МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

Військовий інститут телекомунікацій та інформатизації імені Героїв Крут

ІІІ МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

The third International scientific and practical conference

“Кіберборотьба: розвідка, захист та протидія”

“Cyberwarfare: intelligence, defense and offensive security”

06–07.05.2025

ТЕЗИ ДОПОВІДЕЙ

Київ

Рецензенти:	*Радзівілов Григорій Данилович*	кандидат технічних наук, професор, заступник начальника інституту з наукової роботи
	Чевардін Владислав Євгенійович	доктор технічних наук, професор, старший науковий співробітник, начальник кафедри кібербезпеки
	Ковальчук Людмила Василівна	доктор технічних наук, професор, доцент кафедри кібербезпеки
	Хусаінов Павло Валентинович	кандидат технічних наук, професор, професор кафедри кібербезпеки
	Якуб Сита	доктор філософії, заступник директора Центру морської кібербезпеки Польської військово-морської академії

Кіберборотьба: розвідка, захист та протидія: тези доповідей ІІІ Міжнародної науково-практичної конференції. – Київ: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, 2025. – 47 с. DOI: https://doi.org/10.61929/viti.mnpk.3.2025.

У збірнику матеріалів ІІІ Міжнародної науково-практичної конференції **“Кіберборотьба: розвідка, захист та протидія”** опубліковано тези доповідей вчених, науково-педагогічних та наукових працівників, докторантів, ад’юнктів, здобувачів.

Метою конференції є аналіз шляхів співпраці наукових колективів європейських країн у сучасних проєктах збереження миру та безпеки та використання сучасних навчальних кіберполігонів і платформ для проведення навчання фахівців із кібербезпеки.

Робочі мови конференції – українська, англійська.

Відповідальність за точність, достовірність і зміст поданих матеріалів несуть автори.

Відповідальна за випуск І. В. Цимбал

Підписано до друку 03.06.2025 р. Зам. № 140
Друк. арк. 5,75. Ум.-друк. арк. 5,34. Обл.-вид. арк. 4,97
Формат паперу 60×84/8. Тираж 3 прим.

Адреса друкарні ВІТІ ім. Героїв Крут: 01011, м. Київ, вул. Князів Острозьких, 45/1

З М І С Т

УДК 004.056

DCs, Professor **Chevardin V. Y.** ORCID: 0000-0002-1070-4568 (Kryty Heroes MITIT)

CYBERWARFARE: MODERN NEEDS AND CHALLENGES

Modern technologies are increasingly shifting towards digital solutions, with a growing trend toward automating most processes, using software for action management, and applying artificial intelligence to handle both standard and non-standard procedures.

The experience of war has presented new challenges for the cybersecurity system of the Armed Forces of Ukraine, specifically:

the number of hardware and software, information, and communication tools and systems has increased significantly. In 2022, the number of desktop clients grew from 4,000 to 7,800. In 2023, this number increased from 7,800 to over 16,000. The growth in Android users is shown on the diagram, and the trend is similar. On one hand, this is a compromise between price and quality; on the other, it introduces new vulnerabilities;

the number of informational and automated systems has increased, as noted by previous speakers. Consequently, we are observing persistent activity by Russian hacker organizations; nine of these were identified, while five remain uncertain.

These factors have driven an expansion of cybersecurity services and the creation of new Cybersecurity and Information Security (CIS) units.

The formation of new CIS units required their integration into a unified CIS system for the Armed Forces which was established in the country, combining the entire security sector and critical infrastructure.

The adversary is currently using this war as a testing ground for new technological solutions and weaponry, specifically: employing new signal structures in the electromagnetic spectrum, implementing new dual-use software and hardware solutions for cyber intelligence and cyber influence, and using artificial intelligence elements to detect weaponry and military equipment.

Consequently, these challenges require continuous improvement in the training system for CIS specialists within the Armed Forces.

Given these challenges and needs, the training system has been adapted over the past three years. Close cooperation and experience-sharing with combat units and our clients have been established to meet the modern needs of the forces during operational missions. The knowledge gained, combined with the experience of combat officers, instructors, and master's students who participate in international competitions, has been integrated into the training program for bachelor’s and master’s level specialists. Following this, new scenarios are developed in the coming months to conduct competitions and training sessions at the institute’s cyber range for officers and cadets. This process is cyclical.

Taking into account the needs of the forces, an effective training system has been created for CIS specialists in the Armed Forces, including bachelor’s and master’s level training as well as advanced training courses to gain specific expertise required in SOC of the Armed Forces and other military formations. A system of mobile cybersecurity control teams has been established at the institute, along with the SSOC combat cyber control post.

The education and training of the cybersecurity forces are carried out using modern material and technical means. It enables us to consider the heterogeneity of the computer networks in the Armed Forces, implement various hardware platforms and software for training, and conduct all activities in both offline and online modes while ensuring the physical security of personnel.

УДК 004.056

Hasilin D. L. ORCID: 0009-0000-4636-7666 (NU «LP»)
Dr. Sc., s.r., Prof. **Zhuravel I. M.** ORCID: 0000-0003-1114-0124 (NU «LP»)

DECISION SUPPORT BASED ON INVARIANCE OF STEGANOGRAPHIC METHODS TO ATTACKS

Introduction. Recent statistics in publications show growing popularity in steganography evolution [1]. This increase in research in Steganography could be explained by the growing need for secure communication. The same applies to the platforms with opposite goals — detection methods are a popular topic in steganography, especially after the rise of Deep Learning models' popularity [1]. Hiding a fact of data transmission or existence is a substantial improvement to the commonly used cryptography. Evaluation of robustness for such methods is not publicly developed enough in reviewed papers. This work aims to analyze the comprehensiveness of the current state of research that should form a coherent and unified understanding of the missing building elements involved in the integration of stegosystems, both embedding and detecting.

Literature review. A common approach for inventors of novel methods is ensuring effectiveness based on a few features of a new method. Usually, that is signal ratio measurements such as SNR, PSNR, and SSIM [2], as well as embedding capacity. In rare cases, we see a comparison to efficient methods. Looking at the high-level context, we could see that many important aspects are not taken care of. The resilience of the discussed methods to common attacks is a characteristic that is often overlooked. It would be incorrect to imply that resilience is always ignored, but even when it is investigated, typically only to some specific attack [3] or detection method [1]. The assessment is rarely made comprehensively, yet even then, only small parts of such studies are open-sourced and could be taken as a baseline for further advancement [4]. Significant advantages have detection methods, their development is better addressed and evaluated based on relatively small but well-defined test datasets [5].

