real time constraints. The architecture projects inputs RGB and thermal cameras, a small form factor synthetic aperture radar, a multispectral module, a lightweight LiDAR, and passive RF observation using a software defined radio receiver into a unified reference frame. Through intrinsic and extrinsic calibration and orthorectification, all channels are geospatially aligned. LiDAR data are registered with NDT or ICP, SAR frames are focused and georeferenced, and the RF energy map is rasterized. This stage minimizes residual biases in sensor registration and provides a stable basis for probability-based fusion. In the feature extraction block, channel specific methods are selected. For SAR, CFAR families that account for heterogeneous backgrounds are employed together with texture and polarimetric descriptors. In the multispectral channel, PCA or MNF is used for dimensionality reduction, followed by an RX anomaly detector to expose deviations in material signatures. In the optical thermal pair, both early and late fusion strategies are explored, which enhances complementarity at night and in low visibility. In passive RF observation, clustering of narrowband stationary components yields prior regions that indicate electronic activity and enables selective allocation of computer resources.

The probabilistic fusion is formulated as integration of calibrated per channel probabilities using a product rule. Spatial proximity is modeled with a Markov type influence field, and cross channel dependencies are regularized with penalty terms when the conditional independence assumption is violated. Candidate detections are cleaned with non-maximum suppression, and temporal continuity is maintained with a Kalman filter or multi hypothesis tracking. The resulting fused probability heat map at the end of the chain provides a decision surface that is friendly to both visualization and computation. To satisfy real time requirements, architecture employs several optimization mechanisms. Model quantization and specialized acceleration libraries reduce computational load. Thanks to region of interest

processing, only probability rich parts of a frame undergo deeper processing. For SAR, subframes in stripmap mode keep latency within a controlled range. A representative compute budget can be allocated so that initial detection completes within 50 to 120 milliseconds, probability fusion within 20 to 40 milliseconds, and tracking within 10 to 20 milliseconds. These figures are scaled with platform payload capacity, energy budget, and flight profile.

The operational effect of the methodology is that the complementary nature of channels in heterogeneous backgrounds increases probability of detection and reduces false alarms. In vegetation and dusty environments SAR priors emphasize surface structure, at night and in smoke thermal imagery provides contrast, for material discrimination the multispectral channel separates spectral signatures, and passive RF contributes indirect cues of electronic presence. Residual registration errors, GNSS limitations, and platform vibration can introduce bias in fusion. Therefore, adaptive parameterization with respect to terrain, altitude, and meteorological conditions is integral to the approach. Safe operation also considers the balance between computing and energy, as well as tuning of latency and compression parameters for data links. The modular framework can be adapted to different sensor configurations and mission needs. Future work will address neuromorphic event cameras, semi supervised learning with few labels, and 3D anomaly detection at the SAR LiDAR interface, providing an efficient and realistic solution for detecting visually invisible objects on UAVs.

References

1. Bayramov A.A. eta l. Unmanned Aerial Vehicle Applications for Military GIS Task Solutions //Research Anthology on Reliability and Safety in Aviation Systems, Spacecraft, and Air Transport. – IGI Global Scientific Publishing, 2021. – С. 1092-1115.

2. Muradov, S.A. (2023). Development prospects of beacon systems. *In* Problems of informatization. Vol. 1. p.31.

3. Muradov, S.A. et al. (2023, November). Determining the location of the UAV equipped with a homing device based on radio beacons. In *Modeling, Control and Information Technologies: Proc. of International scientific and practical conference* (No. 6, pp. 54-56).

4. Bayramov A.A. The numerical estimation method of a task success of UAV reconnaissance flight in mountainous battle condition //Сучасні інформаційні системи. – 2017. – №. 1,№ 2. – С. 70-73.

5. Hashimov E., Khaligov G. The issue of training of the neural network for drone detection //Advanced Information Systems. – 2024. – Т. 8. – №. 3. – С. 53-58.

6. 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.

7.Ganimat I. B. Analysis and selection performance indicators multiservice communication networks based on the concept NGN and FN //Computer and information systems and technologies. – 2021.

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

9. Bayramov A.A. Assessment of invisible areas and military objects in mountainous terrain //Defence Science Journal. – 2018. – Т. 68. – №. 4. – С. 343-346.

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

METHODOLOGY AND APPLICATIONS OF AI ENABLED IMAGE RECOGNITION IN UAVS

Balayev F.R.
Baku State University, Baku, Azerbaijan
Hasanov A.H., Hashimov E.G.
National Defense University, Baku, Azerbaijan

This paper provides a systematic examination of artificial intelligence integration for image recognition on unmanned aerial vehicles, covering methodology, application domains, and operational implications. The motivation is the need to secure information superiority by reducing the sensing to decision latency while maintaining accuracy and resilience in contested environments. We propose an end-to-end Edge AI pipeline that runs entirely on the platform and combines multisensor inputs with optimized deep learning models. The architecture comprises five sequential stages: sensor acquisition from EO IR and SAR payloads, preprocessing for compression and normalization, object detection and tracking using configurable families such as YOLO, Faster R CNN, and DETR paired with DeepSORT, human in the loop validation for accountability, and mission management that route confirmed detections to navigation and payload subsystems. The design emphasizes real time operation on GPU or NPU based system on chip modules with strict energy budgets.

Dataset construction follows three principles. First, domain relevance through acquisition in mountainous and urban terrains at varied altitudes and illumination. Second, interoperable labeling using COCO and VOC formats with classes such as armored vehicles, artillery, air defense, logistics vehicles, and personnel. Third, robust splits and class balance using a 70 15 15 partition with focal loss and targeted relabeling when necessary. Performance is evaluated by four axes. Accuracy uses mAP@[0.5:0.95], F1 score, false alarm rate, and ID switch count for tracking. Speed is measured as end-to-end latency and frames per second with a target below 50 ms total latency. Energy efficiency is quantified as joules per frame, where quantization and pruning yield 20 to 35 percent savings. Reliability is assessed under fog, night, urban clutter, camouflage, communications degradation, and GNSS spoofing.

Experimental results demonstrate the inherent speed accuracy trade off. A quantized YOLO S achieves roughly 35 FPS with mAP near 0.55, YOLO M improves accuracy to about 0.62 at 22 FPS, while Faster R CNN reaches mAP near 0.64 with only 8 FPS.

These findings support a configurable model portfolio where mission requirements and onboard compute define the operating point. Multisensor fusion at the AI level reduces false positives by 18 to 27 percent when EO IR and SAR are jointly exploited, which is especially beneficial at night and in low visibility. A representative latency profile allocates 8 to 12 ms to sensor and preprocessing, 15 to 28 ms to inference, and 5 to 10 ms to post processing, remaining under the 50 ms threshold. Thermal headroom in hot climates emerges as a practical constraint that motivates improved heat sinking and dynamic frequency scaling.

Operationally, AI enabled image recognition shortens the reconnaissance to strike cycle, improves fires accuracy, and reduces operator workload, but it also introduces risk factors. Adversarial camouflage can induce spurious detections, GNSS spoofing can perturb guidance, and data links can be degraded by electronic attack.

Mitigations include multichannel verification, behavior level anomaly detection, strict application of Identification Friend or Foe rules, and audit logs for post mission accountability. The human in the loop principle remains central for ethical and lawful use.

For Azerbaijan, priorities include building national datasets, producing localized Edge AI modules, conducting phased range testing, and establishing a university industry military cooperation ecosystem.

These efforts align technical progress with standardization and doctrine. In sum, integrating AI based image recognition on UAVs is a viable path to enhanced operational capability when real time Edge AI, multisensor fusion, and model optimization are co-designed with ethical governance.

References

1. Bayramov A.A. eta l. Unmanned Aerial Vehicle Applications for Military GIS Task Solutions //Research Anthology on Reliability and Safety in Aviation Systems, Spacecraft, and Air Transport. – IGI Global Scientific Publishing, 2021. – С. 1092-1115.

2. Muradov, S.A. (2023). Development prospects of beacon systems. *In* Problems of informatization. Vol. 1. p.31.

3. Muradov, S.A. et al. (2023, November). Determining the location of the UAV equipped with a homing device based on radio beacons. In *Modeling, Control and Information Technologies: Proceedings of International scientific and practical conference* (No. 6, pp. 54-56).

4. Bayramov A.A. The numerical estimation method of a task success of UAV reconnaissance flight in mountainous battle condition //Сучасні інформаційні системи. – 2017. – №. 1, № 2. – С. 70-73.

5. Hashimov E., Khaligov G. The issue of training of the neural network for drone detection //Advanced Information Systems. – 2024. – Т. 8. – №. 3. – С. 53-58.

6. 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.

7. Ganimat I. B. Analysis and selection performance indicators multiservice communication networks based on the concept NGN and FN //Computer and information systems and technologies. – 2021.

8. Nasibov Y. A. et al. Modelling of the rationally deployment of observing systems //Сучасні інформаційні системи. – 2019. – №. 3, № 2. – С. 10-13.

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

10. Bayramov A.A. Assessment of invisible areas and military objects in mountainous terrain //Defence Science Journal. – 2018. – Т. 68. – №. 4. – С. 343-346.

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

RESEARCH ON THE EFFICIENCY PASSIVE OPTICAL NETWORKS

Ibrahimov B.G.
Azerbaijan Technical University, Baku, Azerbaijan
National Defense University, Baku, Azerbaijan
Javadova M.M.
Azerbaijan Construction and Architecture University, Baku, Azerbaijan

The current use optical technologies in building optical telecommunications networks poses a number of challenges and questions for optical equipment developers.

Addressing these challenges is impossible without modern research into optical technologies such as:

– all-optical networks (AON),
– WDM (Wavelength Division Multiplexing),
– DWDM (Dense WDM),
– passive optical networks (PON).

AON technology is a rapidly developing and one of the most promising technologies for high-speed multi-service multiple access over optical fiber, which meets the above requirements.

An AON is a network that uses only optical technologies for switching, multiplexing, and signal retransmission. This means that an all-optical network eliminates the need to convert signals from electrical to optical and back.Transmission of heterogeneous traffic in PON can be implemented using either TDMA (Time Division Multiple Access) or frequency division multiplexing WDM.

Research shows that PON technology offers several advantages:

– minimizes optical fiber lengths;
– provides high-speed bandwidth (up to 10 Gbps);
– provides broadcast capabilities, which is efficient for transmitting digital or analog video;
– eliminates the need for active multiplexers at branch points, simplifying maintenance and minimizing energy costs;
– reduces the cost of onboarding new subscribers;
– reduces network management;
– ncreases the distance over which data can be transmitted;
– eliminates the need for future upgrades.

A passive optical network is an optical access architecture that provides transmission of network traffic (voice, data and video) of various classes between OLT (Optical Line Terminal) and subscriber nodes ONU (Optical Network Unit) without using active optical-electronic components.

To transmit data, PONs use passive optical splitters/combiners (PO-SCs). The PO-SC transmits downstream traffic from the OLT to the ONU and upstream traffic from the ONU to the OLT via fiber optics.

The general PON architecture is shown in Fig. 1.

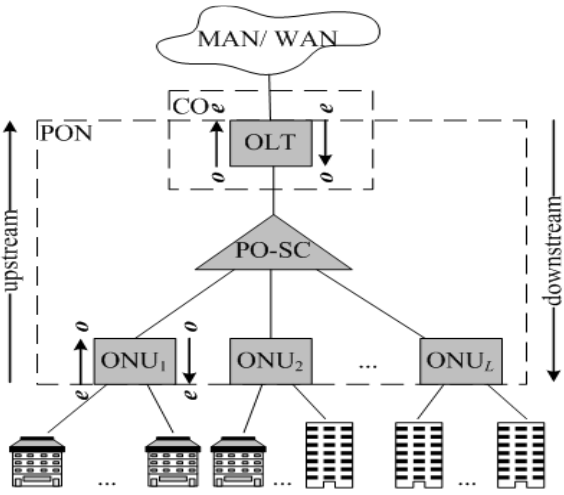

Fig. 1. General architecture of a passive optical network

As can be seen from Fig. 1, the linear terminal is located in the CO, (Central Office), thereby connecting the passive optical network with the urban regional MAN (Metropolitan Area Network), with the global network WAN, (Wide Area Network).

References

1.Ibrahimov, B.G., et al. (2021). Research and analysis efficiency fiber optical communication lines using quantum technology. *T-Comm-Телекоммуникации и Транспорт*, *15*(10), 50-54.

2. Hasanov M. H. et al. Research and analysis performance indicators NGN/IMS networks in the transmission multimedia traffic. *In* 2019 Wave Electronics and its Application in Information and Telecommunication Systems, 2019. – С. 1-4.

3. Ibrahimov B. G., Huseynov F. I. Research and analysis mathematical model for evaluating noise immunity in telecommunication system //Synchroinfo journal. – 2020. – Т. 6. – №. 1. – С. 2-6.

4.Hasanov, A.H. et al. Comparative analysis of the efficiency of various energy storages. Kharkov: Advanced Information Systems. 2023. Vol. 7, №. 3, pp.74-80.

5.Ibrahimov, B.,Islamov, I. (2024, October). Research and Analysis of the Efficiency of Fiber-Optic Communication Lines Based on DWDM Systems. In *The International Symposium for Production Research* (pp. 81-91). Cham: Springer Nature Switzerland.

6. Ganimat I. B., Qiyas H. E. Analysis and selection performance indicators multiservice communication networks based on the concept NGN and FN //Computer and information systems and technologies. – 2021.

7. Zulfugarov B. et al.Comparative analysis of the efficiency of various energy storages //Modeling, Control and Information Technologies: Proceedings of International scientific and practical conference. – 2023. – №. 6. – С. 42-45.

8. İbrahimov, B.G., Hashimov, E.G. Research and analysis of fiber-optic communication lines based on wave multiplexing technology. *İn* Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. -2023, Том 2: - pp.4-5.

DYNAMIC CONTROL AND ROUTE OPTIMIZATION FOR UAV FLIGHT SAFETY AND RESOURCE EFFICIENCY

Kondrashin İ.K.
National Aviation Academy, Baku, Azerbaijan

This paper presents an integrated framework for modeling and controlling Unmanned Aerial Vehicles that couples six degrees of freedom flight dynamics with route planning, wind turbulence modeling, and actuator and sensor nonidealities in a single simulation environment. The objective is to improve trajectory tracking accuracy and energy efficiency under realistic constraints that include meteorological disturbances, payload variation, and computation and actuation limits, while preserving safety and feasibility. The flight dynamics are represented by a nonlinear state space model with translational and rotational equations of motion expressed in the body frame and mapped to the Earth frame through standard kinematic transformations. Aerodynamic forces and moments are modeled with quasi linear dependences on speed, angle of attack, angular rates, and control surface deflections, and include thrust and gravity. Atmospheric turbulence is captured by the Dryden spectral model implemented through continuous time shaping filters and projected onto the body axes; parameter sets are selected by altitude and terrain class.

Two feedback strategies are evaluated side by side: Linear Quadratic Regulation for linearized operating points and Model Predictive Control with explicit state and input constraints. The MPC formulation uses finite horizons and quadratic objectives on tracking errors and control increments, while respecting amplitude and rate limits on actuator commands and envelope constraints on attitude. For guidance, the framework integrates a route planner that merges Rapidly exploring Random Tree Star graphs with Dubins path segments. The planner first explores free space to build a topologically feasible route, then replaces piecewise straight and turning segments with curvature constrained arcs that satisfy minimum turning radius and heading continuity. This hybrid planning approach reduces conflicts between kinematic feasibility and control authority and lowers the frequency of near saturation events in closed loops.

Identification and calibration are performed with flight telemetry through subspace and ARX based methods, with cross validation between sessions to ensure parameter consistency.

Sensor models include Gaussian noise, bias drift, and discretization effects for inertial and satellite navigation units. Actuators are represented by first order dynamics with amplitude and slew rate limits; delays in the loop include sampling and computation time.

The framework is implemented in MATLAB Simulink and Python with ROS and Gazebo for agent level behaviors and STK for communication geometry and flight envelopes. Evaluation metrics include root mean square path deviation, attitude error, an energy proxy formed by the one norm of inputs over time, median decision or computation delay, and violation counts for amplitude and rate constraints.

Simulation campaigns covered multiple wind levels and payload shifts that moved the center of gravity. MPC achieved lower tracking error and peak deviation when constraints were active and nonlinearities were strong, at higher computational cost, while LQR was competitive in benign profiles and less sensitive to delay. Both controllers remained stable under Dryden perturbations, and integrating planning with control reduced curvature mismatches and actuator rate-limit violations. Sensitivity and ablation studies supported turbulence modeling and careful gain tuning to limit overshoot without raising control effort.

The proposed framework contributes to a reproducible workflow that connects high fidelity dynamics, realistic wind and sensing, constraint aware control, and curvature constrained planning.

The approach enhances safety and resource efficiency and provides a clear path to hardware in the loop and flight validation.

Future work will extend the aerodynamic model with data driven refinements and computational fluid dynamics, consider non-Gaussian gusts, optimize real time code generation, and generalize the planner and controller to cooperative multi-UAV missions.

References

1. Bayramov A.A. eta l. Unmanned Aerial Vehicle Applications for Military GIS Task Solutions //Research Anthology on Reliability and Safety in Aviation Systems, Spacecraft, and Air Transport. – IGI Global Scientific Publishing, 2021. – С. 1092-1115.

2. Muradov, S.A. (2023). Development prospects of beacon systems. *In* Problems of informatization. Vol. 1. p.31.

3. Muradov, S.A. et al. (2023, November). Determining the location of the UAV equipped with a homing device based on radio beacons. In *Modeling, Control and Information Technologies: Proceedings of International scientific and practical conference* (No. 6, pp. 54-56).

4. Bayramov A.A. The numerical estimation method of a task success of UAV reconnaissance flight in mountainous battle condition //Сучасні інформаційні системи. – 2017. – №. 1,№ 2. – С. 70-73.

5. Hashimov E., Khaligov G. The issue of training of the neural network for drone detection //Advanced Information Systems. – 2024. – Т. 8. – №. 3. – С. 53-58.

6. 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.

7. Ganimat I. B. Analysis and selection performance indicators multiservice communication networks based on the concept NGN and FN //Computer and information systems and technologies. – 2021.

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

9. Bayramov A.A. Assessment of invisible areas and military objects in mountainous terrain //Defence Science Journal. – 2018. – Т. 68. – №. 4. – С. 343-346.