Invariance to attacks. The main unknowns in providing data for stenographic decisions, apart from the mentioned above integration of various existing components, are the poorly highlighted level of invariance to attacks. Such a feature could be a central piece in a selection of embedding methods based on the communication channel and potential attacks that could be faced. To formalize research goals, it is required to explore the problem of evaluating invariance to attacks, given the specific features of the communication channel and cover images. Also, it is essential to define a set of attacks. This study proposes a baseline of common attacks:

- Lossy compression.
- Affine transformations (mirroring, scaling down/up by an insignificant percentage).
- Editing (such as removing a single line of pixels, cropping).

The list isn’t complete or comprehensive and should be extended and clarified during further research. Since not all embedding methods work with block-based representations of information, it is necessary to design a method for assessing the extent of invariance to attacks. As per the research literature, the Bit-Error Rate (BER) [4] is most commonly used for such purposes. However, after conducting several simulations, it is proposed that a Byte-Error Rate be designed and tested so that it is not affected by false-positive statistical hits while working with streaming data.

Furthermore, it is an inevitable next step in the evolution to incorporate different techniques of assessment of invariance to attacks, capacity, applicability in concrete use-cases, together with additional flow-maintenance features, into one framework. That should also include detection robustness and quality assurance that could help engineers and researchers evaluate embedding methods, attacks, and models used. The main goal of such frameworks is to help facilitate informed decisions; hence, the name Decision Support Systems [6].

Integration problem. Decision support in steganography is a relatively new field, as many regular tools are typically hard to integrate due to numerous dependencies. Therefore, different techniques are used to combine and integrate common, well-known tools into an end-to-end system that provides insights for decision support in real time or near real time.

To leverage the diversity of tools and techniques in one solution, containerization is used. To make such integration seamless and adjustable in real time, the novel technique of agent-based

composition could be adopted. Agents could handle dynamic binding for AI modules, combined with a strict “tools” API to ensure interoperability with older solutions and applications [7].

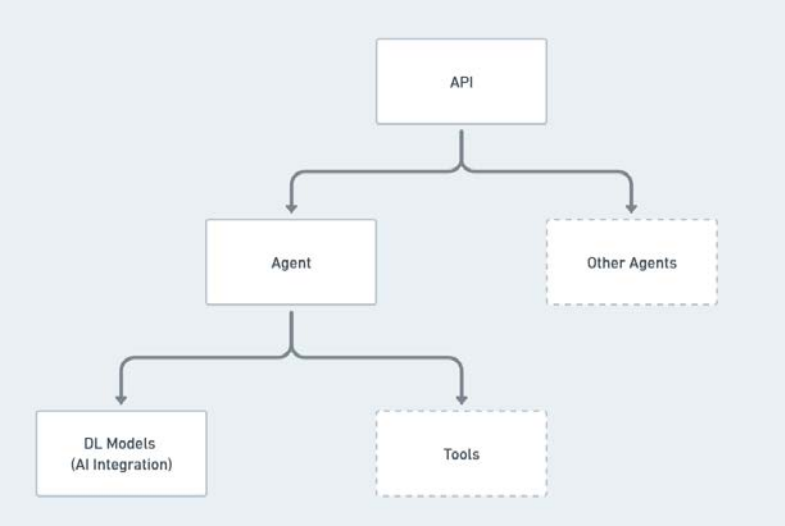

Figure 1. Agent-based system decomposition

Behind the agent-based approach is a simple idea of passing integration management over to AI. APIs of such systems might be defined only to some point required for successful interoperability between agents. An exception is tools, which are performing as an outbound gateway to existing modules with a well-defined API. Each agent in such an approach is independently configurable and sometimes could have control over its execution and scheduling in addition to managing AI/DL models, tools, and often other agents (see Fig. 1). This framework for resolving coordination tasks is generic, and it could fit well as an orchestrated solution. Extensive testing is needed to evaluate this approach properly, but it is considered promising in terms of added value compared to risks and efforts required.

Solving those two concerns is a promising research direction that could illuminate blind spots in a high-level picture of steganographic systems. It is planned to continue working in this area.

REFERENCES

1. Apau R., Asante M., Twum F., Ben Hayfron-Acquah J., Peasah K. O. Image steganography techniques for resisting statistical steganalysis attacks: A systematic literature review. PloS one. 2024. No. 19 (9), e0308807. URL: https://doi.org/10.1371/journal.pone.0308807.

2. Walia, Ekta & Jain, Payal & Navdeep. An analysis of LSB & DCT based steganography // Global Journal of Computer Science and Technology. 2010. No. 10.

3. Zhang Y., Luo X., Wang J., Yang C., Liu F. A robust image steganography method resistant to scaling and detection // Journal of Internet Technology. 2018. No. 19 (2). P. 607–618. URL: https://doi.org/10.3966/160792642018031902029.

4. Kunhoth, Jayakanth & Subramanian, Nandhini & Al-ma'adeed, Somaya & Bouridane, Ahmed. Video steganography: recent advances and challenges // Multimedia Tools and Applications. 2023. No. 82. H. 1–43. URL: https://doi.org/10.1007/s11042-023-14844-w.

5. Alrusaini O. A. Deep learning for steganalysis: Evaluating model robustness against image transformations // Frontiers in Artificial Intelligence. 2025. No. 8, 1532895. URL: https://doi.org/10.3389/frai.2025.1532895.

6. Sigari, Salman & Gandomi, Amir. Analyzing the past, improving the future: a multiscale opinion tracking model for optimizing business performance // Humanities and Social Sciences Communications. 2022. No. 9. URL: https://doi.org/10.1057/s41599-022-01325-y.

7. Google. Agent Development Kit (ADK): An open-source framework for developing and deploying AI agents. 2025. URL: https://google.github.io/adk-docs/.

УДК 004.056.4

Cand. Tech. Sc. Samoilov I. ORCID: 0000-0002-8251-9257 (ISCIP)
Cand. Tech.Sc. Storchak A. ORCID: 0000-0002-5267-3122 (ISCIP)
Cand. Tech. Sc. Konotopets M. ORCID: 0000-0002-6963-1877 (ISCIP)
Ph.D. Lavryk I. ORCID: 0000-0002-3433-9083 (MITIT)

APPLICATION OF ML TECHNIQUES FOR CYBER INCIDENT ANALYSIS

The analysis conducted by [1] showed that the main types of threats remain ransomware, malware, social engineering, data breaches, and availability threats. According to [2], 58.8 % of all incidents in 2024 were related to malware, including ransomware. The significant threat posed by ransomware underscores the need for new technologies to detect and neutralize it. The use of machine learning methods can reduce threat detection times and significantly improve security system efficiency [3].

The main approaches to analyzing cyber incidents and malware are signature, heuristic, static, dynamic, and neural network analysis. Machine learning addresses the challenge of polymorphic and metamorphic viruses by analyzing program behavior patterns and detecting anomalies.

The stages of applying machine learning algorithms to cyber-incident analysis are as follows:

1. Collection of input parameters.
2. Feature extraction and preprocessing.
3. Application of ML algorithms.
4. Identification of “zero-day” threats.
5. Accuracy evaluation using Precision, Recall, and F1 metrics.
6. Integration with SIEM systems (Splunk, IBM QRadar, ArcSight).

In the first stage, a comprehensive dataset is collected to detect polymorphic and metamorphic malware. The second stage extracts relevant features (API call frequency, PE-file structure, etc.) and balances classes to reduce false positives and false negatives.

The following algorithms are used for training and threat detection:

– Random Forest (500 trees, max_depth=30) – resistant to noise and well-suited for a large number of heterogeneous features;

– Isolation Forest – for detecting anomalous patterns and uncovering unseen threats;

– Cluster Analysis – grouping similar samples to identify families of polymorphic malware.

After training, the model is evaluated on a test set to minimize false positives and false negatives. For automatic reporting of suspicious patterns and triggering correlation analysis, the method is integrated with SIEM systems.

The quality of cyber incident analysis using machine learning technologies depends on the training data. Polymorphic and metamorphic malware constantly evolves, so without regular updates and sample expansion, the method's effectiveness will degrade over time. This method should be deployed in critical infrastructure environments with large datasets and high computational resources, as its effectiveness depends on the quality of the training samples and their regular updates. The combined approach (Random Forest, Isolation Forest, clustering) can be resource-intensive, so it is most appropriate for large-scale systems.

REFERENCES

1. European Union Agency for Cybersecurity (2024). Enisa threat landscape 2024. EUROPEAN UNION AGENCY FOR CYBERSECURITY.

2. Оперативний центр реагування на кіберінциденти Державного центру кіберзахисту Державної служби спеціального зв’язку та захисту інформації України. (2024). Звіт системи виявлення та реагування на кіберінциденти та кібератаки за 2024 рік.

3. Zvit IBM pro vartist vytoku danykh za 2023 rik – CoreWin. (n.d.). CoreWin. https://corewin.ua/news/ibm–report–2023.

УДК 004.946.5

д-р філософії **Ахтирцева В. С.** ORCID: 0000-0002-0624-2284 (ЖВІ ім. С. П. Корольова)
Лобода В. В. ORCID: 0000-0002-3535-0233 (ЖВІ ім. С. П. Корольова)
Павленко М. М. ORCID: 0000-0002-1011-5042 (ЖВІ ім. С. П. Корольова)

ПЕРСПЕКТИВНЕ КІБЕРОЗБРОЄННЯ ЯК ВАРІАНТ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

За даними оперативного центру реагування на кіберінциденти Державного центру кіберзахисту (ДЦКЗ) Держспецзв’язку України спостерігається неухильне збільшення кількості кібератак з боку рф. Основними цілями зловмисників були сайти державних органів, відомств, ЗСУ, фінансових установ та інших критично важливих об’єктів інфраструктури України.

Кіберзброя зазвичай використовується приховано, й часто застосовується лише одноразово, наприклад, через використання шкідливого програмного забезпечення, а також використання вразливостей нульового дня (“Zero-day”). Це, в свою чергу, призводить до унеможливлення або ускладнення виявлення таких кібератак. Тому дослідження характеристик кіберзброї противника здебільшого відбувається за наслідками, які спричинені результатом її застосування.

Враховуючи наслідки, які були спричинені кібератаками на Україну, актуальним постає завдання з організації відповідних контрзаходів у кіберпросторі та розроблення кіберозброєння, яке може бути використано не тільки для захисту власних інформаційних ресурсів, а й для впливу на об’єкти противника.

Загальноприйнятим алгоритмом планування та здійснення кібератаки прийнято вважати модель життєвого циклу кібератаки Cyber-Kill Chain, яка розроблена компанією Lockheed Martin. Це класична модель кібербезпеки, розроблена командою реагування на кіберінциденти, які порушують кібербезпеку CSIRT.

Модель Cyber Kill Chain складається із 7 етапів, які виконує сторона, що атакує, для успішної реалізації власної кібератаки:

– розвідка (Reconnaissance);
– озброєння (Weaponization);
– доставка (Delivery);
– експлуатація (зараження) (Exploitation);
– встановлення (Installation);
– управління та контроль (Command and Control);
– виконання дій (Actions on Objective).

Основу кіберозброєння мають складати апаратні (технічні) засоби та програмне забезпечення (загальне, спеціалізоване та шкідливе), що призначені для дій у кіберпросторі в інтересах застосування ЗС України [1]. Це дасть змогу визначити об’єкти (цілі) кіберзброї, серед яких критична інфраструктура противника, системи управління бойовими діями, мережі зв’язку, інформаційні та медіаресурси, окремі особи та групи населення противника.

Враховуючи вищезазначене, пропонується визначити цільове призначення перспективного кіберозброєння ЗС України, яке полягатиме у здійсненні кіберрозвідки для збору інформації та виявлення вразливостей у системах управління противника. Крім того, вона буде використовуватися для впливу на ці системи шляхом зміни їхнього функціонування, проведення кібератак та захисту власних інформаційних ресурсів від кібервпливу противника.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Міхєєв Ю. І., Павленко М. М., Лобода В. В., Латко І. І. Оперативно-тактичні вимоги до перспективного кіберозброєння видів Збройних Сил України // Збірник матеріалів ІІІ Міжнародної науково-технічної конференції. Київ: ВІТІ ім. Героїв Крут, 2023. 379 с.

УДК 004.056

Балан А. В. ORCID: 0009-0008-7567-0339 (ВІТІ ім. Героїв Крут)
канд. техн. наук, доцент **Клімович С. О.** ORCID: 0000-0001-7209-2176 (ВІТІ ім. Героїв Крут)
Загоровець О. В. ORCID: 0009-0008-2566-9217 (ВІТІ ім. Героїв Крут)

АНАЛІЗ ЗМІСТУ ЗАКОНУ УКРАЇНИ «ПРО ВНЕСЕННЯ ЗМІН ДО ДЕЯКИХ ЗАКОНІВ УКРАЇНИ ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ ТА КІБЕРЗАХИСТУ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ, ОБ’ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ»

У 2025 році Державна служба спеціального зв’язку та захисту інформації України прагне перейти на повноцінне запровадження системи декларативного принципу під час побудови захисту інформаційних систем на основі базових профілів безпеки, які базуються на провідних світових стандартах, зокрема Risk Management Framework американського Національного інституту стандартів і технології NIST. Ухвалення Закону України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об’єктів критичної інформаційної інфраструктури» є важливим кроком, який дасть можливість протистояти новим викликам та загрозам у кіберпросторі, а також забезпечить посилення захисту державних інформаційних ресурсів та об’єктів критичної інформаційної інфраструктури, адже російська агресія у кіберпросторі продовжує зростати і вона не закінчиться після закінчення повномасштабної війни, у зв’язку з цим дослідження є **актуальним.**

Метою роботи є аналіз принципових новацій у нормативно-правовому забезпеченні інформаційної безпеки України.