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

AI ASSISTED CONTROL MODEL FOR STRIKE UAV SWARMS

Kovalev V.A.
National Aviation Academy, Baku, Azerbaijan
İsmayıl İ., Bakshali V.İ., Hashimov E.G.
Azerbaijan Technical University, Baku, Azerbaijan

The article proposes a unified, multi-level framework for the mathematical modeling of the swarm employment of strike unmanned aerial vehicles. The aim is to develop an integrated set of models that combine coordinated flight, self-organization, target allocation, and decision making in a UAV swarm that executes reconnaissance, target detection, prioritization, and neutralization within the same operational cycle. The approach comparatively accounts for centralized and decentralized control architectures and seeks enhance resilience in combat environments characterized by communication disruptions, latency, electromagnetic interference, and attrition. The proposed framework systematically integrates bio-inspired coordination rules, optimization methods, and AI-based adaptive control, which increases operational agility and improves the effectiveness of saturation, diversion, and dispersed strike scenarios.

The mathematical core consists of four synthesized modules. In the first module, coordinated motion is achieved through particle swarm optimization, Lloyd relaxation, and multicomponent vector fields to preserve formation, avoid collisions, and bypass obstacles. In the second module, self-organization is modeled using Van Loon-type elliptical formations, Lotka Volterra interaction dynamics, and bio-inspired methods such as ant colony optimization, bee swarm algorithms, and genetic algorithms. The third module establishes control by means of a multi-agent approach, consensus rules, and virtual structures, ensuring the execution of flight trajectories, swarm formation, and group tasks in leader-based or leaderless schemes. In the fourth module, target allocation and resource distribution are solved with optimal decisions through the multi-knapsack problem, assignment algorithms, and heuristics enhanced by deep learning. In the target recognition block, visual identification is performed with convolutional neural networks, while sensor fusion integrates data using Kalman filters and nonlinear variants. These modules are unified on a system of objective functions, constraints, and multi-criteria goals that mathematically link operational functions.

The computational solution addresses near real-time processing requirements. Model reduction, lightweight neural architectures, offboard or edge computing, and event-driven updates reduce latency. Agent-level behaviors are simulated in ROS and Gazebo, control loops in MATLAB Simulink, and flight dynamics and communication maps in the STK suite. Key measures are defined for evaluation. These include mission success probability, median decision time, convergence time under obstacle density, packet loss tolerance threshold, target saturation ratio, energy consumption, and resilience to attrition. Test scenarios cover saturated air attack, distributed air attack, and SEAD-type operations. Under spectrum jamming and GPS degradation, decentralized consensus rules are observed to keep decision times

stable, while virtual structures improve formation stability in high obstacle density. A deep learning enhanced target allocation module, together with the multi-knapsack formulation, accelerates resource distribution and facilitates the synchronization of parallel strike windows.

The proposed framework offers three practical advantages.

First, standardized interfaces between model blocks enable reusability when UAV platforms and sensor configurations change.

Second, decentralized rules designed with communication constraints in mind preserve swarm integrity during network fragmentation.

Third, tuning of multi-criteria objectives enables policy-level trade-offs between strike effectiveness, loss risk, and energy consumption. Limitations include the difficulty of parameterizing models in real environments, the need for counter-learning measures against adversaries, and the challenge of cyber resilience.

Future work should focus on validating lightweight, adaptive, and explainable AI models through field trials, strengthening the communications architecture with elastic spectrum management, and verifying simulation results across multiple scenarios on real UAV platforms. Overall, the combined application of classical optimization and artificial intelligence expands the employment envelope of strike UAV swarms in modern warfare and simultaneously increases operational effectiveness and resilience.

References

1. Muradov, S.A. et al. (2023, November). Determining the location of the UAV equipped with a homing device based on radio beacons. In *Modeling, Control and Information Technologies: Proceedings of International scientific and practical conference* (No. 6, pp. 54-56).

2. Bayramov A.A. The numerical estimation method of a task success of UAV reconnaissance flight in mountainous battle condition //Сучасні інформаційні системи. – 2017. – №. 1,№ 2. – С. 70-73.

3. Muradov, S.A. (2023). Development prospects of beacon systems. *In* Problems of informatization. Vol. 1. p.31.

4. Hashimov E., Khaligov G. The issue of training of the neural network for drone detection //Advanced Information Systems. – 2024. – Т. 8. – №. 3. – С. 53-58.

5. 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.

6. Ganimat I. B. Analysis and selection performance indicators multiservice communication networks based on the concept NGN and FN //Computer and information systems and technologies. – 2021.

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

8. Bayramov A.A. Assessment of invisible areas and military objects in mountainous terrain //Defence Science Journal. – 2018. – Т. 68. – №. 4. – С. 343-346.

9. Bayramov A.A. eta l. Unmanned Aerial Vehicle Applications for Military GIS Task Solutions //Research Anthology on Reliability and Safety in Aviation Systems, Spacecraft, and Air Transport. – IGI Global Scientific Publishing, 2021. – С. 1092-1115.

METHODOLOGY AND APPLICATIONS OF AI ENABLED IMAGE RECOGNITION IN UAVS

Malahov G.H.
Baku State University, Baku, Azerbaijan

This paper assesses high frequency electromagnetic fields as a non-kinetic means for disrupting coordinated drone swarms and situates their performance within an operational and regulatory framework. The motivation arises from the rapid diffusion of autonomous, AI enabled swarms that combine low cost, agility, and resilience through distributed control. Conventional countermeasures such as nets, lasers, short range missiles, and small arms scale poorly against numerous and fast-moving platforms and may raise unacceptable collateral risks in urban airspace. Electromagnetic approaches address information dependencies rather than physical structures by degrading communication, navigation, and consensus formation, which are necessary for swarm coherence.

The study adopts a mixed methods design that integrates expert knowledge and broad professional judgment. Qualitative evidence comes from in depth interviews with 15 specialists in military operations, cybersecurity, drone engineering, and electronic warfare. These interviews have map field constraints, electromagnetic compatibility requirements, safety interlocks, and command integration. Quantitative evidence comes from a structured survey of 405 professionals across military and civilian sectors. Respondents provide comparative judgments on the relative effectiveness of GPS denial, protocol specific disruption, sweep jamming, and reactive jamming and indicate sensitivity to platform class and operating environment.

Findings indicate strong potential for HF EMF interference to interrupt the links that sustain swarm level decision making, including leader election, waypoint synchronization, and collision avoidance exchange. Aggregated survey responses place central tendencies near 80 percent for GPS jamming, 75 percent for protocol-oriented disruption, 70 percent for sweep methods, and 85 percent for reactive techniques that trigger in real time on detected emissions. Vulnerability is not uniform. Civilian platforms tend to rely more heavily on satellite navigation and exhibit higher sensitivity to GPS denial. Military grade systems employ encryption, frequency hopping, and hardened protocols and therefore respond more to tailored protocol level interference. Small UAVs with limited shielding and filtering show marked susceptibility to reactive methods that exploit timing and channel occupancy.

The principal contribution is an operational model that relates expected performance not only to power density and range but also to swarm decision topology. Star, mesh, and multi hub graphs exhibit distinct thresholds for coordination breakdown. The model links detection latency and channel uncertainty to stability margins in the control loop and articulates the trade between power and response time that governs safe and effective employment. A closed loop concept of operations is proposed that couple’s spectrum sensing, signal fingerprinting,

adaptive waveform generation, and geofencing with authorization and logging to protect civil aviation and critical radio services.

Implementation requires careful integration with spectrum management and with rules of engagement. Expert testimony emphasizes multilayer command procedures, electromagnetic compatibility audits, geospatial risk mapping, and post event forensics as prerequisites for reliable field use. Limitations include transfer gaps between laboratory and complex outdoor channels, rapid evolution of adaptive swarm protocols, and heterogeneous legal frameworks. Future work should optimize power and frequency allocation under safety constraints, fuse multi-platform sensing for better target identification, formalize secure and lawful reprogramming channels, and tailor interference policies to mission and topology.

Overall, HF EMF interference emerges as a promising, scalable, and measurable approach to defending against drone swarms. Maturation will depend on standardized test methods, interoperable safety procedures, and regulatory alignment across civil and military stakeholders.

References

1. Bayramov A.A. eta l. Unmanned Aerial Vehicle Applications for Military GIS Task Solutions //Research Anthology on Reliability and Safety in Aviation Systems, Spacecraft, and Air Transport. – IGI Global Scientific Publishing, 2021. – С. 1092-1115.

2. Muradov, S.A. (2023). Development prospects of beacon systems. *In* Problems of informatization. Vol. 1. p.31.

3. Muradov, S.A. et al. (2023, November). Determining the location of the UAV equipped with a homing device based on radio beacons. In *Modeling, Control and Information Technologies: Proceedings of International scientific and practical conference* (No. 6, pp. 54-56).

4. Bayramov A.A. The numerical estimation method of a task success of UAV reconnaissance flight in mountainous battle condition //Сучасні інформаційні системи. – 2017. – №. 1, № 2. – С. 70-73.

5. Hashimov E., Khaligov G. The issue of training of the neural network for drone detection //Advanced Information Systems. – 2024. – Т. 8. – №. 3. – С. 53-58.

6. 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.

7. Ganimat I. B. Analysis and selection performance indicators multiservice communication networks based on the concept NGN and FN //Computer and information systems and technologies. – 2021.

8. Nasibov Y. A. et al. Modelling of the rationally deployment of observing systems //Сучасні інформаційні системи. – 2019. – №. 3, № 2. – С. 10-13.

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

10. Bayramov A.A. Assessment of invisible areas and military objects in mountainous terrain //Defence Science Journal. – 2018. – Т. 68. – №. 4. – С. 343-346.

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

SYSTEM OF SYSTEMS AT WAR: UAV ENABLED SENSING AND STRIKE INTEGRATION

Mashaev E.T.
Baku State University, Baku, Azerbaijan
Hashimov E.G., Hasanov A.H.
National Defense University, Baku, Azerbaijan

This article analyzes how unmanned aerial vehicle technology is reshaping modern warfare at tactical, operational, and strategic levels and assesses the implications for doctrine, law, and ethics. The central claim is that UAV enabled sensing, strike, and command integration compress the reconnaissance to strike cycle, raise decision speed and precision, and redistribute risk across the force. The argument synthesizes recent conflict experience, advances in sensing and edge computing, and observed changes in command and control.

At the tactical level, electro optical and infrared payloads combined with synthetic aperture radar and on-board inference deliver persistent surveillance in degraded visual environments. These payloads support discrimination of targets in urban and mountainous terrain and enable calibrated effects with lower collateral risk. Edge inference using quantized one stage detectors paired with lightweight trackers sustains real time processing within size, weight, and power limits. Human in the loop supervision preserves accountability for lethal decisions and provides a check against model error in cluttered scenes.

At the operational level, UAVs extend the reach and tempo of combined arms by linking distributed sensors to effectors through resilient data links and standardized message formats. Continuous collection generates targetable patterns of life and strengthens dynamic tasking of fires, engineering, and maneuver. Hybrid communication topologies, priority-based routing, and energy aware scheduling improve survivability under electronic attack and contested spectrum. These adaptations push the design of operations toward force packages that mix endurance UAVs, loitering munitions, and small attritable platforms with manned assets in portfolio style employment.

At the strategic level, broader access to capable UAVs alters deterrence and compellence. Precision at affordable cost allows smaller states to offset mass with intelligence driven and time sensitive strikes. This creates asymmetric windows of advantage but also raises escalation management challenges, supply chain dependencies, and diffusion risks. Strategic communication increasingly relies on verifiable battle damage assessment and transparent audit logs that document targeting decisions and effects, which in turn shape legitimacy narratives.

Constraints and failure modes remain significant. Electronic warfare degrades navigation and data links through jamming and spoofing. Deception, decoys, and adversarial camouflage can trigger false positives. Weather windows and counter UAS defenses complicate mission planning and recovery. Mitigation requires multi sensor corroboration, behavior level anomaly detection, conservative rules of engagement, and rigorous pre mission testing with red teaming. Legal and ethical

compliance is foundational. Identification Friend or Foe procedures, proportionality assessments, and post action reviews must be embedded in the technical workflow. Responsible autonomy requires bounded delegations of authority and explicit breakpoints where human approval is mandatory.

Looking forward, three vectors are most consequential. First, edge computing will mature with neural processing units that provide low latency inference and secure model updates, enabling adaptive perception within strict power budgets. Second, multi sensor fusion will expand to include passive RF mapping, compact LiDAR, and cooperative sensing among manned and unmanned teammates, yielding richer confidence estimates for commanders. Third, swarm control will move from scripted formations to consensus or market-based algorithms that allocate roles dynamically under limited communications, which demands stronger cyber hardening and spectrum discipline.

References

1. Bayramov A.A. eta l. Unmanned Aerial Vehicle Applications for Military GIS Task Solutions //Research Anthology on Reliability and Safety in Aviation Systems, Spacecraft, and Air Transport. – IGI Global Scientific Publishing, 2021. – С. 1092-1115.

2. Muradov, S.A. (2023). Development prospects of beacon systems. *In* Problems of informatization. Vol. 1. p.31.

3. Muradov, S.A. et al. (2023, November). Determining the location of the UAV equipped with a homing device based on radio beacons. In *Modeling, Control and Information Technologies: Proceedings of International scientific and practical conference* (No. 6, pp. 54-56).

4. Bayramov A.A. The numerical estimation method of a task success of UAV reconnaissance flight in mountainous battle condition //Сучасні інформаційні системи. – 2017. – №. 1, № 2. – С. 70-73.

5. Hashimov E., Khaligov G. The issue of training of the neural network for drone detection //Advanced Information Systems. – 2024. – Т. 8. – №. 3. – С. 53-58.

6. 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.

7. Ganimat I. B. Analysis and selection performance indicators multiservice communication networks based on the concept NGN and FN //Computer and information systems and technologies. – 2021.

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

9. Nasibov Y. A. et al. Modelling of the rationally deployment of observing systems //Сучасні інформаційні системи. – 2019. – №. 3, № 2. – С. 10-13.

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

11. Bayramov A.A. Assessment of invisible areas and military objects in mountainous terrain //Defence Science Journal. – 2018. – Т. 68. – №. 4. – С. 343-346.

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

INTEGRATED APPLICATION OF REMOTE SENSING IN DEFENSE AND ENVIRONMENTAL OVERSIGHT

Huseynov M., Akhundov R.G.
National Defense University, Baku Azerbaijan
Hashimov E.G.
Azerbaijan Technical University, Baku, Azerbaijan

The article describes the full chain of remote sensing technologies in defense and environmental management, from observation to decision making, and demonstrates the advantages of their integrated application. The main idea is that if data obtained from satellite imagery, unmanned aerial vehicles, and ground sensors are converted into a unified information flow, both operational responsiveness increases and decisions are based on objective indicators. A multilayer architecture is considered necessary especially in areas where border relief is complex and infrastructure and climatic constraints exist [1-6].

The methodology is based on a staged approach. First, data from various sources are collected and fused according to the model $D_{total} = D_{sat} + D_{uav} + D_{ground}$; then radiometric and geospatial calibration is performed, and processing is carried out on cloud-based platforms.

For defense purposes, artificial intelligence models such as automatic object detection are applied, while for ecology spectral indices such as NDVI and change detection algorithms are used.

To evaluate the results, a KPI model based on weighted indicators is employed, where accuracy, processing speed, energy efficiency, and cost efficiency are considered together.

The article separately highlights environmental applications of remote sensing. During disaster monitoring, very high-resolution satellite images and UAV footage precisely identify flood zones, fire sources, and damaged areas. Processes such as forest cover loss, the impact of climate change, and urbanization dynamics can be tracked using multi-temporal satellite imagery.

In agriculture, vegetation indices make it possible to monitor crop status and manage resources more efficiently. The graphics described in the article show that technology achieves higher effectiveness in disaster management, while also delivering results above 80 percent in other areas.

A KPI-based framework is proposed to objectively measure the real status of these systems.

At the strategic level, accuracy, reliability, and scalability are prioritized; at the operational level, speed, low latency, and agility; at the resource level, energy and cost efficiency. Scoring with weighted points treats 8 and above as a high level and indicates that results in the 6 to 7.9 range require improvement.

In the discussion, the author notes that artificial intelligence and big data processing significantly increase the value of remote sensing, but the high cost of infrastructure and shortcomings in personnel training are common problems for both defense and environmental institutions.

Open data environments, regional cooperation, and cloud-based processing can partially mitigate these limitations.

The article concludes that remote sensing serves as a bridge between defense and environmental sustainability, and that sensor fusion together with KPI-based management makes this bridge controllable, repeatable, and durable.

References

1. Jabrayilov, A. R. et al. (2025). Prospects for creating closed ecological life support systems. *Current directions of development of information and communication technologies and control tools* (Vol. 4, pp. 92–93).

2. Talibov, A. M. et al. (2025). Training military personnel in radiation and chemical threat protection methods. *Proceedings of the 15th International Scientific and Technical Conference* (Vol. 4, p. 94–95).

3. Hasanov, A.H. (2022). Analysis of the effectivness of communication and automated management systems. In *Modern directions of development of information and communication technologies and management tools,* (Vol. 1, pp. 1-4).

4. Hashimov, E.G. (2017). Application of GIS and seismic location method for detection of invisible military objects /- Baku: Military Publishing House, 2017, 246 p.

5. Piriyev, H.K. et al. (2016). Modelling of the battle operations. *Monografiya, Herbi Nashriat", Baku.–2017*.

6. Bayramov, A.A. (2018). Assessment of invisible areas and military objects in mountainous terrain. *Defence Science Journal*, *68*(4), 343-346.

7. Talibov, A. et al. (2024). Environmental safety of nanomaterials application. In Problems of Informatization: Proceedings of the 12th International Scientific and Technical Conference (Vol. 3, pp. 55–56).

8. Mammadov, R. et al. (2024). Enhancing special forces management efficiency in modern operations. In *Problems of Informatization: Proceedings of the 12th International Scientific and Technical Conference* (Vol. 3, pp. 31–32).

9. Tahirov, R. K. et al. (2024). Environmental aspects of information technology implementation. In *Problems of Informatization: Proceedings of the 12th International Scientific and Technical Conference* (Vol. 3, pp. 138–139).

10. Islamov, I. et al. (2025). Integrating environmental security into defense strategy with a focus on radiological and chemical risks. İn *Strategic directions of science development: Factors of influence and interaction.* (pp. 115–125). https://doi.org/10.62731/mcnd-26.09.2025

11. Bayramov, A.A. et al. (2016). The detection of invisible objects on the terrain on the basis of GIS technology. *Geography and nature sources*, 124-126.

12. Hashimov, E.G. et al. (2015). Application of relief digital model for combat operation planning. *Military Knowledge*, *4*, 63-69.

13. Hashimov, E. G. (2021). Some aspects of the combat capabilities and application of modern UAVs. *Baku:"National Security and military knowledges*, (3), 7.

14. İbrahimov, B.G. et al. (2022). Research and analysis indicators fiber-optic communication lines using spectral technologies. *Advanced information systems*, *6*(1), 61-64.

15. Ibrahimov, B.G. et al. (2024). Research and analysis mathematical model of the demodulator for assessing the indicators noise immunity telecommunication systems. *Advanced Information Systems*, *8*(4), 20-25.