Ухвалений Закон передбачає низку важливих змін та нововведень, а саме:

1. Система реагування на кіберінциденти (визначено ролі, завдання та сервісні функції команд реагування, встановлено принципи взаємодії суб’єктів багаторівневої мережі реагування).
2. Реагування у кризових ситуаціях (закон передбачає механізми оперативного залучення відповідних сил і засобів у випадках кіберкриз).
3. Обмін інформацією про кіберінциденти (упорядковано обов’язки суб’єктів щодо повідомлення про кіберінциденти, визначено принципи взаємодії, захисту та розкриття інформації).
4. Відмова від обов’язкової комплексної системи захисту інформації (КСЗІ) (запроваджено підхід управління ризиками на основі профілів безпеки, забезпечується підтримка заходів протягом усього життєвого циклу ІТ-систем на основі профілів безпеки, які взяті за основу згідно з НД ТЗІ (таблиця 1)).
5. Система оцінювання стану кіберзахисту (передбачено впровадження незалежного аудиту без надмірного контролю з боку держави).
6. Штатні посади фахівців з інформаційної безпеки (введення відповідних посад із захисту інформації та кібербезпеки у державних органах і на об’єктах критичної інфраструктури).

Закон гармонізує національне законодавство з положеннями директив ЄС щодо: діяльності команд реагування на інциденти (CSIRT) та процедур повідомлення про кіберінциденти. Закон містить положення, які забезпечують імплементацію норм європейських директив із кібербезпеки до національного законодавства щодо функцій команд реагування, практики повідомлень про кіберінциденти та управління ризиками.

Посилення кібербезпеки України та синхронізація стандартів із найкращими західними практиками – необхідна складова обороноздатності та цифрової стійкості України. Реалізація Закону дасть можливість Україні ще ефективніше інтегруватися у глобальну систему кіберзахисту. Впровадження Закону сприятиме підвищенню стійкості систем до сучасних викликів із глобальної системи кіберзахисту та зміцнить кібероборону держави.

Таблиця 1

Таблиця переліку НД ТЗІ щодо створення КСЗІ з використанням базових та цільових профілів безпеки інформації

№ з/п	Назва
1.	НД ТЗІ 3.6-006-24 Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем
2.	НД ТЗІ 3.6-004-21 Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці
3.	НД ТЗІ 3.6-005-21 Порядок категоріювання безпеки інформаційної системи та інформації
4.	НД ТЗІ 3.6-007-21 Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем
5.	НД ТЗІ 2.3-025-24 Т1 Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем
6.	НД ТЗІ 2.3-025-24 Т2 Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем
7.	НД ТЗІ 2.3-025-24 Т3 Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем
8.	НД ТЗІ 2.6-004-21 Порядок авторизації безпеки інформаційних систем
9.	НД ТЗІ 3.6-008-21 Порядок моніторингу безпеки інформаційних систем

Висновок. Закон закладає основу для впровадження нових механізмів захисту критичної інфраструктури і державних інформаційних ресурсів, упорядковує державну координацію у сфері кібербезпеки та наближає наше законодавство до європейських практик. Закон передбачає розширення державно-приватної взаємодії, співпраці з міжнародними партнерами, що дозволить Україні ще ефективніше інтегруватися у глобальну систему кіберзахисту.

Впровадження декларативного принципу є одним із пріоритетних завдань Держспецзв’язку на 2025 рік. Державна служба спеціального зв’язку та захисту інформації України вже створила нормативне та організаційне підґрунтя згідно з НД ТЗІ (таблиця 1).

Відхід від комплексної системи захисту інформації і перехід на декларування відповідності систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації, полегшить введення в дію інформаційних (автоматизованих) систем захисту інформації в Збройних Силах України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. URL: https://www.rada.gov.ua.
2. URL: https://cip.gov.ua/ua.

УДК 004.622: 517.927

д-р техн. наук, професор **Бараннік В. В.** ORCID: 0000-0002-2848-4524 (ХНУ ім. В. Н. Каразіна)
канд. техн. наук **Гуржій П. М.** ORCID: 0000-0002-2552-229X (ВІТІ ім. Героїв Крут)
канд. техн. наук **Бабенко М. В.** ORCID: 0000-0003-2385-2786 (ХНУРЕ)
Єлісєєв Є. С. ORCID: 0000-0002-0953-4397 (ХНУРЕ)
Онищенко Р. С. ORCID: 0000-0002-2332-5196 (ХНУРЕ)

СПОСІБ КОДУВАННЯ ВІДЕОДАНИХ У СПЕКТРАЛЬНО-ПАРАМЕТРИЧНОМУ ПРОСТОРІ

Вступ

У процесі вдосконалення методів стиснення відеоданих потрібно зважати на те, що існують: області когерентності з окресленим особливостями візуальної оцінки; області зображень, які є більш привабливими для стеганографічного вкладання інформації; області зображень із просторовою статистичною надмірністю. Тому потрібно організовувати процеси стиснення в структурно-параметричному просторі. Такі перетворення супроводжуються формуванням векторів довжин $\ell(t;\delta)_\alpha$ та значимих $sign(t;\delta)_\alpha$ компонент локальних когерентностей (ЛКГ) [1–5]. Але обробка таких компонент ЛКГ для вказаних областей організується без обліку їх особливостей в напрямку наявності локальних статистичних властивостей. Поставлене завдання пропонується вирішувати в напрямку вдосконалення методів кодування відеофрагментів та фрагментів-контейнерів з обліком локальних психовізуально-статистичних особливостей зображень у спектральному просторі. Після чого важливим є впровадження таких рішень для комплексів БПАКМ. Для цього необхідно розвивати технології кодування масивів спектральних компонент, в тому числі щодо обробки областей психовізуально-статистичної привабливості. При цьому також необхідно задіяти фактори щодо захисту конфіденційної інформації шляхом її вбудовування до відеопослідовностей. Звідси мета досліджень статті полягає в розробці методу кодування фрагментів-контейнерів для передачі в бездротових телекомунікаційних мережах.

Розробка загальної структури методу обробки відеоданих

Більша ефективність при обробці зображень досягається у разі, коли вихідне зображення попередньо перетворити до спектрального простору. Формуються масиви спектральних компонент (МСК). Внаслідок чого утворюється форма, яка має корисні властивості. Вони використовуються для подальшого скорочення кількості психовізульно-статистичної надмірності. Метод стиснення зображень на основі їх спектрального перетворення реалізовано у такому форматі, як JPEG, де одним з основних етапів роботи є дискретне косинусне перетворення (ДКП). Таке перетворення застосовують до окремих фрагментів розміру 8×8 елементів зображення. Корисним наслідком є переконцентрація енергії в область низьких частот МСК. Формується таке уявлення, для якого: у правому верхньому куті зосереджується низькочастотна компонента – DC-компонента або $y(t)_{1,1}$. Така компонента містить концентровану інформацію щодо фрагмента зображення.

Інші компоненти називаються АС-компонентами. Вони зосереджені в нижньому лівому куті МСК. Відповідно для них притаманний обмежений відсоток інформації про фрагмент зображення. Особливо стосовно областей когерентності. Масив спектральних компонент після ортогонального або хвилевого перетворення має такі властивості:

1) значення компоненти $y(t)_{1,1}$ МСК з координатами (1;1) пропорційно до середньої яскравості локального фрагмента зображення;

2) тенденція зміни значень компонент МСК направлена в бік зниження по діагональному зигзагу: зліва направо та зверху донизу;

3) з’являється можливість для врахування психовізуально-статистичних особливостей для послідовності масивів спектральних компонент.

У сформованому одновимірному векторі $Y_t^{(1)}$ елементів МСК відбуваються етапи побудови спектрально-параметричного опису (СППО): спочатку отримуємо DC-компоненту $y(t)_{1,1}$; після чого для інших елементів МСК пропонується утворювати дві складові $S(t)^{(1)}$, $L(t)^{(1)}$. Такими складовими є наступні послідовності: перша $S(t)^{(1)}$ – вектор градацій спектрального простору. Він формується на основі виявлення значимих градацій нерівномірного спектрального простору МСК; друга $L(t)^{(1)}$ – шкала спектральних інтервалів. Він створюється на основі довжин спектральних інтервалів між двома градаціями. За результатами чого маємо: $Y_t^{(1)} = \{DC; S(t)^{(1)}; L(t)^{(1)}\}$. Це дозволяє скоротити кількість повторюваних елементів МСК. Тому вектор $L(t)^{(1)}$ пропонується в подальшому позначати як шкалу спектральних інтервалів. Компоненти $\ell(t)_\alpha$ вектора $L(t)^{(1)}$ визначають кількість повторів значень значущих $sign(t)_\alpha$ градацій МСК [28; 29]. Отже вектор $Y_t^{(1)}$ описується двоелементною сукупністю параметрів $lc(t)_\alpha = \{\ell(t)_\alpha; sign(t)_\alpha\}$. Тут маємо: $sign(t)_\alpha$ – значення *i*-ї значущої градації у складі розгорнутої до одновимірної послідовності МСК; $\ell(t)_\alpha$ – кількість елементів МСК з однаковими градаціями.

Висновки

Розроблено спосіб кодування шкали спектральних інтервалів, яка базується на його розбитті двома складовими: довжина першої послідовності незначимих елементів складової СППО; підвектор, який складається з елементів другої компоненти за виключенням першої та останньої послідовності незначимих елементів СППО. Це дозволяє виявляти додаткові структурні закономірності, усунути статистичну надмірність.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бараннік В. В., Бабенко Ю. М., Бараннік В. В., Колесник В. О. Метод кодування значимих за впливом на семантичну цілісність відеосегментів для забезпечення доступності. *Наукоємні технології*. 2022. № 2 (54). С. 118–126. DOI: https://doi.org/10.18372/2310-5461.54.16749.

2. Баранник В. В., Игнатьев А. А., Бабенко Ю. М., Баранник В. В., Сидченко Е. С. Технология компоновочного кодирования микросегментов для повышения безопасности видеоресурсов в инфокоммуникационных системах. *Безпека інформації*. 2020. № 3. С. 181–190.

3. Barannik V., Tarasenko D. Method coding efficiency segments for information technology processing video. *Problems of Infocommunications. Science and Technology (PIC S&T)*: proceedings of 4th International Scientific-Practical Conference. (Kharkov, Ukraine, October 10–13, 2017), Kharkov, 2017. P. 551–555. DOI: 10.1109/INFOCOMMST.2017.8246460.

4. Barannik V., Babenko Y., Barannik V., Kolesnyk V., Zhuikov D. 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. P. 66–71. DOI: 10.1109/ATIT58178.2022.10024193.

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

УДК 004.622: 517.927

д-р техн. наук, професор **Бараннік В. В.** ORCID: 0000-0002-2848-4524 (ХНУ ім. В. Н. Каразіна)
Берчанов А. А. ORCID: 0009-0004-4301-6384 (ХНУ ім. В. Н. Каразіна)
Бараннік В. В. ORCID: 0000-0003-3516-5553 (ХНУРЕ)
Перцев П. Д. ORCID: 0009-0002-1692-0090 (ХНУРЕ)
Курлан О. О. ORCID: 0009-0002-0295-1398 (ХНУРЕ)

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ДОВЕДЕННЯ ІНФРАЧЕРВОНИХ ЗНІМКІВ МЕТОДОМ СПЕКТРАЛЬНО-ХВИЛЬОВОГО КОДУВАННЯ

Вступ

Сучасні інфокомунікаційні технології інтенсивно інтелектуалізуються завдяки розвитку теоретичної бази та обчислювальних засобів. Це стосується й сервісів видової інформації, зокрема інфрачервоних зображень (ІЧЗ), які є цінним джерелом інформації в умовах низької видимості, маскування або високої об’єктної насиченості. Інтелектуальний аналіз ІЧЗ дозволяє ідентифікувати об’єкти, класи, стани, здійснювати кластеризацію та семантичний пошук.

Такі підходи знаходять застосування в дистанційному моніторингу, автономному наведенні, створенні баз даних, супроводженні об’єктів тощо. Користувачами можуть бути як оператори, так і автоматизовані системи. Особливої актуальності набуває застосування ІЧЗ у бортових комплексах, що працюють у гібридному режимі управління – поєднуючи ручний, автоматизований та автономний підходи.

Зростання вимог до повноти, точності та частоти оновлення ІЧЗ обумовлює високі навантаження на інфокомунікаційні системи. Виникає суперечність між оперативністю передачі та цілісністю зображення, що унеможливлює застосування деяких стандартних методів компресії. Нині для вирішення такої задачі розробляються та застосовуються технології обробки зображень з елементами інтелектуального аналізу. До них слід віднести такі: JPEG2000, PNG. Основними напрямками технологічних розробок тут є наступні:

1) локалізації однорідних областей кадру;

2) застосування моделі описання імпульсної інформації, яка в загальному випадку може використовуватись для відокремлення шумової складової та інформації дрібних об’єктів;

3) визначення класу об’єктів та групового їх описання на ІЧЗ;

4) використання пакету типових об’єктів і технологій їх виявлення на кадрах;

5) технологій інтерполяційного опису фонових областей ІЧЗ.