INTEGRATING UAV IMAGERY WITH GIS-BASED SPATIAL ANALYTICS TO FORECAST BORDER RISKS

Javadov J.M.
State Border Service Academy, Republic of Azerbaijan
Akhundov R.G.
National Defense University, Baku Azerbaijan
Hashimov E.G.
Azerbaijan Technical University, Baku, Azerbaijan

This article substantiates the integrated application of Unmanned Aerial Vehicles (UAVs) and Geographic Information Systems (GIS) in border security within a scientific and practical framework and presents a methodological pipeline for near real time situational monitoring, risk forecasting, and patrol route optimization. The conceptual approach rests on three pillars: first, extending observation capabilities under low-visibility conditions via electro-optical and infrared (EO/IR) sensor suites mounted on highly maneuverable multirotor UAV platforms; second, synchronous georeferencing of layers such as the border line, terrain, vegetation, and crossing points with UAV telemetry in the ArcGIS Pro environment; third, mapping risk zones based on kernel density analysis and ensuring traceability from requirements to testing within a V-Model structure.

The methodology consists of four stages. 1 Selection and configuration. A UAV equipped with EO/IR cameras and GNSS/IMU telemetry is selected, and initial calibration is performed for flight stability and payload limits. 2 Geospatial data processing. UAV imagery is automatically converted into an orthophoto mosaic, overlaid with the border line, terrain, and landscape masks, and georeferencing accuracy is verified using ground control points. 3 Risk modeling. Anomalous movement patterns are revealed on the kernel density map, the dynamics of a risk index are measured through time series analyses, and patrol trajectories are directed toward high probability zones. 4 V-Model integration. The left arm covers requirements, system design, and integration, the right arm covers subsystem, system, and acceptance tests, thereby maintaining a traceable chain from monitoring and analytics to decision making and operations.

Application results confirm the synergy effect in mountainous and hard-to-access areas. Fusing UAV imagery with GIS layers reduces redundant loops in patrol routes, enables timely retasking toward high-risk areas, and shortens response time. Automated legends using green for low risk, yellow for medium, and red for high create objective interpretation and reduce the influence of subjective judgments. Comparative analysis over time quantifies how seasonal transitions, vegetation density, and terrain shading affect the field of view, enabling agile adjustment of patrol resource allocation.

A management KPI set is established. The probability of detection Pd, false alarm rate FAR, mean response time, patrol coverage percentage, OODA loop duration, and a route efficiency index serve as baseline indicators for planning and reporting. Sensitivity scenarios consider weather conditions, radio link losses, GNSS

drifts, and power supply constraints, while calibration intervals and thresholds are updated dynamically. Constraints include infrastructure noise, line-of-sight gaps caused by terrain, and multi-source synchronization challenges. Recommended mitigation measures include EO/IR–LiDAR fusion, backup mesh communication nodes, edge computing for pre-processing, and AI-based image analytics.

In conclusion, UAV–GIS integration strengthens early warning in border protection, accelerates the rationalization of patrol resources, and enhances the transparency of decisions. The proposed framework, with its scalable architecture, V-Model traceability, and KPI-driven management, provides a practical basis for regional deployment and standardization. Future work concerns cooperative route planning for UAV swarms, the use of 5G and LEO links, real time updating of risk maps, and testing within a digital twin environment.

References

1. Javadov J.M., Hashimov E.G.. Application of UAV in the protection of state borders: gis integration and risk management. İn *Інноваційні тенденції сьогодення в сфері природничих, гуманітарних та точних наук*. Вінниця, Україна, 2025. p.p. 115-124. DOI:10.62731/mcnd-15.08.2025.003

2. Muradova, E. E. et al. (2025). Analytical evaluation of UAV-based logistical operations in contemporary military systems. In *Topical issues of science development.* (pp. 351–360). https://doi.org/10.62731/mcnd-31.10.2025

3. Babayev, S. et al. (2025). The impact of unmanned aerial vehicles on the strategy and tactics of modern warfare. In *Modern tools and methods of scientific investigations.* (pp. 28–36). https://doi.org/10.36074/scientia-10.10.2025

4. Tabunenko, V. et al. (2025). The dynamics of UAV flight integrated with route planning. In *Modern tools and methods of scientific investigations.* https://doi.org/10.36074/scientia-10.10.2025

5. Islamov, I. et al. (2025). The use of unmanned systems and artificial intelligence to enhance radiation and chemical safety in military ecology. In *Innovations and the scientific potential of the world.* (pp. 183–192). https://doi.org/10.62731/mcnd-10.10.2025

6. Tahirov, R. K. et al. (2024). Environmental aspects of information technology implementation. In *Problems of Informatization: Proceedings of the 12th International Scientific and Technical Conference* (Vol. 3, pp. 138–139).

7. Kovtun, A. V. et al. (2025). Techno-economic assessment of a hybrid solar, wind, and biomass system for suburban power supply. In *The driving force of science and trends in its development.* pp. 112–119. https://doi.org/10.36074/scientia-17.10.2025

8. Islamov, I. et al. (2025). Hybrid communication models for UAV swarms: Towards scalable and energy-aware network optimization. İn *Scientific guidelines: Theory and practice of research.* pp. 185–195. https://doi.org/10.62731/mcnd-03.10.2025

9. Ismayil, I. et al. (2025). Optimization of composite material selection in the design of military UAV wings. İn *Scientific review of the actual events, achievements and problems.* pp. 107–115. https://doi.org/10.36074/scientia-03.10.2025

10. Babayev, S. et al. (2025). Enhancing operational effectiveness through command and control integration of autonomous robot swarms. İn *Scientific review of the actual events, achievements and problems.* pp. 75–82. https://doi.org/10.36074/scientia-03.10.2025

11. Talibov, A. M. et al. (2025). The use of unmanned aerial vehicles for monitoring chemical and radiation contamination. In *Current directions of development of information and communication technologies and control tools.* (Vol. 4, pp. 88-89).

HYBRID ACOUSTIC SEISMIC APPROACH FOR THE IDENTIFICATION OF MOVING TARGETS

Kartashov O.S., Talıbov A.M.,
İnstitute of Control Systems, Baku, Azerbaijan
Akhundov R.G.
National Defense University, Baku, Azerbaijan
Hashimov E.G.
Azerbaijan Technical University, Baku, Azerbaijan

This article provides a systematic assessment of the hybrid application of acoustic and seismic methods based on scientific principles for the detection of moving objects and proposes a unified model to improve near real time performance in various environments. The relevance of the problem is conditioned by the limitations of radar and optical systems in non-classical conditions such as underwater areas, behind dense materials and wide-open spaces. Acoustic methods rely on the propagation and reflection of sound waves, while seismic methods are based on measuring vibrations occurring on the ground surface and in deeper layers. Integration of the complementary properties of these two approaches increases signal sensitivity and spatio temporal accuracy, which in turn enables a reduction in false alarms, an increase in detection probability and stability in complex background noise.

The methodological framework is built on three pillars. The first pillar presents the physical models of separate acoustic and seismic channels. Acoustic propagation reaches long distances in water with low loss, while attenuation is faster in air. Seismic waves are effectively transmitted in soil and rock layers, while they propagate weakly in air and water. The second pillar forms the signal processing sequence. Low pass and band pass filters, adaptive noise suppression, impulse event detection, spectro temporal feature extraction and time synchronization of event windows are applied. The third pillar develops a multi-level data fusion mechanism for data integration. At the pixel level energy maps are generated, at the feature level mel spectral and HHT attributes are used, and at the decision level final probability maps are constructed through Bayesian rules or Dempster Shafer combination. For spatial localization triangulation or hybrid TDoA AoA solutions are used.

Analysis of the results shows that the hybrid acoustic seismic approach can provide up to a 20 percent increase in detection even at low signal to noise ratios compared to single channel solutions and can reduce the false alarm rate by approximately a factor of two. In terrestrial environments soil type and moisture, and in aquatic environments temperature and salinity gradients change propagation speed and attenuation.

Through a corresponding adaptive calibration stage, the thresholds of the sensor network are tuned dynamically. Field applications are summarized in three blocks. In defense and security, it is evaluated as a target-oriented solution for border surveillance and control of maneuver routes. In environmental monitoring it is suitable for tracking fauna migration routes and underwater currents. In industrial

safety it is suitable for monitoring the vibration signatures of pipelines and heavy machinery.

Limitations are also taken into account. Signal interference caused by environmental variability, the complexity of processing large data volumes and the requirements for multichannel synchronization are the main challenges. In response to these risks, noise robust features, multi modal time synchronization, aggregation of decisions with signal reliability weights and distributed computing nodes are proposed. In sensitivity scenarios updating calibration coefficients for such factors as changes in soil layers, water depth and wind load keeps the system stable.

The practical contribution is that the presented visual and computational sequence facilitates the phased deployment of acoustic and seismic channels in field networks and makes it possible to regularly measure indicators such as probability of detection, false alarm rate, localization error and latency as a KPI set. As a result, hybrid acoustic seismic systems serve as an extensible and reliable detection platform in defense, environmental monitoring and industrial safety.

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. – С. 124-126.

2. Bayramov, A.A., & Hashimov, E. (2017). The numerical estimation method of a task success of UAV reconnaissance flight in mountainous battle condition. *Сучасні інформаційні системи*, (1,№ 2), 70-73.

3. Bayramov, A.A. (2018). Assessment of invisible areas and military objects in mountainous terrain. *Defence Science Journal*, *68*(4), 343-346.

4. Ganimat, I. B. (2021). Analysis and selection performance indicators multiservice communication networks based on the concept NGN and FN. *Computer and information systems and technologies*.

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

6. Hashimov, E.G. (2017). Application of GIS and seismic location method for detection of invisible military objects /- Baku: Military Publishing House, 2017, 246 p.

7. İbrahimov, B.G. et al. (2022). Research and analysis indicators fiber-optic communication lines using spectral technologies. *Advanced information systems*, *6*(1), 61-64.

8. Ibrahimov, B.G. et al. (2024). Research and analysis mathematical model of the demodulator for assessing the indicators noise immunity telecommunication systems. *Advanced Information Systems*, *8*(4), 20-25.

9. Piriyev, H.K. et al. (2016). Modelling of the battle operations. *Monografiya, Herbi Nashriat", Baku.–2017*.

10. Гашимов Э. Г. Сейсмолокационная станция //Военное обозрение. – 2016. – Т. 1. – №. 01. – С. 30-41.

11. Гашимов Э. Г. Метод детектирования скрытного перемещения бронетехники противника //Военное знание. – 2015. – Т. 3. – С. 30-41.

12. Гашимов Э. Г., Байрамов А. А. Обнаружение передвижения ненаблюдаемой бронетехники противника сейсмолокационным методом //Национальная безопасность и военные науки. – 2015. – Т. 1. – №. 1. – С. 128-132.

ACCELERATING DECISION MAKING AND OPERATIONAL EFFICIENCY THROUGH C4ISR ARCHITECTURE

Krikun, V.L., Hashimov E.G.
Azerbaijan Technical University, Baku, Azerbaijan
Akhundov R.G.
National Defense University, Baku, Azerbaijan
Talibov A.M.
İnstitute of Control Systems, Baku, Azerbaijan

This article systematizes the application of C4ISR systems in modern military and security operations from a functional-architectural perspective and proposes an integration framework that increases the speed, accuracy and transparency of decision making. The aim of the study is to present the interdependencies of the subcomponents of Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance within a single operational model, to shorten the near real time information circulation, multisource data fusion and cyber protected decision loop (OODA). The novelty of the approach is the alignment of operational - systems - technical views of C4ISR in both visual and computational form, the inclusion of UAV-centered intelligence packages, meshed tactical communications, BMS integration resilient in EW conditions, as well as the embedding of a KPI based management module into a single pipeline.

The methodology consists of four stages. 1) Conceptual mapping: a traceability axis is established between C and C2 decision flows, C3-C4 communication-computing layers and the ISR cascade, and interfaces are harmonized at operational, systems and technical layers. 2) Data fusion: satellite, MALE/tactical UAV, border radar posts, EO/IR and SIGINT sources are time-space synchronized with STANAG-compliant metadata, and fusion is applied at pixel, feature and decision levels using Bayesian, D-Shafer or ensemble networks. 3) Cybersecurity and resilience: zero trust principle, a quantum resistant encryption plan, adaptive spectrum use in electronic warfare (jam/spoof) conditions and continuity plans are introduced. 4) KPI management: indicators such as OODA time, ISR latency, target identification accuracy, ROE compliance share, collateral damage indicators, communication recovery time and operational availability are selected, and prioritization is carried out with sensitivity scenarios.

The results show that when the inter-function traceability of C4ISR is strengthened and the UAV based ISR package is supported by near real time fusion, preparation and execution of decisions are synchronized, operational delays are reduced and target identification accuracy increases. In border security, risk zones are visualized in a preventive manner through the geographic overlay of sensor networks.

In counterterrorism, cross validation of multichannel signals (OSINT/SIGINT/IMINT) reduces false alarms. In emergency situations, information exchange between command posts and civilian services makes recovery plans more realistic.

Cyber risk modeling shows that for maintaining the confidentiality-integrity-availability (CIA) balance, network slicing and hybrid signature based plus anomaly based analysis of telemetry increase continuity.

The practical contribution is that the proposed framework formalizes C4ISR components not only as a list but as a system linked to an operational sequence and control loop, and it provides visual and computational standards for application in national security, border control and urban environment operations. The scientific contribution is the standardization of the KPI set and fusion procedures as well as the mapping of C4ISR development-test phases with V-Model principles. Future work will be extended to AI based adaptive decision trees, 5G/LEO convergence, quantum resistant crypto protocols and testing in a digital twin.

References

1. Maharramov, R.R. et al. (2025). Application of C4ISR systems in military and security operations. *Матеріали конференцій МЦНД*, (15.08.2025; Харків, Україна), 125–134. https://doi.org/10.62731/mcnd-15.08.2025.004

2. Khudeynatov, E.K. (2025). Application of V-model in the protection of oil pipelines. *Collection of Scientific Papers «SCIENTIA»*, (August 8, 2025; Liverpool, UK), 67–74. Retrieved from https://previous.scientia.report/index.php/archive/article/view/2896

3. Elnur K. V-Model for Air Defense Systems //Modeling, Control and Information Technologies: Proceedings of International scientific and practical conference. – 2023. – №. 6. – С. 46-49.

4. Babayev, S. et al. (2025). Enhancing operational effectiveness through command and control integration of autonomous robot swarms. *Scientific review of the actual events, achievements and problems.* pp. 75–82. https://doi.org/10.36074/scientia-03.10.2025

5. Islamov, I. et al. (2025). Hybrid communication models for UAV swarms: Towards scalable and energy-aware network optimization. *Scientific guidelines: Theory and practice of research.* pp. 185–195. https://doi.org/10.62731/mcnd-03.10.2025

6. Islamov, I. et al. (2025). Integrating environmental security into defense strategy with a focus on radiological and chemical risks. *Strategic directions of science development: Factors of influence and interaction.* pp. 115–125. https://doi.org/10.62731/mcnd-26.09.2025

7. Tahirov, R. K. et al. (2024). Environmental aspects of information technology implementation. In *Problems of Informatization: Proceedings of the 12th International Scientific and Technical Conference* (Vol. 3, pp. 138–139).

8. Kovtun, A. V. et al. (2025). Techno-economic assessment of a hybrid solar, wind, and biomass system for suburban power supply. In *The driving force of science and trends in its development.* (pp. 112–119). https://doi.org/10.36074/scientia-17.10.2025

9. Salmanov, E. I. et al. (2025). Ways to improve logistical support in the Azerbaijani Army. In *The driving force of science and trends in its development.* (pp. 88–95). https://doi.org/10.36074/scientia-17.10.2025

10. Huseynov, M. et al. (2025). Application of modern multi-sensor technologies for ground target detection. In *Innovations and the scientific potential of the world.* pp.172–182. https://doi.org/10.62731/mcnd-10.10.2025

11. Tabunenko, V. et al. (2025). The dynamics of UAV flight integrated with route planning. In *Modern tools and methods of scientific investigations.* (pp. 46–56). https://doi.org/10.36074/scientia-10.10.2025

IMPACT OF HIGH-FREQUENCY ELECTROMAGNETIC FIELDS ON UAV SWARMS AND COUNTERMEASURES

Maharramov R.R., Akhundov R.G.
National Defense University, Baku Azerbaijan
Hashimov E.G.
Azerbaijan Technical University, Baku, Azerbaijan

The increasing use of AI-enabled UAV swarms in recent years is forming a new threat configuration for traditional air defense systems. Since swarm architecture enables the autonomous coordination of numerous platforms, it makes possible mass, agile, and comparatively low-cost operations. The aim of this study is to evaluate, both analytically and empirically, the impact of high-frequency electromagnetic fields (HF EMF) against UAV swarms, with particular focus on radio-electronic jamming and reprogramming approaches, and to identify application scenarios and limitations. The hypothesis is that targeted disruption of communication channels and navigation signals via HF EMF reduces the stability of swarm control, generates coordination losses, and enables neutralization without the need for physical destruction.

The methodology is based on a mixed design. Within the qualitative component, in-depth interviews are conducted with 15 experts from the fields of military affairs, cybersecurity, drone engineering, and electronic warfare. The questions focus on application constraints, technical barriers, and operational principles. In the quantitative component, a structured survey of 405 professional respondents is carried out. The targets are to assess the effectiveness of HF EMF technologies, compare types of electronic jamming, and evaluate reprogramming capabilities. Additionally, scenario-based modeling is used to analyze the optimization of interference parameters for different swarm dynamics. For reliability checks, measurement repeatability, a topic-fit index for expert responses, and response consistency are employed.

The main results show that applying HF EMF slows command dissemination within the swarm, increases communication delays, and creates synchronization disruptions in distributed decision-making algorithms. According to the survey data, reactive jamming has the highest relative effectiveness because signals are detected and targeted in real time, while GPS jamming exhibits high sensitivity especially in commercial UAVs. Protocol-oriented jamming is rated as more effective against military-grade UAVs since this class employs multilayer encryption and frequency-hopping schemes. Expert interviews emphasize the importance of legal and ethical frameworks. In particular, regulatory control of spectrum management, power, and directional parameters is necessary to minimize risks to civil aviation navigation. Operationally, directional antenna arrays, adaptive power control, and real-time spectrum analytics stand out as the most suitable solutions for airport and urban environments.

Technological limitations include spectrum congestion, multipath effects arising from the environment, frequency hopping in high-speed swarms, and

waveform diversity. To overcome these barriers, a multimodal interference concept is proposed. The core elements of the concept are dynamic spectrum selection with cognitive radio, machine-learning-based signal classification, time-synchronized reactive jamming, and selective directional energy focusing techniques. In an integrated operational scheme, connecting the HF EMF module to the air defense surveillance and command-and-control loop enhances situational awareness, shortens response cycles, and reduces collateral risks.