Водночас такі технологічні механізми є:

1) складними з позиції обчислювальної реалізації;

2) низько ефективними у разі обробки ІЧЗ: з нетиповим змістом, наприклад у разі попереднього моніторингу операційних районів із високим рівнем насиченості апріорно невизначених об’єктів; зі складною топологією взаємного розташування великої кількості неоднорідних об’єктів;

3) такими, що супроводжуються внесенням спотворень, які призводять до виключення можливості зворотного відновлення семантичних складових кадрів.

Отже, актуальною є задача розробки методів інтелектуального групового кодування фрагментів ІЧЗ із забезпеченням високого ступеня стиснення без втрати семантичної цілісності. **Мета дослідження** – створення методу спектрально-хвильового групового кодування для ефективної обробки ІЧЗ.

Розробка методу групового кодування інфрачервоних зображень у спектрально-хвильовому просторі

Перетворимо елементи мінісегмента $A_{r,t}^{(k,l)}$ у різницевий простір $A_{r,t}^{\prime(k,l)}$, використовуючи таку формулу:

$$A'^{(k,l)}_{r,t}(q,s) = A^{(k,l)}_{r,t}(q,s) - \mu^{(k,l)}_{r,t} \quad (1)$$

Представимо застосування вейвлетних перетворень як функціонал WH:

$$WH(A'^{(k,l)}_{r,t}) = \{L^{(k,l)}_{r,t}(I), H^{(k,l)}_{r,t}\}, \quad (2)$$

де:

- $A'^{(k,l)}_{r,t}$ – різницевий мінісегмент, до якого застосовується WH;
- $H^{(k,l)}_{r,t}$ – група високочастотних значень;
- $L^{(k,l)}_{r,t}(I)$ – кінцеве низькочастотне значення.

Застосуємо метод групового кодування до утворених частотних груп. У результаті сегмент $A^{(1,1)}$може бути представлений п’ятьма кодовими значеннями: $CL^{(1,1)}$, $CH^{(1,1)}_{1,1}$, $CH^{(1,1)}_{1,2}$, $CH^{(1,1)}_{2,1}$, $CH^{(1,1)}_{2,2}$, де кожне кодове значення відповідає частотній групі, на основі якої було отримано.

Висновки

Створено метод групового кодування інфрачервоних зображень у спектрально-хвильовому просторі. Метод заснований на: ієрархічній декомпозиції ІЧЗ на сегменти та мінісегменти для локалізації однорідних областей; перетворенні інформації у різницевий простір для зменшення динамічного діапазону значень із врахуванням кореляційних залежностей; перетворенні просторового домену інформації у спектрально-хвильовий домен із використанням вейвлет перетворення на базисі Хаара; групуванні високих та низьких частот для врахування їх структурних закономірностей; застосуванні спектрально-групового кодування до утворених сукупностей для їх ефективного бітового представлення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Barannik D., Barannik V. Steganographic Coding Technology for Hiding Information in Infocommunication Systems of Critical Infrastructure // ATIT. 2022. P. 88–91. URL: https://doi.org/10.1109/ATIT58178.2022.10024185.

2. Barannik V. et al. A method to control bit rate while compressing predicted frames // CADSM. 2015. P. 36–38. URL: https://doi.org/10.1109/CADSM.2015.7230789.

УДК 621.327:681.5

д-р техн. наук, професор **Бараннік В. В.** ORCID: 0000-0002-2848-4524 (ХНУ ім. В. Н. Каразіна)
канд. техн. наук, доцент **Красноруцький А. О.** ORCID: 0000-0001-9098-360X (ХНУПС)
канд. техн. наук **Гуржій П. М.** ORCID: 0000-0002-2552-229X (ВІТІ ім. Героїв Крут)
Прокопенко Р. О. ORCID: 0009-0006-0789-9073 (ХНУРЕ)
Семенченко О. А. ORCID: 0000-0009-3881-6628 (ХНУРЕ)

ТЕХНОЛОГІЯ КОДУВАННЯ ВІДЕОКОНТЕНТУ ІЗ ЗАБЕЗПЕЧЕННЯМ ЇХ ДОСТОВІРНОСТІ В БЕЗДРОТОВИХ ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ ДИСТАНЦІЙНОГО ВІДЕОСЕРВІСУ

Інформаційне забезпечення систем управління критичною інфраструктурою в сучасному кіберпросторі характеризується наступними аспектами: поширене використання відеоконтенту для аналізу та прийняття рішень щодо стану та динаміки об’єктів моніторингу; зростання застосування дистанційних мобільних сенсорів, в тому числі безпілотних авіаційних комплексів, для збору та реєстрації відеоінформації; застосування бездротових інфокомунікаційних мереж, в тому числі на базі бортових платформ, для обміну інформацією.

Заразом зростають вимоги щодо: повноти ресурсів відеоконтенту (кількість пікселів у відеокадрі зросла в середньому в 16 разів); оперативності та достовірності інформаційного відеоконтенту. Тут оперативність розуміється як сумарні часові затримки на обробку та передавання інформації з дистанційних мобільних сенсорів на пункт приймання. Достовірність встановлюється як відповідність відеоконтенту, що отримується на приймальній стороні, до його початкового представлення як відповідного об’єкта моніторингу. Отже постає питання щодо забезпечення потрібних якісних показників надання дистанційного відеосервісу. Тут необхідно зважати на особливості аналізу відеоінформації та її критичність щодо впливу на процес прийняття рішень, а саме рівень наслідків у разі його порушення. Враховуючи це, існують вимоги щодо достовірності отриманого відеоконтенту (для найвищої критичності інформації необхідно забезпечити режим обробки та передачі без втрат інформації, тобто кількість спотворених пікселів або PSNR повинні дорівнювати нулю). Щодо часових затримок, то такий показник залежно від критичності та часу актуальності (старіння) інформації має бути на рівні декількох мілісекунд. Означені тенденції вимагають використання інфокомунікаційних мереж із необхідним рівнем швидкості передачі інформації. Водночас, використання бездротових мереж на авіаційних платформах пов’язане з дисбалансом. Він стосується відставання темпів підвищення продуктивності інфокомунікаційних мереж за швидкістю передачі даних відносно темпів зростання бітової інтенсивності потоків відеоконтенту, які формуються на борту такої платформи. Такий дисбаланс спонукає виникненню значних часових затримок у процесі доставки відеоінформації, а отже призводить до втрат інформаційної актуальності щодо поточного стану об’єктів моніторингу (у разі обмеженого часу зв’язку з платформою відеокадр або їх група буде отримана не в повному обсязі). Отже, існує насущна потреба у вирішенні науково-прикладної задачі, яка полягає в підвищенні якості надання дистанційних відеосервісів із використанням бездротових інфокомунікаційних мереж у сучасному кіберпросторі.