The conclusion shows that when properly configured, HF EMF approaches provide a practical basis for non-kinetic neutralization against UAV swarms. Nevertheless, maintaining stable effects requires parallel solutions for energy budget, early detection, targeting accuracy, and legal compliance. Future work prioritizes joint optimization of multi-level interference strategies, cooperative jamming networks, and the discovery of vulnerability models in swarm algorithms.

References

1. Muradova, E. E. et al. (2025). Analytical evaluation of UAV-based logistical operations in contemporary military systems. In *Topical issues of science development.* (pp. 351–360). https://doi.org/10.62731/mcnd-31.10.2025

2. Babayev, S. et al. (2025). The impact of unmanned aerial vehicles on the strategy and tactics of modern warfare. In *Modern tools and methods of scientific investigations.* (pp. 28–36). https://doi.org/10.36074/scientia-10.10.2025

3. Tabunenko, V. et al. (2025). The dynamics of UAV flight integrated with route planning. In *Modern tools and methods of scientific investigations.* https://doi.org/10.36074/scientia-10.10.2025

4. Islamov, I. et al. (2025). The use of unmanned systems and artificial intelligence to enhance radiation and chemical safety in military ecology. In *Innovations and the scientific potential of the world.* (pp. 183–192). https://doi.org/10.62731/mcnd-10.10.2025

5. Tahirov, R. K. et al. (2024). Environmental aspects of information technology implementation. In *Problems of Informatization: Proceedings of the 12th International Scientific and Technical Conference* (Vol. 3, pp. 138–139).

6. Kovtun, A. V. et al. (2025). Techno-economic assessment of a hybrid solar, wind, and biomass system for suburban power supply. In *The driving force of science and trends in its development.* pp. 112–119. https://doi.org/10.36074/scientia-17.10.2025

7. Islamov, I. et al. (2025). Hybrid communication models for UAV swarms: Towards scalable and energy-aware network optimization. İn *Scientific guidelines: Theory and practice of research.* pp. 185–195. https://doi.org/10.62731/mcnd-03.10.2025

8. Ismayil, I. et al. (2025). Optimization of composite material selection in the design of military UAV wings. İn *Scientific review of the actual events, achievements and problems.* pp. 107–115. https://doi.org/10.36074/scientia-03.10.2025

9. Babayev, S. et al. (2025). Enhancing operational effectiveness through command and control integration of autonomous robot swarms. İn *Scientific review of the actual events, achievements and problems.* pp. 75–82. https://doi.org/10.36074/scientia-03.10.2025

10. Talibov, A. M. et al. (2025). The use of unmanned aerial vehicles for monitoring chemical and radiation contamination. In *Current directions of development of information and communication technologies and control tools: Proceedings of the 15th International Scientific and Technical Conference* (Vol. 4, pp. 88-89).

SYSTEM-LEVEL METHODS FOR ENHANCING UAV FLIGHT SAFETY AND RESOURCE EFFICIENCY

Muradov S.A., Huseynov B.S., Akhundov R.G.
National Defense University, Baku Azerbaijan
Hashimov E.G.
Azerbaijan Technical University, Baku, Azerbaijan

This article presents a unified simulation and control framework that ensures reliable and efficient operation of unmanned aerial vehicles in dynamic environments.

The approach integrates, within a single environment, a six-degree-of-freedom nonlinear state-space model, the Dryden turbulence model, sensor–actuator imperfections, and a route-planning module. The objective is accurate trajectory tracking under various wind regimes and payload profiles, optimization of energy consumption, compliance with actuator limits, and preservation of real-time computational stability.

As control algorithms, a linear quadratic regulator and model-based predictive control are comparatively evaluated, and parameter identification is performed using real flight telemetry.

In the methodology, the equations of motion in the body frame are formed using aerodynamic, gravitational, thrust, and wind force and moment components; transformation operators are employed for Euler angles and rates.

Dryden filters project wind components onto the body axes; Gaussian noise, bias drift, and discretization are incorporated in the IMU and GNSS models. Actuator dynamics are represented by a first-order transfer function with amplitude and rate limits.

In route planning, topological search is built on an RRT* graph, while kinematic matching is ensured by Dubins segments that satisfy constant turn radius and course continuity requirements. Evaluation criteria include the RMS of trajectory deviation, the RMS error of attitude angles, an energy-consumption proxy, and the average computation delay.

The results show that in regimes where constraints are active and aerodynamic nonlinearities intensify, model-based predictive control yields lower tracking error and peak deviation than the linear quadratic regulator, albeit at higher computational cost. For simpler profiles, the linear quadratic regulator delivers competitive performance and exhibits lower sensitivity to delays. In scenarios with ±10 percent variation of Dryden parameters, both controllers remain stable; when sensor noise increases, the extended Kalman filter plays a decisive role in maintaining robustness of state estimation. The integration of RRT* and Dubins paths reduces the mismatch between actuator constraints and maneuver requirements, leading to more efficient energy distribution along the route and statistically lower lateral deviation in turning segments.

From a computational standpoint, with multisensory data discretized at 100 Hz, the control-loop latency is kept within real-time limits; additions such as anti-

windup, rate limiting, and reference shaping mitigate the effects of actuator saturation. The proposed framework enables unified, sequential synthesis of control while accounting for a full six-degree-of-freedom model, wind modeling, and practical constraints.

This leads to enhanced flight safety, efficient use of resources, and improved adaptive stability.

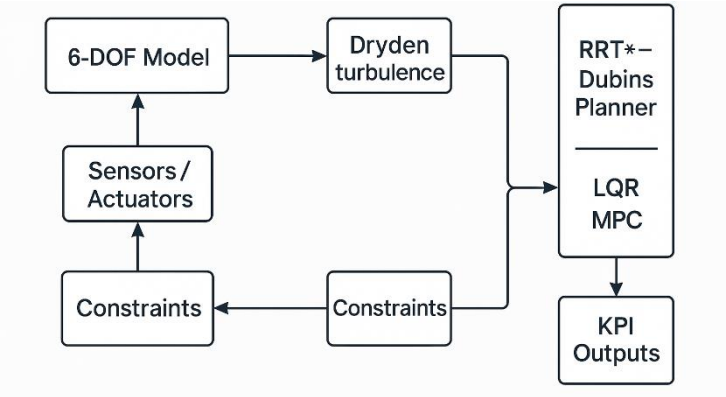

Fig. 1. Flight Control Framework: *6-DOF model, Dryden turbulence, sensor–actuator chain, RRT*–Dubins planning, and LQR/MPC control flow

The practical significance of the results is improved stability and control quality in applications such as military–logistic reconnaissance, environmental monitoring, emergency response, and infrastructure inspection.

Future work will extend toward higher-fidelity aerodynamic models, non-Gaussian wind scenarios, real-time code optimization, and cooperative control with multiple UAVs.

References

1. Islamov, I. et al. (2025). Hybrid communication models for UAV swarms: Towards scalable and energy-aware network optimization. *Scientific guidelines: Theory and practice of research.* pp. 185–195. https://doi.org/10.62731/mcnd-03.10.2025

2. Tahirov, R. K. et al. (2024). Environmental aspects of information technology implementation. In *Problems of Informatization: Proceedings of the 12th International Scientific and Technical Conference* (Vol. 3, pp. 138–139).

3. Babayev, S. et al. (2025). The impact of unmanned aerial vehicles on the strategy and tactics of modern warfare. In *Modern tools and methods of scientific investigations*. pp. 28–36. https://doi.org/10.36074/scientia-10.10.2025

4. Talibov, A. M. et al. (2025). The use of unmanned aerial vehicles for monitoring chemical and radiation contamination. In *Current directions of development of information and communication technologies and control tools: Proceedings of the 15th International Scientific and Technical Conference* (Vol. 4, pp. 88-89).

5. Ismayil, I. et al. (2025). Optimization of composite material selection in the design of military UAV wings. Scientific review of the actual events, achievements and problems. pp. 107–115. https://doi.org/10.36074/scientia-03.10.2025

6. Islamov, I. et al. (2025). The use of unmanned systems and artificial intelligence to enhance radiation and chemical safety in military ecology. In *Innovations and the scientific potential of the world.* pp. 183–192. https://doi.org/10.62731/mcnd-10.10.2025

7. Tabunenko, V. et al. (2025). The dynamics of UAV flight integrated with route planning. In *Modern tools and methods of scientific investigations: Proceedings of the VI International Scientific and Theoretical Conference* (pp. 46–56). https://doi.org/10.36074/scientia-10.10.2025

8. İskhandarov, Kh. et al. (2025). Artificial intelligence in logistics operations. In *Topical issues of science development: Proceedings of the VI International Scientific Conference* (pp. 433–442). https://doi.org/10.62731/mcnd-31.10.2025

9. Muradova, E. E. et al. (2025). Analytical evaluation of UAV-based logistical operations in contemporary military systems. In *Topical issues of science development: Proceedings of the VI International Scientific Conference* (pp. 351–360). https://doi.org/10.62731/mcnd-31.10.2025

10. Hasanov, A.H. (2022). Analysis of the effectivness of communication and automated management systems. In *Modern directions of development of information and communication technologies and management tools,* (Vol. 1, pp. 1-4).

11. Hashimov, E.G. et al. (2015). Application of relief digital model for combat operation planning. *Military Knowledge*, *4*, 63-69.

12. Hashimov, E. G. (2021). Some aspects of the combat capabilities and application of modern UAVs. *Baku:"National Security and military knowledges*, (3), 7.

13. Hashimov, E.G. (2017). Application of GIS and seismic location method for detection of invisible military objects /- Baku: Military Publishing House, 2017, 246 p.

14. İbrahimov, B.G. et al. (2022). Research and analysis indicators fiber-optic communication lines using spectral technologies. *Advanced information systems*, *6*(1), 61-64.

15. Ibrahimov, B.G. et al. (2024). Research and analysis mathematical model of the demodulator for assessing the indicators noise immunity telecommunication systems. *Advanced Information Systems*, *8*(4), 20-25.

16. Bayramov, A.A. et al (2018). The supervisory control systems deployment in mountainous terrain. In *VIII Int. Conf."Modern development trends of ICT and control methods* (pp. 3-4).

17. Bayramov, A.A. et al. (2016). The detection of invisible objects on the terrain on the basis of GIS technology. *Geography and nature sources*, 124-126.

18. Bayramov, A.A., & Hashimov, E. (2017). The numerical estimation method of a task success of UAV reconnaissance flight in mountainous battle condition. *Сучасні інформаційні системи*, (1,№ 2), 70-73.

19. Bayramov, A.A. (2018). Assessment of invisible areas and military objects in mountainous terrain. *Defence Science Journal*, *68*(4), 343-346.

20. Ganimat, I. B. (2021). Analysis and selection performance indicators multiservice communication networks based on the concept NGN and FN. *Computer and information systems and technologies*.

21. Hashimov E., Sabziev E., Muradov S. Development prospects and mathematical solution methods for integrating beacon systems into UAVS //Reliability: Theory & Applications. – 2025. – Т. 20. – №. SI 7 (83). – С. 66-73.

22. Nasibov Y. A. et al. Modelling of the rationally deployment of observing systems //Сучасні інформаційні системи. – 2019. – №. 3,№ 2. – С. 10-13.

23. Ibrahimov B.G et al. Research and analysis mathematical model of the demodulator for assessing the indicators noise immunity telecommunication systems //Advanced Information Systems. – 2024. – Т. 8. – №. 4. – С. 20-25.

SMALL SIZED UNMANNED AERİAL VEHİCLES SIGNAL PROTECTION AGAINST DETECTION TECHNOLOGIES AND RESILIENCE OF TELEMETRY SYSTEMS

Rustamov A.R., Gasanov A.G.
National Defense University, Baku, Azerbaijan
Azizullayev M.G.
National Aerospace Agency, Baku, Republic of Azerbaijan
Hasanli R.A.
Sumqait State University, Sumqait, Azerbaijan

The paper examines the issues of detecting small-sized unmanned aerial vehicles and ensuring the robustness of telemetry systems against signal interference in the event of detection. First, the acoustic, electro-optical, radar, radio frequency and multisensor technologies used in detecting unmanned aerial vehicles are analyzed from a technical point of view, and their advantages and limitations in operating conditions are comparatively evaluated . Then, methods of protection against radio electronic interference (jamming and spoofing) directed against the control and communication systems of detected UAVs are presented - including anti-jamming technologies, frequency hopping (FHSS), complex modulation methods and encryption algorithms. In the experimental part of the article, comparative tests of NRF24L01+ and RFD900x modules at a distance of 100 - 500 meters were conducted in laboratory conditions, and the results were analyzed based on indicators such as SNR, BER, packet loss and delay. The results show that while the RFD900x module provides more stable and interference-resistant communication, the NRF24L01+ can only be used over short distances[1-5].

Laboratory tests and analyses have shown that the performance of UAV telemetry systems is directly dependent on distance and interference conditions. The RFD900x module, with its higher output power and ability to provide a stable signal, has shown superior results compared to the NRF24L01+. Especially at distances above 300 meters, the NRF24L01+ module has increased signal attenuation, packet loss, and transmission delay, which makes it unsuitable for long-range communication. Thus, the RFD900x module is more suitable for use in military and critical communication systems, while the NRF24L01+ is recommended for short-range and energy-efficient applications. It is recommended that interference-resistant technologies – such as FHSS, encryption, and error checking mechanisms - be applied to telemetry systems. Future research should focus on simulating signal protection and LoS / NLoS scenarios in systems operating with limited power[6-8].

References

1. Gasanov, A.G. (2025). Problems of optimal planning of air defense means against low-altitude air targets, Збірник наукових праць з матеріалами IX Міжнародної Наукової конференції, pp. 409-418.
2. Rustamov A.R., Gasanov A.G., Azizullayev, M.G. (2024). Effective application of telemetry systems of unmanned aerial vehicles. // Modern directions development information and communication technology and means management, Vol/ 2: sections 3– 6, pp. 66-70.

3. Rustamov, A.R., Gasanov, A.G., Azizullayev, M.G. (2024). The role of navigational and hydrographical support in ensuring security of the Caspian Sea. 2nd International Conference on Logistics, Transport and Distribution in the Caspian Region, May 15-17, Baku, Azerbaijan.

4. Rustamov, A.R., Gasanov, A.G., Azizullayev, M.G. (2024). Analysis of modules and systems used in effective control of UAVs in radio electronic combat environment. Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. Тези доповідей чотирнадцятої міжнародної науково-технічної конференції 25 - 26 квітня, pp. 47-48, doi: https://doi.org/10.32620/ICT.24.t1

5. Gasanov, A.G., Karimov, Y. Sh. (2023). Optimal management of the application of a group of unmanned aerial vehicles (UAVs) of the same type to different targets, The Journal of Defense Resources Management (JoDRM), vol 14, Issue 2 (27), pp. 125-130.

6. Piriyev G. K. et al. Modelling of the battle operations //Monografiya, Herbi Nashriat", Baku. – 2017.

7. Hasanov A. H. 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.

8. Hashimov E.G. et al. Mathematical modeling of military systems. Textbook. -Baku: Military publishing house, -2018. -266 p.

9. Alieva, R. A., Pashaev, F. G., Gasanov, A. G., & Mahmudov, K. T. (2009). Quantum-chemical calculations of the tautomeric forms of azo derivatives of acetylacetone and determination of the stability constants of their complexes with rare-earth metals. *Russian Journal of Coordination Chemistry*, *35*(4), 241-246.

10. Gadzhieva S. R. et al. Thermodynamic characteristics of metal complexation with 3-[4-iodophenylazo]-2, 4-pentanedione in an aqueous ethanol solution //Russian Journal of Inorganic Chemistry. – 2007. – T. 52. – №. 4. – C. 640-644.

11. Aliyev A. A. et al. Earthquake and activation of mud volcano (causal link and interaction) //Proc. Geol. Inst. – 2001. – T. 29. – C. 26-39.

12. Ahmadov A. I. et al. Calculation of the Energy of the Interelectron Interaction in Molecules in a Basis of Slater Functions //Russian Physics Journal. – 2019. – T. 61. – №. 10. – C. 1848-1854.

STATEMENT OF THE INVERSE PROBLEM OF THE TIKHONOV-LAVRENTIYEV TYPE

Huseynov A.G., Abdullayeva A.J.
National Defense University, Baku, Azerbaijan
Mamedov İ.G.
Institute of Control Systems, Baku, Azerbaijan
Sumgait State University, Sumgait, Sumgait, Azerbaijan

The relationship between the memory of objects and inverse problems of mathematical physics. In the physical sense, the memory of an object means that a material or environment does not forget the effects of the past, that is, its current state depends not only on its current conditions, but also on the history of previous loading and effects. In memory systems, differential equations often take the form

of integro-differential. In particular, the role of memory in inverse problems is very important. The goal of inverse problems of mathematical physics is to find the internal properties of the system from observed results (measured data). Since objects have memory, inverse problems of mathematical physics try to restore memory, that is, read back the history of the system from measured results. This shows both the necessity of regularization methods from a mathematical point of view and the complexity of observing and modeling environments with memory from a physical point of view.

Tikhonov-Lavrentyev type coefficient inverse problem. Stefan-type inverse problem and its application to variable boundary problems in fluid mechanics. The following problems will be studied in this work [1-4]. Tikhonov-Lavrentyev-type inverse problem in the model case for $u_{xy} = ku(x,y), k \geq 0$ the telegraph equation [5, 6]. Stefan-type inverse problem in the model case for the telegraph equation.

$u_{xy} = ku(x,y), k \geq 0$ - the formulation of the Tikhonov-Lavrentyev-type inverse problem in the model case for the telegraph equation. Telegraph-type equations arise naturally in media with memory of bodies (for example, elastic, relaxing or non-locally conducting materials). The main difference in media with memory is that the answer depends not only on the current time, but also on past moments: This equation can model the propagation of an electric signal along a line, the attenuation of electromagnetic waves, or the conduction of heat at a finite speed. The inverse problem means finding the internal parameters or initial conditions of the system based on the results.