Предметом обговорення є методи стиснення відеоконтенту в умовах забезпечення потрібного рівня їх достовірності в процесі доставки з використанням бездротових телекомунікаційних технологій на базі авіаційних платформ. Мета: обґрунтування технології кодування відеозображень для збільшення рівня їх стиснення в умовах забезпечення потрібної достовірності. Завдання: обґрунтувати підхід щодо структурної кластеризації трансформованих відеосегментів в умовах збереження їх достовірності; обґрунтувати розроблений метод структурно-статистичного кодування трансформант у спектрально-кластерному просторі.

Запропоновано нові принципи системи кодування відеоконтенту, що не пов’язані з можливою втратою інформації. Обґрунтовано розробку технології реструктурування трансформанти зображення для забезпечення перерозподілу їх компонент таким чином, щоб закон розподілу ймовірностей їх появи прагнув до нерівномірного; зменшення потужності

сукупностей (кластерів) даних; відмова від умови щодо забезпечення префіксності кодограм у разі збільшення потужності сукупностей даних або/та зменшення ймовірностей появи окремих компонент (використання рівномірного кодування); використання рівномірних кодових конструкцій, в тому числі в якості інформаційних опорних маркерів (тут кодограми окремих компонент можуть використовуватися як опорні маркери рівномірної довжини між послідовностями нерівномірних кодограм інших компонент); зменшення бітових витрат на інформативну частину кодової конструкції трансформанти та створення умов для стабілізації зміни ймовірностей для трансформант сегмента (стаціонарність статистичної моделі для трансформант в межах сегмента).

Варіантом для створення відповідних умов є здійснення кластеризації трансформанти зображення. Кластеризацію трансформанти пропонується здійснювати в двійковому просторі їх компонент. Створюється потенціал відносно додаткового скорочення кількості надмірності без втрат інформації з врахуванням залежностей у двійковому описі. В основі кластеризації лежить підхід до розбиття загального простору двійкових послідовностей із визначеною біт-довжиною. Такий загальний простір визначається сукупністю можливих перестановок із повторенням, які утворюються з двійкових послідовностей. Отже, кластеризація простору двійкових послідовностей з визначеною біт-довжиною полягає у формуванні окремих підмножин за структурною ознакою. При цьому необхідно забезпечити умову, коли підмножини не перетинаються.

Пропонується процес кодування кластеризованих компонент із додатковим врахуванням структурних залежностей. Відповідно, тут розроблений технологічний механізм обмеження росту довжин нерівномірної послідовності кодограм, особливо у випадку збільшення потужності кластеру або якщо розподіл ймовірностей появи компонент у кластері наближається до рівномірного закону. В основі такого технологічного механізму пропонується використовувати принцип дуальності компонент трансформанти. Він полягає в тому, що кластеризована компонента може одночасно розглядатись як елемент статистичного простору кластеру; допустимий елемент структурного кластеру, тобто як одна з допустимих перестановок із повтореннями з визначеною кількістю серій одиниць.

Отримані результати. Обґрунтовано потенційна ефективність представлення трансформанти в кластеризованому просторі за кількістю серій одиниць у двійковому описі їх компонент. Створено метод структурно-статистичного кодування в спектрально-кластерному просторі. Базовою складовою цього технологічного підходу є визначення та порівняння оцінок щодо потенційної спроможності усунення різних видів надмірності в поточному кластері у разі застосування методів кодування, які відповідно враховують його статистичні та структурні особливості. Порівняльне оцінювання виявило переваги створеного методу відносно методів кодування в стандартизованих платформах за показником пікового відношення сигнал/шум, як найменш на 30 %, за коефіцієнтом стиснення в середньому на 12 %.

Висновки. Наукова новизна отриманих результатів полягає в наступному: вперше створено метод структурно-статистичного кодування відеосегментів у спектральному просторі на основі їх кластеризації. Відмінності методу полягають: у використанні принципу дуальності компонент трансформанти, стосовно їх одночасної інтерпретації як: елемент статистичного простору кластеру; одна з допустимих перестановок із повтореннями з визначеною кількістю серій одиниць; визначенні потенційної спроможності щодо усунення різних видів надмірності в кластері у разі застосування методів кодування, які враховують його статистичні та структурні особливості. Це забезпечує підвищення рівня стиснення відеозображень для заданого рівня їх достовірності.

д-р філософії **Бернацький А. П.** ORCID: 0000-0003-0379-075X (ВІТІ ім. Героїв Крут)

ІННОВАЦІЙНІ ВЕКТОРИ ЦІЛЕСПРЯМОВАНОГО ВПЛИВУ НА АРС В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ВІЙНИ

У сучасній парадигмі ведення бойових дій застосування автономних роботизованих систем (АРС) набуває впливового значення у формі оперативних і тактичних одиниць, здатних самостійно чи групою виконувати розвідувальні, бойові та логістичні завдання в умовах динамічного та інформаційно-насиченого середовища. У зв’язку з цим потреба дослідження методів цілеспрямованого впливу на функціонування АРС, яка передбачає не лише їхнє фізичне ураження, а також охоплює широкий спектр інформаційних, кібернетичних та радіоелектронних засобів, постає як сучасний перспективний науковий виклик.

Ефективна протидія ворожим автономним роботизованим системам неможлива без глибокого аналізу векторів впливу на їхню інформаційно-кібернетичну архітектуру. У сучасних умовах АРС отримують більший інтелектуальний рівень, виступаючи автономними бойовими одиницями, спроможними до самостійного прийняття рішень і динамічного реагування на зміну обстановки, через що традиційні підходи до їх нейтралізації стають неефективними. Натомість формується системний підхід до інформаційно-кібернетичного впливу, що охоплює як фізичні, так і когнітивні рівні функціонування роботизованих платформ.

До найважливіших напрямів такого впливу слід віднести радіоелектронне придушення каналів зв’язку, що забезпечує ізоляцію системи шляхом глушіння, ін’єкції помилкових команд або порушення навігаційних протоколів (зокрема GNSS-jamming). Атакуючий вплив на сенсорні канали дозволяє штучно змінити просторове сприйняття системи, зокрема через засліплення камер, дестабілізацію LiDAR або вплив на інерціальні сенсори. Застосування кіберін’єкцій у комунікаційні та операційні протоколи відкриває шлях до проникнення в системи керування, особливо при наявності відкритих портів, застарілих прошивок або ненадійних API. Виконання поведінкових атак на ШІ-модулі базується на впровадженні хибних образів або навчальних патернів, що змушує автономну систему діяти помилково в умовах, які візуально або контекстно були модифіковані. Створення дестабілізації SWARM-координації реалізується через підміну командного вузла або ін’єкцію хибних повідомлень в алгоритми колективної взаємодії.

Усі ці вектори мають спільну мету переведення АРС зі стану цілеспрямованого функціонування у режим хаотичної або контрольованої дезорієнтації, що створює передумови для його локалізації, нейтралізації або знищення. Важливо розуміти, що маючи власну точку впливу, вони дозволяють не лише порушити цілісність бойового алгоритму, а й здійснити потенційні переорієнтації системи у вигідному для атакуючої сторони стратегічному напрямі.