Let's look at the telegraph equation, which is widely used in communication:

$$u_{xy}(x,y) = ku(x,y), k \geq 0, \qquad (x,y) \in G. \tag{1}$$

Here $u = u(x,y)$ is the function to be sought, G defined in the domain; are the measurable functions given in the domain.$G = G_1 \times G_2$, here $G_1 = [x_0, x_1]$, $G_2 = [y_0, y_1]$. The telegraph equation is a hyperbolic equation. It has two real simple characteristics: $x = const$, $y = const$. This equation is found in communications and in the theory of inverse problems. For this telegraph equation, the boundary conditions classically set in the middle of the region can be given as follows:

$$\begin{cases} u/_{x=\sqrt{x_0 x_1}} = \Phi(y), \\ u/_{y=\sqrt{y_0 y_1}} = \Psi(x). \end{cases} \tag{2}$$

Here $\Phi(y), \Psi(x)$ G are the functions given in the region. It is clear that, in addition to the conditions Φ, Ψ of the functions in (2), $\Phi \in C^1(G_2), \Psi \in C^1(G_1)$ the following condition must also be satisfied:

$$\Phi\left(\sqrt{y_0 y_1}\right) = \Psi\left(\sqrt{x_0 x_1}\right). \tag{3}$$

This is called the compromise condition. The fact is that the compromise condition in the formulation of problems (1) and (2) means that condition (2) gives some additional information about the solution of the problem. Therefore, the problem of finding boundary conditions is posed such that these boundary conditions do not contain additional information about the solution and which do not require

any additional conditions as a compromise condition. In this regard, let us consider the following boundary conditions:

$$\begin{cases} V_{0,0}u \equiv u(\sqrt{x_0x_1},\sqrt{y_0y_1}) = \phi_{0,0} \\ (V_{1,0}u)(x) \equiv u_x(x,\sqrt{y_0y_1}) = \phi_{1,0}(x), \\ (V_{0,1}u)(y) \equiv u_y(\sqrt{x_0x_1},y) = \phi_{0,1}(y). \end{cases} \quad (4)$$

Here $\phi_{0,0} \in R$ are the functions given in the region. It is clear that, in addition to the conditions of the functions in (2), the following condition must also be satisfied, here $\phi_{0,0} \in R$ is a given number, and $\phi_{i,j}$ are given functions, satisfying the following conditions:

$$\phi_{1,0}(x) \in C(G_1), \phi_{0,1}(y) \in C(G_2).$$

If the function $u \in C^{1,1}(G)$ (1), (2) is a solution to the conditional problem in the middle of the region in the classical way, then it is a solution to the problem (1), (4) $\phi_{i,j}$and is defined by the following equations:

$$\begin{cases} \phi_{0,0} = \Phi(\sqrt{y_0y_1}) = \Psi\left(\frac{x_0+x_1}{2}\right), \\ \phi_{1,0}(x) = \Psi_x(x), \\ \phi_{0,1}(y) = \Phi_y(y). \end{cases} \quad (5)$$

This research is devoted to the study of memory phenomena in various materials and the improvement of methods for reading the information stored in them. The mechanisms of shape memory in alloys (e.g., nitinol), polymers, foams, as well as the phenomena of residual stress in metals and glasses were considered. It was found that the application of optical and magnetic technologies, as well as quantum and DNA memory, expands traditional approaches to stored information. Special attention is paid to methods that allow reading acoustic traces stored at the microstructural level, for example, on wooden surfaces, such as laser vibrometry, infrared and ultrasonic diagnostics.

References

1. Arif Hasanov, Islam Islamov, Arzuman Gasanov and Aynura Abdullayeva. Methodology for Solving the Problem of Objects Having Memory. Int. Conf. On Managment And Control İn Solving Engineer Problems, March 13-15, 2025. Baku, Azerbaijan.

2. Mamedov I. G., Abdullaeva A. J. On an optimal control problem for 3D Bianchi integro-differential equations with nonsmooth coefficients under conditions in the geometric middle of the domain //Informatics and Control Problems. -2020. -T.40. -№. 1. -C.32-40.

3. Mamedov I. G., Abdullayeva A. J. Fundamental solution of one boundary value problem on the geometric middle of the domain for the 3d Bianchi integro-differential equation //Journal of Contemporary Applied Mathematics. -2024. -T.14. – №.2. -C.26-37.

4. Mamedov I., Abdullayeva A. Combined boundary value problem for the bianchi intego-differential equation with nonsmooth coefficients and its application in radio engineering weapons. – 2024.

5. Islamov I. J., Mamedov I. G., Abdullayeva A. J. Mathematical Modeling and Experimental Research of Microwave Waveguide Taking into Account Boundary Value

Problems on the Geometric Middle of the Domain //International Journal of Microwave & Optical Technology. – 2024. – Т. 19. – №. 6.

6. Islamov, I. et al. (2025). Hybrid communication models for UAV swarms: Towards scalable and energy-aware network optimization. *Scientific guidelines: Theory and practice of research – Proceedings of the VI International Scientific Conference* (Kyiv, Ukraine, October 3, 2025), pp. 185–195. https://doi.org/10.62731/mcnd-03.10.2025

7. Islamov, I. et al. (2025). Integrating environmental security into defense strategy with a focus on radiological and chemical risks. *Strategic directions of science development: Factors of influence and interaction: Collection of scientific papers with materials of the VII Int. Sci. Conf. (Cherkasy)* (pp. 115–125). https://doi.org/10.62731/mcnd-26.09.2025

8. Vanchenko, O. V. et al. (2025). Technical aspects of wind energy production. In *Global perspectives on multidisciplinary research: Theory and practice: Proceedings of the II International Scientific and Theoretical Conference* (pp. 65–72). Florence, Italy: International Center of Scientific Research. https://doi.org/10.36074/scientia-24.10.2025

9. İskhandarov, X. et al. (2025). Artificial intelligence in logistics operations. In *Topical issues of science development: Proceedings of the VI International Scientific Conference* (pp. 433–442). https://doi.org/10.62731/mcnd-31.10.2025

10. Muradova, E. E. et al. (2025). Analytical evaluation of UAV-based logistical operations in contemporary military systems. In *Topical issues of science development: Proc. of the VI Int. Scientific Conf.* (pp. 351–360). https://doi.org/10.62731/mcnd-31.10.2025

11. Akhundov, R., & Hashimov, E. (2025). Enhancing the efficiency of the military environmental security system through the implementation of advanced technical means. *In Modeling, Control and Information Technologies,* (No. 8, pp. 348–352) https://doi.org/10.31713/MCIT.2025.108

12. Tahirov, R. K. et al. (2024). Environmental aspects of information technology implementation. In *Problems of Informatization: Proceedings of the 12th International Scientific and Technical Conference* (Vol. 3, pp. 138–139).

13. Kovtun, A. V. et al. (2025). Techno-economic assessment of a hybrid solar, wind, and biomass system for suburban power supply. In *The driving force of science and trends in its development: Collection of scientific papers «SCIENTIA» with proceedings of the IX International Scientific and Theoretical Conference* (pp. 112–119). London, England: International Center of Scientific Research. https://doi.org/10.36074/scientia-17.10.2025

14. Salmanov, E. I. et al. (2025). Ways to improve logistical support in the Azerbaijani Army. In *The driving force of science and trends in its development: Collection of scientific papers «SCIENTIA» with proceedings of the IX International Scientific and Theoretical Conference* (pp. 88–95). London, England: International Center of Scientific Research. https://doi.org/10.36074/scientia-17.10.2025

15. Huseyn-Zada, K. et al. (2025). Spatial patterns of automobile emissions in urban areas: A GIS-based study of Baku. In *Development of scientific thought in the post-industrial society: Modern discourse: Proceedings of the VIII Int. Scientific Conference* (pp. 170–179). Khmelnytskyi, Ukraine: Ukrlogos Group. https://doi.org/10.62731/mcnd-17.10.2025

16. Islamov, I. et al. (2025). The use of unmanned systems and artificial intelligence to enhance radiation and chemical safety in military ecology. In *Innovations and the scientific potential of the world: Proceedings of the VII International Scientific Conference* (pp. 183–192). Sumy, Ukraine: Ukrlogos Group. https://doi.org/10.62731/mcnd-10.10.2025

17. Huseynov, M. et al. (2025). Application of modern multi-sensor technologies for ground target detection. In *Innovations and the scientific potential of the world: Proceedings of the VII International Scientific Conference* (pp. 172–182). Sumy, Ukraine: Ukrlogos Group. https://doi.org/10.62731/mcnd-10.10.2025

MULTISENSOR DETECTION ARCHITECTURES ON UAV PLATFORMS: METHODOLOGY, INDICATORS AND IMPLEMENTATION IN AZERBAIJAN

Huseynov B.S., Muradov S.A., Akhundov R.G.
National Defense University, Baku Azerbaijan
Hashimov E.G.
Azerbaijan Technical University, Baku, Azerbaijan

This article presents, on a scientific basis, a multisensor, AI-supported integrated detection architecture for the timely and accurate detection of ground targets in modern combat conditions and assesses its application prospects in the context of the needs of the Armed Forces of Azerbaijan. The main hypothesis is that multilayer fusion of radar, LiDAR, infrared, and electro-optical channels, as well as the use of an AI module built on convolutional neural networks and transformers, increases detection probability, reduces the share of false alarms, and ensures real-time stability compared with single-sensor approaches.

The methodological framework is formed by a Sensor Integration Model. In the input stage, radar echoes from the target, optical images, IR thermal signatures, and LiDAR range profiles are collected. In the processing stage, a Doppler filter is applied for radar, Gaussian noise attenuation for LiDAR, and median and Sobel filters for the IR and optical channels. The fusion stage covers three hierarchical levels: pixel-level synthesis, feature-level fusion, and decision-level integration. In the AI module, the detection probability $P_{\text{det}}$is modeled using the vector of sensor outputs and a learned set of parameters. The quality metric

$$\eta = \text{TP}/(\text{TP} + \text{FP} + \text{FN})$$

is adopted, and tests are conducted in the digital twin of a multisensory UAV platform.

The results show that when only the radar channel is used under adverse weather, accuracy is approximately in the 71–73 percent range, whereas radar combined with IR increases it to about 85 percent, and a complex of radar, LiDAR, IR, and AI achieves an average accuracy of 94 percent. The false-alarm probability drops from 18 percent to 6 percent, and the miss rate decreases from 15 percent to 8 percent. When fusing multisensory streams at 100 Hz, latency is recorded at 62 ms and can be reduced to the 35–40 ms interval with an edge-computing module. The effects of weather and terrain are disaggregated. In fog, the effectiveness of the optical and IR channels decreases by 20–25 percent, but radar and LiDAR compensate for part of this loss. In forested and mountainous areas, LiDAR detects subsurface or partially occluded objects more consistently. The proposed synergy effect is approximated by $\eta = \eta_0 + k \cdot (n_f - 1)$, with k estimated in the 0.08 to 0.12 range. The effectiveness function is written as

$$\eta = W_{\text{out}}/W_{\text{src}} = f(\alpha, \beta, \gamma),$$

allowing separate calibration of the effects of sensor integration, optical transparency, and AI decision optimization. Under these conditions, ηrises from the

0.55–0.65 range in classical systems to the 0.88–0.92 range with AI-enabled multisensor integration. Detection range increases by a factor of 1.8–2.3, and overall stability improves by roughly 30 percent.

From an application perspective, the findings provide a practical roadmap for ecological and tactical security systems. Priority directions include installing multisensor modules on mobile eco-monitoring platforms, integrating LiDAR and IR cameras on UAVs, employing spectral analysis in CBRN reconnaissance, and establishing synchronized radar and EO networks for border surveillance. Joint development with national scientific and industrial centers is considered a strategic line for digitalization and technological autonomy. In conclusion, multisensor fusion with AI support increases detection accuracy, resilience, and real-time performance, reduces false-alarm risk for decision making, and enables adaptive behavior in complex operational conditions.

References

1. Islamov, I. et al. (2025). Hybrid communication models for UAV swarms: Towards scalable and energy-aware network optimization. *Scientific guidelines: Theory and practice of research.* pp. 185–195. https://doi.org/10.62731/mcnd-03.10.2025

2. Tahirov, R. K. et al. (2024). Environmental aspects of information technology implementation. In *Problems of Informatization: Proceedings of the 12th International Scientific and Technical Conference* (Vol. 3, pp. 138–139).

3. Babayev, S. et al. (2025). The impact of unmanned aerial vehicles on the strategy and tactics of modern warfare. In *Modern tools and methods of scientific investigations: Proceedings of the VI International Scientific and Theoretical Conference* (pp. 28–36). Antwerp, Belgium: Scientia. https://doi.org/10.36074/scientia-10.10.2025

4. Talibov, A. M. et al. (2025). The use of unmanned aerial vehicles for monitoring chemical and radiation contamination. In *Current directions of development of information and communication technologies and control tools: Proceedings of the 15th International Scientific and Technical Conference* (Vol. 4, pp. 88-89).

5. Ismayil, I. et al. (2025). Optimization of composite material selection in the design of military UAV wings. Scientific review of the actual events, achievements and problems: Collection of scientific papers «SCIENTIA» with Proc. of the V International Scientific and Theoretical Conference (pp. 107–115) https://doi.org/10.36074/scientia-03.10.2025

6. Islamov, I. et al. (2025). The use of unmanned systems and artificial intelligence to enhance radiation and chemical safety in military ecology. In *Innovations and the scientific potential of the world: Proceedings of the VII International Scientific Conference* (pp. 183–192). Sumy, Ukraine: Ukrlogos Group. https://doi.org/10.62731/mcnd-10.10.2025

7. Tabunenko, V. et al. (2025). The dynamics of UAV flight integrated with route planning. In *Modern tools and methods of scientific investigations: Proceedings of the VI International Scientific and Theoretical Conference* (pp. 46–56). Antwerp, Belgium: Scientia. https://doi.org/10.36074/scientia-10.10.2025

8. İskhandarov, Kh. et al. (2025). Artificial intelligence in logistics operations. In *Topical issues of science development: Proceedings of the VI International Scientific Conference* (pp. 433–442). https://doi.org/10.62731/mcnd-31.10.2025

9. Muradova, E. E. et al. (2025). Analytical evaluation of UAV-based logistical operations in contemporary military systems. In *Topical issues of science development: Proceedings of the VI International Scientific Conference* (pp. 351–360). https://doi.org/10.62731/mcnd-31.10.2025

10. Hasanov, A.H. (2022). Analysis of the effectivness of communication and automated management systems. In *Modern directions of development of information and communication technologies and management tools*, (Vol. 1, pp. 1-4).

11. Hashimov, E.G. et al. (2015). Application of relief digital model for combat operation planning. *Military Knowledge*, *4*, 63-69.

12. Hashimov, E. G. (2021). Some aspects of the combat capabilities and application of modern UAVs. *Baku:"National Security and military knowledges*, (3), 7.

13. Hashimov, E.G. (2017). Application of GIS and seismic location method for detection of invisible military objects /- Baku: Military Publishing House, 2017, 246 p.

14. İbrahimov, B.G. et al. (2022). Research and analysis indicators fiber-optic communication lines using spectral technologies. *Advanced information systems*, *6*(1), 61-64.

15. Ibrahimov, B.G. et al. (2024). Research and analysis mathematical model of the demodulator for assessing the indicators noise immunity telecommunication systems. *Advanced Information Systems*, *8*(4), 20-25.

16. Bayramov, A.A. et al (2018). The supervisory control systems deployment in mountainous terrain. In *VIII Int. Conf."Modern development trends of ICT and control methods* (pp. 3-4).

17. Huseynov, M. et al. (2025). Application of modern multi-sensor technologies for ground target detection. In *Innovations and the scientific potential of the world: Proceedings of the VII International Scientific Conference* (pp. 172–182). Sumy, Ukraine. https://doi.org/10.62731/mcnd-10.10.2025

18. Bayramov, A.A. et al. (2016). The detection of invisible objects on the terrain on the basis of GIS technology. *Geography and nature sources*, 124-126.

19. Bayramov, A.A., & Hashimov, E. (2017). The numerical estimation method of a task success of UAV reconnaissance flight in mountainous battle condition. *Сучасні інформаційні системи*, (1,№ 2), 70-73.

20. Bayramov, A.A. (2018). Assessment of invisible areas and military objects in mountainous terrain. *Defence Science Journal*, *68*(4), 343-346.

AI IN LOGISTICS. INTERACTION MECHANISMS AND APPLICATION

İsrayılova N.M.
National Defense University, Baku Azerbaijan

The application of artificial intelligence (AI) in logistics is one of the most dynamic directions of the modern digital economy, and it is no coincidence that in recent years AI-based solutions have rapidly proliferated across subdomains such as supply chain management, transport organization, warehousing systems, and customer services. By its nature, logistics is a complex network in which numerous actors, diverse geographies, fluctuating demand, and constrained resources are managed. In such systems, the participation of intelligent algorithms alongside human reasoning accelerates decision making, reduces errors, and anticipates risks. Unlike traditional planning, the AI-enabled logistics model is agile, data-driven, forecast-oriented, and capable of real-time updates.

AI influences logistic flows along two main lines. The first is optimization. This includes automatic route selection, proper allocation of loads to vehicles, minimization of empty backhauls, coordination of multimodal transport, and consideration of

external factors such as congestion, weather, border crossings, and customs procedures. For example, a reinforcement learning algorithm recalculates the route each time and selects the option that meets a chosen criterion such as minimal fuel consumption or shortest travel time. In doing so, the system does not only rely on a static map. It also incorporates the outcomes of prior shipments, driver behaviors, seasonal variations, and even customer delivery windows. The second line is forecasting. Demand forecasts are produced in line with sales dynamics, pre-season inventory levels in warehouses are determined, and emerging short-term demand hotspots for specific products in specific regions are identified in advance. As a result, logistics transforms from a purely reactive system into a proactively managed one. It is necessary to highlight the interaction mechanism of AI in logistics. At the core of this mechanism lies the consolidation of data within a unified environment. IoT sensors record cargo temperature, vibration levels, and whether a container has been opened. GPS and telemetry systems transmit precise vehicle coordinates. ERP and WMS platforms display the status of orders. The AI platform integrates, cleans, and standardizes all these streams and then forwards them to analytical modules. In the analytical phase, machine learning models detect anomalies, signal the planning module, and assess risk levels.

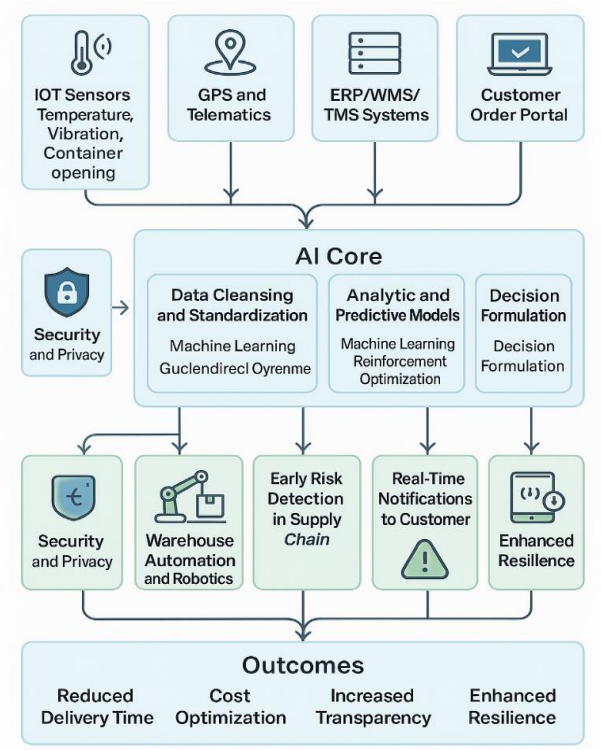

Fig. 1. Integration model of Artificial Intelligence in logistics

In the execution phase, the system is already able to perform certain routine tasks without human instruction. For example, if warehouse capacity exceeds a critical threshold, it automatically generates an additional transport order. If a delay risk emerges, it sends an advance notification to the customer.

The application areas are wide. In warehouse logistics, AI optimizes the routes of robotic picking lines, aligns product placement with ABC classification, and shortens loading and unloading times. In transport logistics, AI-based intelligent dispatching systems distribute orders among carriers in a fair and efficient manner. In strategic supply chain planning, AI builds scenario models and shows the enterprise which alternative routes and contingency schemes should be activated if a given port is closed, if a specific road becomes unusable for military or natural reasons, if prices spike sharply, or if one of the suppliers fails. This is particularly important in unstable regions.

AI brings more than efficiency to logistics. It also creates transparency because a digital trace of all actions is preserved. The customer can see exactly where the order is. The manager can observe in real time which vehicle is delayed more frequently, which route is more costly, and in which warehouse spoilage is more prevalent. This transparency increases mutual trust among participants across the entire chain. At the same time, AI enables the accumulation of large historical datasets on transport operations, which subsequently allows deep learning models to deliver more accurate results.

There are also constraints. Data confidentiality can pose problems, especially in cross-border transport, because AI systems collect information from multiple sources and these data can constitute trade secrets. In addition, since AI models sometimes operate as black boxes, managers may struggle to explain how a given decision was reached. This can be unacceptable for regulators. Therefore, the deployment of explainable AI approaches, auditable algorithms, and cyber-resilient cloud infrastructure is essential in parallel with AI adoption in logistics. Workforce development should be treated as a distinct line of effort, since even the best AI platform will not operate at full potential in the hands of an operator unfamiliar with logistics processes.

The overall conclusion is as follows. AI in logistics should not be viewed merely as a technology applied to isolated modules. It should be implemented as an intelligent management layer spanning the entire supply chain. When this is achieved, in-house systems, partner companies, and international logistics networks communicate in a unified digital language.

This leads to a logistics model that is agile, resilient, transparent, and economically advantageous

References

1. İskhandarov, X. et al. (2025). Artificial intelligence in logistics operations. In *Topical issues of science development: Proceedings of the VI International Scientific Conference* (pp. 433–442). https://doi.org/10.62731/mcnd-31.10.2025

2. Muradova, E. E. et al. (2025). Analytical evaluation of UAV-based logistical operations in contemporary military systems. In *Topical issues of science development:*

Proceedings of the VI International Scientific Conference (pp. 351–360). https://doi.org/10.62731/mcnd-31.10.2025

3. Mammadov, E.S. et al. (2025). Environmental impact of transportation systems: Challenges and sustainable solutions. In *Scientific review of the actual events, achievements and problems: Proceedings of the V International Scientific and Theoretical Conference* (pp. 120–128). https://doi.org/10.36074/scientia-03.10.2025

4. Huseyn-Zada, K. et al. (2025). Spatial patterns of automobile emissions in urban areas: A GIS-based study of Baku. In *Development of scientific thought in the post-industrial society: Modern discourse: Proceedings of the VIII International Scientific Conference* (pp. 170–179). Khmelnytskyi, Ukraine: Ukrlogos Group. https://doi.org/10.62731/mcnd-17.10.2025

5. Salmanov, E. I. et al. (2025). Ways to improve logistical support in the Azerbaijani Army. In *The driving force of science and trends in its development: Collection of scientific papers «SCIENTIA» with proceedings of the IX International Scientific and Theoretical Conference* (pp. 88–95). London, England: International Center of Scientific Research. https://doi.org/10.36074/scientia-17.10.2025

6. Tahirov, R. K. et al. (2024). Environmental aspects of information technology implementation. In *Problems of Informatization: Proceedings of the 12th International Scientific and Technical Conference* (Vol. 3, pp. 138–139).

7. Ismayil, I. et al. (2025). Optimization of composite material selection in the design of military UAV wings. İn *Scientific review of the actual events, achievements and problems*. pp. 107–115. https://doi.org/10.36074/scientia-03.10.2025

8. Mammadov, R. et al. (2024). Enhancing special forces management efficiency in modern operations. In *Problems of Informatization: Proceedings of the 12th International Scientific and Technical Conference* (Vol. 3, pp. 31–32).

9. Jabrayilov, A. R. et al. (2025). Prospects for creating closed ecological life support systems. İn *Current directions of development of information and communication technologies and control tools* (Vol. 4, pp. 92–93).

10. Talibov, A.M. et al. (2023, May). Optimal placement of logistics centers in the Republic of Azerbaijan. In *2nd International Conference on Problems of Logistics, Management and Operation in The East-West Transport Corridor*. (pp. 24-26).

11. Talibov, A.M. (2024). Vehicle transport cost calculation method. *In* Current directions of development of information and communication technologies and control tools. (Vol. 2, pp. 3-6).

12. Garayev, M., & Hashimov, E. (2025). BALANCING INNOVATION AND SUSTAINABILITY: THE ECOLOGICAL RISKS OF MODERN TECHNOLOGIES. *Collection of Scientific Papers «SCIENTIA»*, pp.52–59. Retrieved from https://previous.scientia.report/index.php/archive/article/view/3001

13. Muradova E. E. Modern threats to financial and economic stability. – 2025.

14. Ibrahimov, B. G. (2025). Special purpose machine learning and data mining methods. İn *Current directions of development of information and communication technologies and control tools.*

15. Hashimov E., Talibov A., Iskandarov K. The Socioeconomic Impact of the Zangezur Corridor on the South Caucasus Region //Social Development and Security. – 2025. – Т. 15. – №. 4. – С. 1-18.

16. Muradova E.E.Financial and economic security in the era of global risks. *İn* New technologies - for the protection of air space. – Kh.: KhNUPS named after I. Kozheduba, 2025. - p.717-718

SYSTEM-LEVEL OPTIMIZATION OF AZERBAIJANI WIND PROJECTS: AEP, LCOE, AND GRID STABILITY

İsmayil İ., Akhundov R.G.
National Defense University, Baku Azerbaijan
Garayev M.F., Hashimov E.G.
Azerbaijan Technical University, Baku, Azerbaijan

This article presents an optimization method that integrates resource mapping, aerodynamic layout, operations, and grid integration within a unified framework for a typical wind farm in Azerbaijan.

The objective is to justify analytically that LCOE can be reduced while maintaining system reliability.

The central question is whether joint optimization of resource calibration, siting, and operational management can sustainably lower LCOE through gains in AEP and reduced power variability.

The methodological approach is modular yet presented as a sequential, integrated process. In stage one, a high-accuracy resource characterization is built from long-term reanalysis, a local anemometric mast, Doppler lidar, and SCADA telemetry.

Data quality control is performed, outliers are removed, gaps are statistically infilled, and sensor calibration is verified. Wind speed is parameterized with a Weibull model; k and c are estimated by maximum likelihood. Ten-meter measurements are extrapolated to hub height using the power law or the Monin Obukhov profile.

Dominant directions are represented with a wind rose.

In stage two, site constraints are converted into a digital mask, including ecological buffers, residential areas, aviation and military airspace, geotechnical risks, and grid connection points.

An initial turbine array is configured in accordance with the wind rose, with spacings in rotor-diameter units. Wake effects are modeled by direction and speed classes.

Effective wind speed and turbulence are convolved with the turbine power curve to compute AEP_gross. Electrical losses, availability, and grid constraints are tracked separately.

In stage three, global search algorithms minimize the objective function. The target is to minimize LCOE, equivalently to maximize AEP_net over CAPEX_effective.

Net annual energy AEP_net equals AEP_gross multiplied by a composite loss factor accounting for wake, electrical, curtailment, and availability effects. Turbine selection and tower height are aligned to the resource distribution. The capacity factor CF is estimated from the convolution of the Weibull distribution with the power curve. Increasing height adds CAPEX, but LCOE decreases when CF gains dominate.

In stage four, operations are optimized. Short-term power forecasts use an ensemble of NWP, SCADA, and short horizon lidar and are calibrated by MAE and RMSE.

SCADA-based anomaly detection, vibration monitoring, and oil analytics enable early fault identification. Service intervals are scheduled via a CMMS, and availability is managed as a KPI. For grid integration, reactive power control follows a Q-U-Q characteristic.

Ten-to-thirty-minute storage buffers short ramps to meet a $dP/dt \leq r\_max$ constraint. Harmonic distortion is maintained within standard limits.

Results show that resource calibration reduces bias in hub-height speed and turbulence, improves power-curve conformity, and lowers turbine-selection risk. Aerodynamically efficient layouts reduce wake losses but must be co-optimized with cable and logistics costs.

Forecasting and predictive maintenance increase availability while reducing balancing costs and forced curtailment. Sensitivity analysis indicates that LCOE is most sensitive to CF and availability, while CAPEX and OPEX impacts are scenario dependent.

In conclusion, joint optimization of resource, aerodynamics, operations, and grid decisions increases AEP and reduces LCOE while preserving grid reliability. It provides a practical development trajectory for near- and medium-term onshore projects and for medium to long term offshore wind potential.

References

1. İvanchenko, O. V. et al. (2025). Technical aspects of wind energy production. In *Global perspectives on multidisciplinary research: Theory and practice*. pp. 65–72. https://doi.org/10.36074/scientia-24.10.2025

2. Tahirov, R. K. et al. (2024). Environmental aspects of information technology implementation. In *Problems of Informatization: Proceedings of the 12th International Scientific and Technical Conference* (Vol. 3, pp. 138–139).

3. Ismayil, I. et al. (2025). Optimization of composite material selection in the design of military UAV wings. İn Scientific review of the actual events, achievements and problems. pp. 107–115. https://doi.org/10.36074/scientia-03.10.2025

4. Akhundov, E.F. et al. (2023). Increasing Efficiency of Operation of Shut-Off Valves in Pipelines. *International Organization*.

5. Garayev, M. et al. (2025). Wind, sun, and hydroenergy: a look into Azerbaijan's green energy future. *Collection of Scientific Papers «ΛΟΓΟΣ»*, 125–133.

6. İsmayil, İsmayil. (2025). Security and protection of Azerbaijan's oil and gas pipelines: cybersecurity and risk management approaches. *Матеріали конференцій МЦНД*, 136–144. https://doi.org/10.62731/mcnd-11.07.2025.004

7. Amanov, Y.K. et al. (2025) Tribological characterization of surface layer hardness and wear resistance under abrasive scratching. International Journal on Technical and Physical Problems of Engineering, vol.17, N3. p.414-420.

8. Tabunenko, V. et al. (2025). The dynamics of UAV flight integrated with route planning. In *Modern tools and methods of scientific investigations*. pp. 46–56. https://doi.org/10.36074/scientia-10.10.2025

ІНТЕГРАЦІЯ ВАГОВИХ СИСТЕМ ТИПУ КВ В ІНФРАСТРУКТУРУ ТРАНСПОРТНИХ ТЕРМІНАЛІВ

Черепащук Г.О., Потильчак О.П.
Національний аерокосмічний університет
«Харківський авіаційний інститут», Харків, Україна
Бикова Т.В.
Харківський національний університет ім. В. Н. Каразіна, Харків, Україна

Метою доповіді є вирішення задачі інтеграції вагових систем для зважування контейнерів у інфраструктуру сучасних транспортних терміналів. **В доповіді** наводяться відомості про специфіку зважування контейнерів у транспортних терміналах, про принцип дії та особливості будови вагових систем для зважування контейнерів, а також про способи інтеграції вагових систем у інфраструктуру транспортних терміналів.

Контейнерні перевезення є основою сучасної міжнародної логістики, забезпечуючи своєчасне, надійне та стандартизоване транспортування товарів на далекі відстані. Саме завдяки широкому застосуванню контейнерів стало можливим значне скорочення часу доставки, зменшення витрат на навантажувально-розвантажувальні операції, а також підвищення рівня збереження вантажів. Контейнери дозволяють здійснювати перевезення різними видами транспорту без розпакування, що значно підвищує ефективність логістичних операцій. У результаті контейнерні перевезення стали ключовим інструментом у системі міжнародної торгівлі, відіграючи важливу роль у функціонуванні глобальних ланцюгів постачання.

Невід'ємною частиною ефективного управління такими перевезеннями є точне визначення ваги контейнерів. Невідповідність заявленої та фактичної ваги вантажу може призвести до критичних наслідків – порушення норм безпеки, перевантаження транспортних засобів, нерівномірного розподілу навантаження, що підвищує ризик аварій. Крім того, помилки під час зважування можуть спричинити логістичні затримки, фінансові штрафи, пошкодження вантажу, порушення графіків постачання та проблеми з митним оформленням. У зв'язку з цим забезпечення точного зважування контейнерів є не лише технічним питанням, а й стратегічною необхідністю для будь-якої логістичної системи [1].

Положення центру мас (ЦМ) контейнера, як і його вага, є одним із ключових параметрів, що впливають на безпеку перевезення. Координати ЦМ визначають рівномірність навантаження на транспортний засіб, стабільність під час руху та опору зовнішнім силам, наприклад, вітру, хвилям чи інерційним навантаженням. Особливо критичним є контроль ЦМ у випадках перевезення великої кількості вантажів, коли сумарна вага контейнерів може сягати сотень або навіть тисяч тон.

Неправильне визначення або неконтрольоване зміщення ЦМ контейнера може мати серйозні наслідки: перекіс контейнера під час навантаження, нерівномірний тиск на стики вагонів або палубу судна, підвищене

навантаження на окремі елементи конструкції транспортного засобу. У найгіршому випадку це може призвести до втрати стійкості судна, крену або навіть його перекидання, а також до аварій на залізничному транспорті, особливо під час гальмування, на поворотах чи при русі нерівними ділянками колії [2].

Для вирішення задач визначення ваги та координат ЦМ контейнерів авторами запропоновано вагові системи типу КВ [3, 4], зокрема, КВ-40Р і КВ-60Р, структурну схему яких зображено на рис. 1.

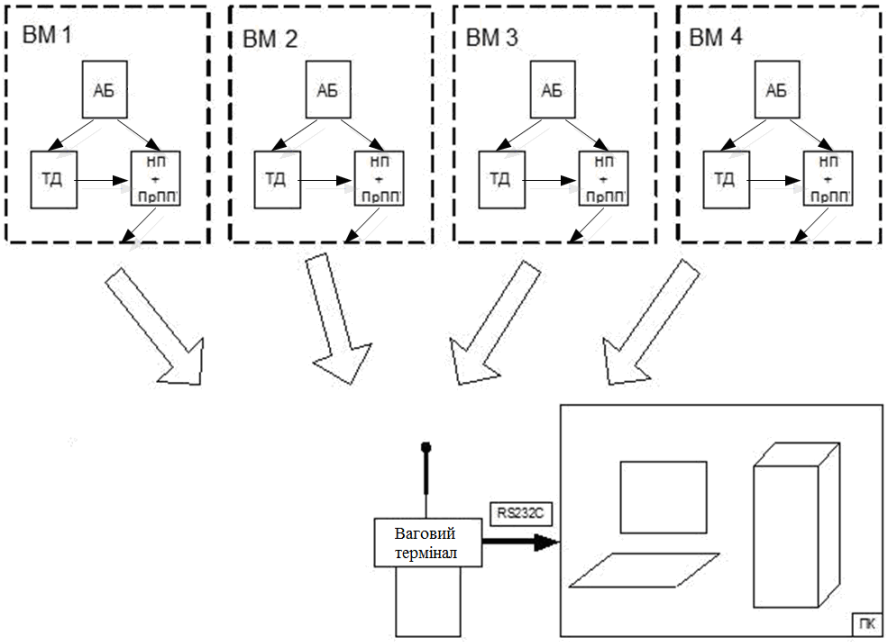

Рис. 1. Структурна схема вагової системи типу КВ

Вагові системи типу КВ призначені для

- статичного зважування вантажних контейнерів;
- контролю рівномірності завантаження контейнера, який реалізовано шляхом визначення відхилення ЦМ вантажного контейнера відносно його осей симетрії;
- поетапного зважування та визначення відхилення ЦМ під час завантаження контейнера;
- контролю ваги під час приймання контейнера.

Вагова система типу КВ складається з чотирьох окремих вагових модулів (ВМ) та вагового терміналу (ВТ).

Кожен ВМ містить:

тензодатчик (ТД) фірми FLINTEC,

нормуючий перетворювач (НП) з приймально-передавальним пристроєм (ПрПП);

акумуляторний блок (АБ).

Представник даного типу, вагова система КВ-40Р, має такі основні технічні характеристики:

- верхня межа зважування вагового модуля: 10000 кг;
- верхня межа зважування системи: 40000 кг;
- ціна повірювальної поділки вагового модуля: 20 кг;
- ціна повірювальної поділки системи: 100 кг;
- клас точності згідно з ДСТУ EN 45501: 2017: середній (III);
- дальність дії радіоканалу: 100 м.

Використання вагових систем типу КВ дозволяє удосконалити процес визначення параметрів завантаження контейнера, завдяки таким перевагам, як:

- модульна структура,
- передавання даних по радіоканалу
- наявність функції контролю рівномірності завантаження контейнера.

Інтеграція вагової системи в інфраструктуру підприємства, зокрема, транспортного терміналу, є критичним кроком на шляху до автоматизації та оптимізації логістичних процесів.

Сучасні вимоги до точності, швидкості обробки даних і безпеки обміну інформацією створюють необхідність інтеграції вагових систем до систем управління і зберігання інформації.

Завдяки такій інтеграції, вагові системи не лише виконують свою основну задачу – вимірювання ваги, але й стають частиною загальної технологічної мережі терміналу.

Вони забезпечують миттєвий обмін даними з іншими системами, що дозволяє контролювати логістику, а також отримувати точні звіти для прийняття рішень.

При цьому вагова система може передавати такі дані:

- значення ваги, виміряні кожним ваговим модулем;
- сумарне значення ваги контейнера (вага брутто);
- вага порожнього контейнера (вага тари);
- вага вантажу (вага нетто);
- поздовжнє центрування контейнера (відносне зміщення ЦМ у відсотках від довжини контейнера);
- поперечне центрування контейнера (відносне зміщення ЦМ у відсотках від ширини контейнера);
- ступінь заряду акумуляторних батарей вагових модулів і вагового терміналу;
- ідентифікатор контейнера;
- код статусу (норма, перевантаження, нерівномірне завантаження контейнера);
- мітка часу.

Схему інтеграції вагової системи типу КВ зображено на рис. 2.

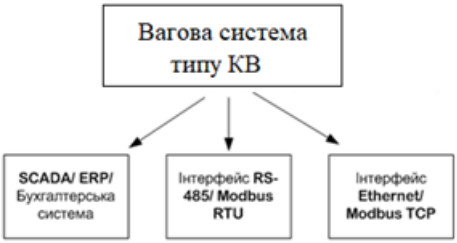

Рис. 2. Схема інтеграції вагової системи типу КВ

На рис. 2 зображено три можливі рівні інтеграції вагової системи у інфраструктуру транспортного терміналу:

- з'єднання вагової системи з промисловим контролером через послідовний інтерфейс RS-485 (протокол Modbus RTU). Промисловий контролер у цьому випадку є проміжною ланкою між ваговою системою та інформаційною мережею транспортного терміналу;
- безпосередня інтеграція вагової системи в інформаційну мережу транспортного терміналу з використанням мережі Ethernet (протокол Modbus TCP/IP);
- вбудовування вагової системи в SCADA-систему управління транспортними процесами з використанням технологій IoT [5].

Вибір рівня інтеграції залежить від особливостей побудови інформаційної інфраструктури конкретного транспортного терміналу. Реалізація інтеграції вагової системи типу КВ у інфраструктуру транспортного терміналу дозволить підвищити ефективність її використання для визначення параметрів завантаження контейнерів.

Список літератури

1. Андрієнко М.М. Оцінка ефективності контейнерних перевезень на транспорті. *Ефективна економіка*. 2011. №10. URL: http://nbuv.gov.ua/UJRN/efek_2011_10_9

2. Стрелко О.Г., Бердниченко Ю.А., Вознюк В.С., Ковальський І.Л. Аналіз розвитку контейнерних перевезень залізничним транспортом в Україні. *Наукові праці Вінницького національного технічного університету*. 2020. № 2. doi: https://doi.org/10.31649/2307-5376-2020-2-39-44

3. Черепащук Г.О., Потильчак О.П., Бикова Т.В. Оптимізація процесу завантаження контейнерів під час контейнерних перевезень. *Transport Development*. 2024. № 2(21), p. 100 – 110. doi: https://doi.org/10.33082/td.2024.2-21.09

4. Черепащук Г.О., Потильчак О.П., Бикова Т.В. Застосування багатомодульних тензометричних ваг з радіоканалом під час завантаження контейнерів. *XVIII International scientific and practical conference «Innovations in Scientific Research: World Experience and Realities»* (April 10-12, 2024) Riga, Latvia. International Scientific Unity, 2024. PP. 218 – 220.

5. SCADA-системи: основа ефективного управління та моніторингу процесів. URL: http://www.alectro.com.ua/blog/scada/

МОДЕЛЬ ЕКСПЛУАТАЦІЇ ТРАНСПОРТНИХ ЗАСОБІВ ДЛЯ КОНТРОЛЮ ЇХ ТЕХНІЧНОГО СТАНУ

Бурак А.В., Воловоденко Ю.М., Мосійчук М.В.
Національний технічний університет «ХПІ», Харків, Україна

Розроблення математичних моделей експлуатації сучасних технічних комплексів, у тому числі транспортних засобів, базується на використанні теорії систем і методів нелінійного програмування [1, 2]. Однак модель експлуатації із застосуванням теорії систем має головний недолік, який полягає у розгляді складових комплексу як окремих елементів дослідження, та не досліджує комплекс у цілому [1, 3]. Це призводить до внесення значних похибок у отримані характеристики експлуатації транспортних засобів, що є причиною помилкового визначення їх технічного стану.

Метою доповіді є розробка моделі експлуатації транспортних засобів для контролю їх технічного стану.

У доповіді показано, що однією зі складових удосконалення системи контролю технічного стану транспортних засобів є визначення оптимальних параметрів (основних характеристик) експлуатації, у тому числі параметрів контролю. Одним з найбільш ефективних способів розв'язання задачі визначення оптимальних параметрів експлуатації транспортних засобів є розроблення (удосконалення) математичної моделі їх експлуатації. Запропоновано використання теорії надійності та методів невизначеності для розроблення моделі експлуатації транспортних засобів для дослідження їх технічного стану.. Для статистичного оцінювання (за результатами імітації) функціональної готовності системи експлуатації транспортних засобів необхідно в деякі випадкові моменти часу знати її стан. Для цього запропоновано використання методу статистичного моделювання. Така модель експлуатації більш точно описується математичним апаратом теорії надійності у поєднанні з методами невизначеності.

Список літератури

1. Brytov O., Bieliaiev D., Kukobko S. and etc. Justification of the Method of Evaluation of the Efficiency of Air Reconnaissance by Unmanned Aviation of Ground (Sea) Objects. *Proceedings of the 3rd International Scientific and Practical Conference "Scientific Trends and Trends in The Context of Globalization"*. 2021. P. 431-434. DOI: https://doi.org/10.51582/interconf.21-22.12.2021.050

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

3. Dzhus V., Roshchupkin Y., Kukobko S. and etc. Estimation of Noise Radiance Point Sources Multichannel Direction Finding Systems Resolution by Linear Prediction Method. *Information Processing Systems*. 2021. Is. 4 (167). P. 19-26. DOI: https://doi.org/10.30748/soi.2021.167.02

МЕТОД КОНТРОЛЮ ТЕХНІЧНОГО СТАНУ СКЛАДОВИХ ЕЛЕКТРООБЛАДНАННЯ ТРАНСПОРТНИХ ЗАСОБІВ

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

Забезпечення надійної та безпечної експлуатації різних видів сучасних транспортних засобів залежить від справності складових електрообладнання та досягається застосуванням раціональної системи контролю технічного стану. Система технічного контролю при цьому повинна включати періодичний контроль функціонування, пошук дефектів і несправності у роботі складових електрообладнання, визначення ступеня небезпеки дефектів і оцінювання остаточного ресурсу обладнання [1, 2].

До основних вимог сучасних методів контролю технічного стану складових електрообладнання транспортних засобів належать:

рівень достовірності виявлення несправності та можливих пошкоджень двигунів, його складових вузлів і агрегатів (не нижче 90 %) [3];

своєчасне виявлення основних електричних і механічних дефектів за рахунок використання спеціалізованих датчиків [4];

проведення необхідних вимірювань при контролі технічного стану дистанційно;

низька трудомісткість і простота технічного контролю складових електрообладнання (проведення вимірювань визначених параметрів);

проведення аналітичної обробки отриманих результатів вимірювань за короткий час для обґрунтованого рішення про технічний стан (застосування інформаційно-вимірювальних систем і комплексів).

Метою доповіді є проведення аналізу методів контролю технічного стану електрообладнання транспортних засобів і обґрунтування раціонального для застосування у сучасних засобах.

У доповіді наведено складові електрообладнання сучасних транспортних засобів, які є складною технічною системою, що складається з джерела постійного струму, генератора і великої кількості вузлів, агрегатів і окремих деталей, які взаємодіють між собою [2, 3]. Широкий частотний діапазон коливальних процесів в транспортному засобі обумовлює швидку реакцію віброакустичного сигналу на зміну технічного стану. Це є визначальним в аварійних ситуаціях [2, 4]. Складові (елементи, вузли та агрегати) електрообладнання, від надійності та безаварійного функціонування яких залежить справність транспортного засобу, вимагають особливої уваги. Актуальним є своєчасне виявлення та не допущення поширення дефектів, які стануть причиною виходу з ладу складових електрообладнання, що може привести до втрати працездатності транспортного засобу [4].

У доповіді обґрунтовано сутність проблеми віброакустичної діагностики складових електрообладнання, яка полягає в розробці та практичній реалізації алгоритмів оцінювання параметрів технічного стану складових без їх розбирання за характеристиками віброакустичних процесів, які

супроводжують його функціонування [3]. Для складових електрообладнання транспортного засобу виділимо основні джерела виникнення вібрації [1, 4]:

коливання від незбалансованих обертових мас;
вібрації, обумовлені зубчастими передачами редукторів;
коливання підшипників, власні коливання лопаток, дисків, корпусів;
аеродинамічні коливання;
вібрації, порушувані процесами в газо-повітряному тракті;
вібрації агрегатів і трубопроводів.

Запропоновано метод синтезу вібраційного вимірювального сигналу, в основі якого є представлений алгоритм обчислення оцінки дисперсії вимірювального вібраційного сигналу. Зміна параметрів вібраційного вимірювального сигналу під час функціонування елементів електрообладнання є маркерами дефектів (несправності) транспортних засобів. Визначено аналітичні залежності, які визначають основні параметри вібраційного вимірювального сигналу. Наведено результати комп'ютерного моделювання запропонованих фільтрів, результати якого підтвердили доцільність використання отриманих результатів. В подальших роботах планується представити результати дослідження різних видів модуляції часових параметрів синтезованого вібраційного вимірювального сигналу для дистанційного контролю та діагностування технічного стану елементів електрообладнання є маркерами дефектів (несправності) транспортних засобів. Це дозволить підвищити оперативність виявлення можливих відмов (за рахунок відсутності потреби у демонтуванні елементів, вузлів і агрегатів транспортного засобу), тобто підвищити їх ефективність функціонування.

Список літератури

1. Brytov O., Bieliaiev D., Kukobko S. and etc. Justification of the Method of Evaluation of the Efficiency of Air Reconnaissance by Unmanned Aviation of Ground (Sea) Objects. *Proceedings of the 3rd International Scientific and Practical Conference "Scientific Trends and Trends in The Context of Globalization"*. 2021. P. 431-434. DOI: https://doi.org/10.51582/interconf.21-22.12.2021.050

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

3. Dzhus V., Roshchupkin Y., Kukobko S. and etc. Estimation of Noise Radiance Point Sources Multichannel Direction Finding Systems Resolution by Linear Prediction Method. *Information Processing Systems*. 2021. Is. 4 (167). P. 19-26. DOI: https://doi.org/10.30748/soi.2021.167.02

4. 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.

ВИКОРИСТАННЯ БЕЗДРОТОВИХ ТЕХНОЛОГІЙ У ПОБУДОВІ МОБІЛЬНИХ ВИМІРЮВАЛЬНИХ КОМПЛЕКСІВ

Ні Я.С., Ні О.В., Шостак М.В., Шостак В.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні мобільні вимірювальні комплекси (МВК) є важливою складовою інфраструктури для моніторингу, контролю та діагностики різноманітних технічних та природних об'єктів. Їх застосування охоплює промислові підприємства, транспортні системи, енергетичні мережі та екологічний контроль. В умовах швидкого розвитку бездротових технологій спостерігається тенденція до створення компактних, автономних та високоефективних МВК, що забезпечують оперативне збирання, обробку та передавання даних у реальному часі. Використання бездротових технологій, таких як Wi-Fi, LTE/5G, LoRaWAN та Zigbee, дозволяє розробляти мобільні комплекси без потреби прокладання складної кабельної інфраструктури. Це особливо актуально для польових вимірювань, де швидкість розгортання та гнучкість системи є критично важливими. Бездротові технології дозволяють забезпечити масштабованість мережі сенсорів, інтеграцію з існуючими інформаційними системами та оперативне реагування на зміни параметрів навколишнього середовища чи об'єкта контролю. Однією з основних переваг бездротових МВК є можливість створення розподілених систем збору даних. Кожен сенсорний вузол може автономно вимірювати параметри, обробляти сигнали та передавати результати на центральний сервер або в хмарне середовище для подальшого аналізу. Такий підхід забезпечує стійкість до відмов окремих вузлів, знижує ризик втрати інформації та дозволяє оптимізувати енергоспоживання. Застосування мобільних МВК з бездротовими технологіями особливо ефективне у складних умовах, таких як польові експедиції, об'єкти з обмеженим доступом, аварійні або воєнні ситуації. Використання технологій 5G забезпечує високу пропускну здатність та низьку затримку передачі даних, що дозволяє реалізувати оперативний моніторинг у режимі реального часу. LoRaWAN та Zigbee, у свою чергу, забезпечують енергоефективну передачу на великі відстані для сенсорних мереж з низьким обсягом даних.

Сучасні дослідження показують, що інтеграція бездротових технологій з мобільними платформами, такими як дрони, автомобілі або роботизовані пристрої, дозволяє розширювати функціональні можливості МВК. Дрони можуть використовуватися для оперативного картографування та контролю важкодоступних об'єктів, автомобільні платформи – для вимірювань на транспортній інфраструктурі, а стаціонарні мобільні вузли – для моніторингу параметрів навколишнього середовища. Одним із ключових аспектів є забезпечення надійності та безпеки передачі даних у бездротових МВК. Для цього застосовуються методи шифрування, аутентифікації та захисту від перешкод, що особливо актуально у воєнний час або на об'єктах з підвищеними вимогами до безпеки інформації. Крім того, інтеграція з хмарними платформами дозволяє проводити аналіз великих обсягів даних, застосовувати алгоритми

машинного навчання для прогнозування та автоматизованого прийняття рішень. Використання бездротових технологій у мобільних вимірювальних комплексах також забезпечує підвищення ефективності ресурсів. Знижується потреба у великій кабельній інфраструктурі, зменшується час на розгортання системи та скорочується обсяг технічного обслуговування. Це дозволяє значно зменшити експлуатаційні витрати та підвищити мобільність комплексів, забезпечуючи їх використання у різних умовах і середовищах.

Метою доповіді є дослідження сучасних бездротових технологій у контексті побудови мобільних вимірювальних комплексів, аналіз їх переваг, обмежень та перспектив розвитку для забезпечення ефективного і безпечного збору, обробки та передавання даних. У доповіді наведено огляд існуючих технологій бездротового зв'язку, проаналізовано особливості інтеграції мобільних платформ та сенсорних мереж, оцінено ефективність використання різних стандартів для конкретних умов застосування та запропоновано рекомендації щодо побудови стійких, масштабованих і енергоефективних МВК.

Список літератури

1. Петренко О.В., Іванченко М.Д. Бездротові технології у мобільних вимірювальних системах: сучасний стан та перспективи. – Харків: Радіоелектроніка, 2023. – 184 с. DOI: 10.34725/wireless.2023.011

2. Rault T., Bouabdallah A., Challal Y. Energy efficiency in wireless sensor networks: A top-down survey. Computer Networks. – 2022. – 67, P. 104–122. DOI: 10.1016/j.comnet.2014.10.003

3. Gupta L., Jain R., Vaszkun G. Survey of important issues in UAV communication networks. IEEE Communications Surveys & Tutorials. – 2023. – 18(2). – P. 1123–1152. DOI: 10.1109/COMST.2015.2475653

4. LoRa Alliance. LoRaWAN Specification. 2023. DOI: 10.14778/3238816.3238820

5. Міністерство цифрової трансформації України. Розвиток бездротових мереж для мобільних систем моніторингу. – Київ, 2023. DOI: 10.37017/mdc.gov.ua.2023.045

КОРИГУВАННЯ ЧАСТОТНОЇ ХАРАКТЕРИСТИКИ ВИМІРЮВАЛЬНОГО КАНАЛУ ЗА ДОПОМОГОЮ ОБЕРНЕНОГО АДАПТИВНОГО МОДЕЛЮВАННЯ

Бондар М.С., Запорожець О.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Одним з факторів, які суттєво впливають на похибку вимірювань, є нерівномірність коефіцієнта передачі вимірювального тракту в робочому діапазоні частот. Це призводить до появи додаткової систематичної похибки й спотворення форми вимірюваного сигналу. Одним з ефективних методів розв'язання даної проблеми є використання адаптивного фільтра-компенсатора, що здійснює вирівнювання частотної характеристики вимірювального каналу [1–3]. Розглянута задача є особливо актуальною для інформаційно-вимірювальних систем, у яких переважає цифрова обробка вимірювальної інформації, що дозволяє реалізувати широкий спектр методів цифрової фільтрації сигналів.

Метою доповіді є побудова адаптивної системи вирівнювання частотної характеристики каналу інформаційно-вимірювальної системи та дослідження її властивостей. Вимірювальний канал – це сукупність засобів вимірювальної техніки, засобів зв'язку та інших технічних засобів, призначених для створення сигналу вимірювальної інформації про одну вимірювану величину. Вимірювальний канал є однією з основних складових частин інформаційно-вимірювальної системи. Практика показує, що навіть у смузі пропускання каналу АЧХ не буває ідеально рівномірною, що призводить до появи частотної або динамічної похибки, обумовленої відхиленням реального значення коефіцієнта передачі від його номінального значення. Для вирівнювання частотної характеристики вимірювального каналу пропонується використовувати обернене адаптивне моделювання. Обернена модель динамічної системи з невідомою передаточною функцією являє собою систему з передаточною функцією, яка у деякому смислі є найкращим наближенням функції, оберненої до невідомої передаточної функції. Узагальнену структуру адаптивної системи вирівнювання частотної характеристики вимірювального каналу наведено на рис.1.

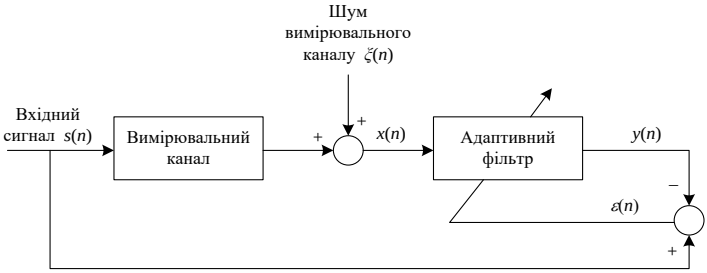

Рис. 1. Структура адаптивної системи вирівнювання частотної характеристики вимірювального каналу

У результаті процесу адаптації коефіцієнти адаптивного фільтра, що є в цьому випадку оберненою моделлю вимірювального каналу, настроюються таким чином, щоб його вихідний сигнал $y(n)$ був найкращим наближенням сигналу $s(n)$ на вході вимірювального каналу. Для налаштування коефіцієнтів адаптивного фільтра пропонується використовувати рекурентний метод найменших квадратів, який працює в реальному часі, забезпечує швидку збіжність оцінок та є стійким до впливу завад. Для дослідження властивостей запропонованої адаптивної системи здійснювалось імітаційне моделювання в середовищі MATLAB з використанням функцій проєктування адаптивних фільтрів бібліотеки DSP System Toolbox та функцій аналізу цифрових фільтрів бібліотеки Signal Processing Toolbox. У процесі моделювання досліджувався вплив виду вхідного сигналу і власних шумів вимірювального каналу на якість адаптивного вирівнювання частотної характеристики. У якості вхідного калібрувального сигналу використовувалися такі види сигналів: 1) періодична послідовність прямокутних імпульсів (меандр); 2) періодична послідовність трикутних імпульсів (пилкоподібний сигнал); 3)

випадковий сигнал (білий гаусівський шум з нульовим середнім значенням); 4) частотно-модульований гармонійний сигнал з лінійним законом зміни частоти (ЛЧМ-сигнал). Результати дослідження наведено в табл. 1 та на рис. 2.

Таблиця 1 – Результати моделювання

Вид вхідного калібрувального сигналу	Максимальне відхилення частотної характеристики від номінальної	Середньоквадратичне відхилення частотної характеристики від номінальної
1. Прямокутні імпульси	0,0630	0,0136
2. Пилкоподібний сигнал	0,0742	0,0227
3. Випадковий сигнал	0,0076	0,0027
4. ЛЧМ-сигнал	0,0076	0,0037

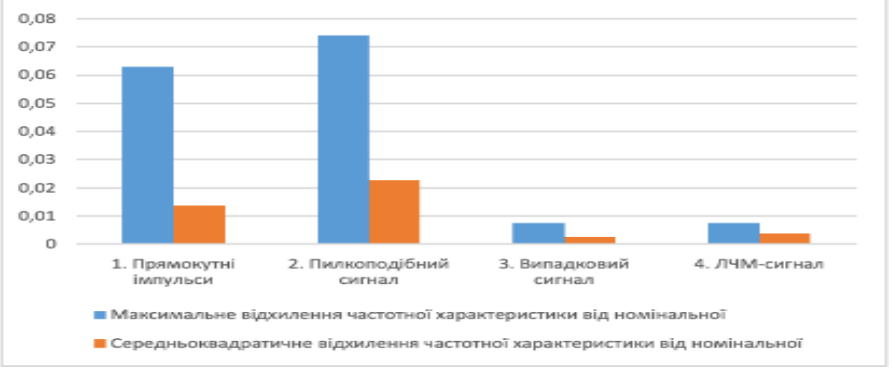

Рис. 2. Результати моделювання адаптивної системи вирівнювання частотної характеристики вимірювального каналу

Аналіз результатів імітаційного моделювання показав, що для адаптивного вирівнювання частотної характеристики вимірювального каналу більш придатними є випадковий і частотно-модульований калібрувальні сигнали, оскільки вони забезпечують кращу якість вирівнювання в порівнянні з періодичними сигналами. У цілому результати імітаційного моделювання повністю підтверджують працездатність запропонованої адаптивної системи вирівнювання частотної характеристики і узгоджуються з теоретичними викладками. Практичне значення дослідження полягає в тому, що використання запропонованого адаптивного коректора дозволить істотно зменшити систематичну похибку динамічних вимірювань, викликану нерівномірністю частотної характеристики вимірювального каналу.

Список літератури

1. Widrow B., Stearns S. D. Adaptive signal processing. Prentice-Hall, 1985. 474 p.
2. Запорожец О. В. Коррекция частотной характеристики измерительного канала с помощью адаптивного фильтра. *Системи обробки інформації*. 2007. Вип. 9(67). С. 52–55.
3. Запорожец О. В. Адаптивное выравнивание частотной характеристики канала информационно-измерительной системы. *Автоматизированные системы управления и приборы автоматики*. 2007. № 141. С. 96-101.

АЛГОРИТМ ФУНКЦІОНУВАННЯ ПЕРСПЕКТИВНОЇ ПЛІС-ТЕХНОЛОГІЇ ДЛЯ ЗАДАЧ SMART GRID

Бовчалюк С.Я., Комендант А.А.
Харківський національний університет радіоелектроніки, Харків, Україна

Постійне зростання складності енергетичних систем і перехід до концепції Smart Grid потребують створення високопродуктивних контролерів для моніторингу, аналізу та керування потоками енергії в режимі реального часу. Традиційні контролери, побудовані на базі мікропроцесорів або цифрових сигнальних процесорів, не забезпечують необхідної швидкодії при обробці великих обсягів даних і виконанні багатопотокових операцій.

Метою доповіді є розробка ПЛІС-технології та алгоритму її функціонування для вирішення задач інтелектуальних енергетичних мереж Smart Grid.

В [2] показано, що одним із перспективних напрямів Smart Grid є застосування ПЛІС, що дозволяють реалізувати адаптивну логіку керування на апаратному рівні. Це відкриває можливості для створення перспективних технологій на базі ПЛІС-контролерів паралельної дії, що здатні динамічно реагувати на зміни параметрів енергомережі, мінімізувати часові затримки та підвищувати стабільність роботи системи.

У роботі пропонується алгоритм функціонування ПЛІС-контролера паралельної дії, що реалізує поетапну обробку інформаційних потоків: - збір даних з датчиків енергомережі; - попередня фільтрація сигналів; - аналіз параметрів стану мережі; - прийняття рішень щодо оптимізації режимів роботи; - формування керуючих впливів на виконавчі елементи. Проведено структурно-функціональне моделювання роботи контролера у середовищах MATLAB/Simulink та Xilinx Vivado, що підтвердило ефективність застосування паралельних обчислювальних структур. Результати дослідження показали, що використання ПЛІС може забезпечити суттєве зменшення затримок при обробці даних і підвищення надійності системи керування Smart Grid.

Запропонований підхід може бути використаний для побудови енергоефективних адаптивних систем розподіленого керування, що є важливим кроком до практичної реалізації концепції цифрової енергомережі майбутнього.

Список літератури

1. Allani M.Y., Riahi J., Vergura S., Mami A. “FPGA-Based Controller for a Hybrid Grid-Connected PV/Wind/Battery Power System with AC Load.” Energies, 2021, vol. 14, no. 8, 2108. DOI:10.3390/en14082108.

2. Prakash N. Krishna, Surjith B. “FPGA Based Remote Monitoring System in Smart Grids.” Indian Journal of Science and Technology, 2017, vol. 10, no. 5, pp. 1-5. DOI:10.17485/ijst/2017/v10i5/108829.

СИСТЕМА АВТОМАТИЧНОГО МЕТЕОМОНІТОРИНГУ НА БАЗІ ТЕХНОЛОГІЇ LORA

Бовчалюк С.Я., Жигалкін Є.В.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасному світі моніторинг навколишнього середовища відіграє ключову роль у багатьох сферах людської діяльності – від сільського господарства та екологічного контролю, до прогнозування погодних умов та забезпечення роботи інфраструктури. Зі зростанням кількості джерел даних та потребою у безперервному зборі й передачі інформації, постає питання розробки ефективних автономних систем, здатних працювати у віддалених районах із мінімальним енергоспоживанням. Одним із перспективних напрямів є використання бездротових технологій передачі даних великої дальності, зокрема LoRa (Long Range), яка забезпечує стабільний зв'язок на великих відстанях навіть у складних умовах рельєфу [1].

Метою доповіді є розробка системи автоматичного метеомоніторингу на базі технології LoRa із застосуванням мікроконтролерних модулів сімейства Arduino.

У запропонованій системі один з модулів виконує функцію передавального вузла, що зчитує дані з датчиків та отримує інформацію про стан навколишнього середовища, такі як: температура повітря, вологість, атмосферний тиск. Передавальний вузол розроблено на базі датчика BME280, що забезпечує високу точність вимірювань за низького енергоспоживання. Модулі метеостанції реалізовано на основі Arduino Nano з підключенням LoRa-модуля SX1278 із робочим діапазоном частот 433 МГц. Завдяки низькому енергоспоживанню LoRa, система може функціонувати від автономного живлення (сонячна панель, акумулятор), що дозволить розгортати її у польових умовах. Перевагою розробленої системи є можливість масштабування – тобто підключення кілька передавальних вузлів, до одного приймального центру.

Отже, пропонована система є прикладом ефективного застосування сучасних бездротових рішень для побудови енергоощадних і надійних комплексів, що дозволяють суттєво знизити витрати на розгортання та обслуговування порівняно з традиційними рішеннями на базі GSM чи Wi-Fi. Завдяки простоті інтеграції, гнучкості налаштувань і високій надійності передавання даних, система може бути використана у проектах «розумного міста», для контролю мікроклімату в сільському господарстві, екологічному моніторингу, організації роботи промислових об'єктів, або наукових спостереженнях.

Список літератури

1. Centenaro M., Vangelista L., Zanella A., Zorzi M. Long-range communications in unlicensed bands: the rising stars in the IoT and smart city scenarios / IEEE Wireless Communications. – 2016. – Vol. 23, No. 5. – P. 60–67.

OPTIMIZING REAL TIME DECISION MAKING IN UAVS WITH REINFORCEMENT LEARNING

Mammadov E.S.
National Defense University; Baku, Azerbaijan

This article examines the present application possibilities and near-term prospects of machine learning technologies in unmanned aerial vehicles, with emphasis on autonomy, perception, navigation, decision making, and coordinated multi-UAV operations. The analysis synthesizes results from recent field deployments and simulation studies to show how data driven models increase mission success under uncertainty, reduce operator workload, and expand the feasible envelope of operations in cluttered, dynamic, or communication constrained environments. In perception, supervised and self-supervised learning have enabled robust object detection, terrain classification, and semantic segmentation across diverse weather and illumination conditions by fusing RGB, thermal, LIDAR, radar, and GNSS inertial signals. Learning based visual inertial odometry and event camera pipelines improve state estimation at high angular rates, while learned depth completion stabilizes mapping in scenes with partial observability. In navigation and obstacle avoidance, model predictive control augmented by learned cost maps outperforms rule-based planners in urban canyons and forested areas where GPS is degraded, and end to end imitation learning from expert demonstrations reduces collision risk without hand crafted features.

Reinforcement learning contributes to decision making under nonstationary task and threat models. Algorithms such as Q Learning, DQN, PPO, and SAC learn policies that balance safety, energy, latency, and reward shaped mission objectives such as coverage, time to detect, and probability of intercept. Curriculum learning and domain randomization accelerate training and improve sim to real transfer, while risk sensitive policy optimization constrains tail events that matter for certification and public safety. At the fleet level, collective intelligence and swarm coordination enable distributed task allocation, adaptive formation control, and resilient coverage when individual platforms fail or communication links are intermittent. Market based assignments, consensus protocols, and graph neural network controllers maintain performance when topology changes, and mixed initiative control allows a single human to supervise many vehicles through intent level interfaces.

Three enabling vectors shape short term progress. The first is communication and compute. Edge offloading over 5G and future 6G reduces perception latency, while on board accelerators for convolutional, transformer, and graph workloads make inference feasible within strict size, weight, and power envelopes. Model compression through pruning, quantization, distillation, and low rank adaptation lowers energy per decision and extends endurance. The second is energy and airworthiness. Energy aware trajectory planning, aerodynamic learning for gust rejection, and predictive health monitoring increase mission length and reduce unscheduled landings. The third is trust, security, and compliance. Robustness to

sensor spoofing and weather induced distribution shift, interpretable perception and control, secure command and control links with formal verification of safety invariants, and standardized test catalogs for regression prevent silent performance erosion as models evolve.

Sector case studies demonstrate tangible gains. In agriculture, multi spectral mapping with learned segmentation improves nitrogen prescription and pest hotspot detection, while coordinated route planning cuts flight hours per hectare. In environmental monitoring, anomaly detection on streaming video speeds early wildfire spotting and oil spill delineation. In public safety and disaster response, victim detection models and learned search patterns shorten time to first contact. In logistics and medical delivery, learned landing zone selection and wind aware path planning improve reliability under urban turbulence. Military and border protection applications leverage target recognition, pattern of life modeling, and cooperative geolocation, while remaining within the bounds of safety and responsible use.

Open challenges remain. Training data curation at scale is costly and biased, and the long tail of rare events limits generalization. Hardware variability across airframes complicates transfer of learned controllers. Battery energy density constrains long range missions, and high-fidelity simulation for aeroelastic effects is still maturing. Legal geofencing, privacy, and airspace integration must be encoded into planning stacks, not treated as afterthoughts. A research agenda that combines high quality datasets with uncertainty aware learning, hybrid model based and model free control, and continual learning under supervision is most likely to deliver certifiable performance.

The weight of evidence indicates a shift from scripted autonomy to data centric autonomy, where perception, prediction, and policy are learned from multimodal data and are refined through rigorous validation, closed loop testing, and lifecycle MLOps. As datasets, computer platforms, and certification frameworks improve, ML enabled UAVs will operate with greater independence and coordination across civilian and military domains while meeting stricter safety and reliability requirements.

References

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

2. Muradov, S.A. et al. (2023, November). Determining the location of the UAV equipped with a homing device based on radio beacons. In *Modeling, Control and Information Technologies: Proceedings of International scientific and practical conference* (No. 6, pp. 54-56).

3. Bayramov A.A. eta l. Unmanned Aerial Vehicle Applications for Military GIS Task Solutions //Research Anthology on Reliability and Safety in Aviation Systems, Spacecraft, and Air Transport. – IGI Global Scientific Publishing, 2021. – С. 1092-1115.

4. Muradov, S.A. (2023). Development prospects of beacon systems. *In* Problems of informatization. Vol. 1. p.31.

5. Bayramov A.A. The numerical estimation method of a task success of UAV reconnaissance flight in mountainous battle condition //Сучасні інформаційні системи. – 2017. – №. 1,№ 2. – С. 70-73.

6.Hashimov E., Khaligov G. The issue of training of the neural network for drone detection //Advanced Information Systems. – 2024. – Т. 8. – №. 3. – С. 53-58.

7.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.

8.Ganimat I. B. Analysis and selection performance indicators multiservice communication networks based on the concept NGN and FN //Computer and information systems and technologies. – 2021.

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

10. Bayramov A.A. Assessment of invisible areas and military objects in mountainous terrain //Defence Science Journal. – 2018. – Т. 68. – №. 4. – С. 343-346.

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

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

13. Hasanov A.H..Analysis of the effectivness of communication and automated management systems. *İn* Modern directions of development of information and communication technologies and management tools. – 2022. – Т. 1. – С. 1-4.

14. Piriyev H.K. et al. Modelling of the battle operations //Monografiya, Herbi Nashriat", Baku.–2017. – 2016.

15. Bayramov A.A.. The supervisory control systems deployment in mountainous terrain //VIII Int. Conf."Modern development trends of ICT and control methods. – 2018. – С. 3-4.

16. Islamov, I. et al. (2025). Hybrid communication models for UAV swarms: Towards scalable and energy-aware network optimization. *Scientific guidelines: Theory and practice of research – Proceedings of the VI International Scientific Conference* (Kyiv, Ukraine, October 3, 2025), pp. 185–195. https://doi.org/10.62731/mcnd-03.10.2025

17. Ismayil, I. et al. (2025). Optimization of composite material selection in the design of military UAV wings. Scientific review of the actual events, achievements and problems: Collection of scientific papers «SCIENTIA» with Proceedings of the V International Scientific and Theoretical Conference (pp. 107–115) https://doi.org/10.36074/scientia-03.10.2025

18. Tahirov, R. K. et al. (2024). Environmental aspects of information technology implementation. In *Problems of Informatization: Proceedings of the 12th International Scientific and Technical Conference* (Vol. 3, pp. 138–139).

19. Islamov, I. et al. (2025). The use of unmanned systems and artificial intelligence to enhance radiation and chemical safety in military ecology. In *Innovations and the scientific potential of the world: Proceedings of the VII International Scientific Conference* (pp. 183–192). Sumy, Ukraine: Ukrlogos Group. https://doi.org/10.62731/mcnd-10.10.2025

20. Tabunenko, V. et al. (2025). The dynamics of UAV flight integrated with route planning. In *Modern tools and methods of scientific investigations: Proceedings of the VI International Scientific and Theoretical Conference* (pp. 46–56). Antwerp, Belgium: Scientia. https://doi.org/10.36074/scientia-10.10.2025

УЧАСНИКИ КОНФЕРЕНЦІЇ (секції 3, 7)

ОРГАНІЗАЦІЇ, ЯКІ ПРИЙНЯЛИ УЧАСТЬ У КОНФЕРЕНЦІЇ

Академія Державної прикордонної служби Республіки Азербайджан, Баку, Азербайджан

Азербайджанська академія спорту, Баку, Азербайджан

Азербайджанський технічний університет, Баку, Азербайджан

Азербайджанський університет будівництва та архітектури, Баку, Азербайджан

Бакинський державний університет, Баку, Азербайджан

Військовий науково-дослідний інститут, Баку, Азербайджан

Військовий інститут імені Гейдара Алієва, Баку, Азербайджан

Військовий інститут танкових військ НТУ "Харківський політехнічний інститут", Харків, Україна

Військово-морські сили Азербайджану, Баку, Азербайджан

Державний біотехнологічний університет, Харків, Україна

Державний університет "Київський авіаційний інститут", Київ, Україна

Інститут освіти Азербайджанської Республіки, Баку, Азербайджан

Інститут систем управління Азербайджанської Національної академії наук, Баку, Азербайджан

Ленкоранський державний університет, Ленкорань, Азербайджан

Нахічеванський державний університет, Нахічевань, 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 аерокосмічний університет "Харківський авіаційний інститут", Харків, Україна

Національний технічний університет "Харківський політехнічний інститут", Харків, Україна

Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна

Національний університет оборони Азербайджанської республіки, Баку, Азербайджан

Національний університет "Одеська політехніка", Одеса, Україна

Національний університет цивільного захисту України, Харків, Україна

Педагогічний університет імені Комісії Національної Освіти, Краків, Польща

Празький університет економіки та бізнесу, Прага, Чехія

Придніпровська державна академія будівництва та архітектури, Дніпро, Україна

Сумгаїтський державний університет, Сумгаїт, Азербайджан

ТОВ «AMS», Харків, Україна

Український науково-дослідний інститут екологічних проблем», Харків, Україна

Університет технології і гуманітарних наук, Бельсько-Бяла, Польща

Управління метрології та стандартизації, Київ, Україна

Фаховий коледж інформаційних технологій НУ "Львівська політехніка", Львів, Україна

Харківський національний університет внутрішніх справ, Харків, Україна

Харківський національний економічний університет ім. 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

Харківський радіотехнічний фаховий коледж, Харків, Україна

ЗМІСТ

НАУКОВЕ ВИДАННЯ

ПРОБЛЕМИ ІНФОРМАТИЗАЦІЇ

Тези доповідей
тринадцятої міжнародної науково-технічної конференції
(27 – 28 листопада 2025 року)
Том 2: секції 3, 7

Відповідальна за випуск *Н. Г. Кучук*
Технічний редактор *І. А. Лєбедева*
Коректор *В. В. Богомаз*
Комп'ютерне складання та верстання *Н. Г. Кучук, І. Ю. Петровська*

Адреса оргкомітету: вул. Кирпичова, 2, Харків, 61002, Україна
НТУ «ХПІ», Вечірній корпус, кімната 314
тел. +38 (057) 707 61 65

Підписано до друку 20.11.2025 Формат 60 × 84/16
Ум.-вид. арк. 10,0. Тираж 100 пр. Зам. 1120-25/2

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**