Якщо ми хочемо не просто, «захищати» кібернетичні системи, а й будувати превентивну оборону й активно впливати на ворога, виникає потреба оцінити кожен метод саме як вектор атаки, де точка входу, що використовується як засіб впливу, і яка мета. Для кращого розуміння концепту застосування вектора атаки в якості превентивного захисту представлена матриця атак на кібернетичні АРС як систематизована таблиця.

Особливу увагу в системі засобів впливу на АРС слід приділити радіоелектронній розвідці (РЕР), яка, на відміну від традиційно пасивної ролі, дедалі частіше виконує функцію активного інформаційного вектора атаки. На сучасному етапі розвитку бойових АРС практично всі відомі системи характеризуються наявністю широкого спектра радіочастотної активності – від обміну телеметрією й командними пакетами до періодичної синхронізації в межах SWARM-протоколів. Саме ці сигнали, навіть за відсутності прямого контакту, є джерелами критично важливої інформації про тип, стан, режим роботи, а також топологію групового застосування АРС.

Методи РЕР дозволяють здійснювати реверс-аналіз протоколів зв’язку, визначати сигнатурні характеристики випромінювання та створювати так звані радіофізичні профілі

цілей. Така інформація в умовах бойового застосування може бути використана для формування предиктивних моделей поведінки, ідентифікації фаз активності, а також точного виявлення моментів запуску, перезавантаження чи комунікаційної синхронізації (таблиця 1).

Таблиця 1

№	Вектор атаки	Тип впливу	Ціль атаки	Приклад реалізації
1	Радіозв’язок	RER + протокольний вплив	Командні пакети, heartbeat, телеметрія	Spoofing команд; replay-атаки; MITM
2	LiDAR/Камера/ ІЧ-сенсор	Сенсорна атака	Навігація, картографія	Лазерне засліплення, LiDAR spoofing
3	IMU, GPS	Деструктивний вплив	Орієнтація, курс, позиціонування	GPS spoofing/jamming, магнітна ін’єкція
4	Wi-Fi/5G інтерфейс	Кіберпротокольний вплив	Доступ до API, обмін даними	Злом по SSH, ін’єкція через відкриті порти
5	Вразливість ROS/OS	Впровадження шкідливого ПЗ	Поведінка, навігація, виконання коду	Data poisoning, підміна карти, модифікація behavior tree
6	AI perception module	Маніпуляція через зображення	Модулі розпізнавання/дій	False QR codes, adversarial input для нейромереж
7	Swarm Protocol	Атака на алгоритм координації	Взаємодія між одиницями	Вкидання фейкового лідера, злам swarm-схеми
8	РЕР-профілювання	Пасивна атака + предикція	Виявлення, локалізація, поведінка	Визначення позицій за радіопідписом; предикція фаз дій
9	Фазові переходи системи	Атака на час/режим	Моменти оновлення/ перезавантаження	Захоплення при старті/ оновленні або скиданні стану
10	API/Update канали	Firmware poisoning	Повна компрометація системи	Fake update server; "підписані" шкідливі модулі

Крім того, РЕР дозволяє виявити потенційні вікна вразливості, пов’язані з оновленням програмного забезпечення, передачею нешифрованих пакетів або зміною режиму взаємодії з базовими станціями. У разі доступу до таких фаз відкривається можливість для прецизійної ін’єкції шкідливих сигналів, модифікації SWARM-команд або впровадження фальшивих структур управління.

Ще одним перспективним напрямом застосування РЕР є психологічне моделювання електронного середовища: шляхом створення приманкових або хибних сигналів можливо змусити ворожу систему вийти на контакт, виявити свою позицію, або ініціювати несанкціоновану поведінку. Такі операції можуть поєднуватись із активними заходами РЕБ, утворюючи багаторівневу систему впливу, що дестабілізує взаємодію не лише окремих одиниць, а й усього угруповання роботизованих платформ.

Отже, РЕР трансформується із класичного засобу спостереження у високоточний інструмент інформаційного втручання, здатний формувати нову якість бойової переваги. У поєднанні з кіберінструментами, когнітивною інженерією та методами поведінкової маніпуляції, РЕР стає критичним елементом наступальної інформаційно-роботизованої доктрини, де перемога визначається не лише потужністю засобів, а глибиною проникнення в логіку противника.

Таким чином, сучасні методи впливу на АРС мають розглядатись не лише з позицій безпеки, а й у якості елементів активної бойової стратегії. Їх інтеграція до загального інформаційно-розвідувального контуру дозволяє не просто реагувати на дії противника, а формувати випереджальну тактику глибокого інформаційного домінування. У межах сучасних і майбутніх збройних конфліктів саме такі підходи, що об’єднують засоби РЕР,

кіберрозвідки, ШІ-моделювання та протоколювання дій, визначатимуть ефективність керування і протидії автономним роботизованим формуванням на полі бою.

При цьому РЕР розглядається не лише як допоміжний інструмент ситуаційної обізнаності, а й як повноцінний вектор високоточних атак, що дозволяє як виявляти структурні вразливості АРС, так й ініціювати активні фази інформаційного впливу. В такому контексті РЕР набуває стратегічного значення як ключовий компонент інформаційно-роботизованої бойової доктрини, а її інтеграція в загальний архітектурний простір управління операціями створює передумови для прийняття випереджальних рішень у протидії автономним загрозам. Саме тому дослідження та моделювання атакуючих превентивних векторів є критично важливим для формування ефективних інформаційно-роботизованих стратегій у сучасному воєнному середовищі.

УДК 004.056

Блінов М. О. ORCID: 0009-0006-2164-3779 (ХНУ імені В.Н. Каразіна)
канд. техн. наук, ст. наук. співр. **Сватовський І. І.** ORCID: 0000-0002-1836-5599
(ХНУ ім. В. Н. Каразіна)

МЕТОДИ ТЕСТУВАННЯ БЕЗПЕКИ МЕРЕЖ: АНАЛІЗ І ПРАКТИЧНЕ ЗАСТОСУВАННЯ

Пентестинг, або тестування на проникнення, стає ключовим інструментом у сучасному підході до забезпечення кібербезпеки організацій, підприємств і державних установ. Через постійний розвиток цифрових технологій, зростання складності мережевих архітектур і збільшення обсягів оброблюваної інформації актуальність впровадження системного тестування на проникнення лише посилюється. Глобальний кіберпростір переживає хвилі атак, які дедалі частіше орієнтовані не лише на великі корпорації та органи державної влади, але й на невеликі компанії, освітні заклади, медичні установи. У цих умовах пентестинг дозволяє завчасно виявити вразливості в системах захисту, протестувати стійкість мережевої інфраструктури до атак і запобігти реальним інцидентам безпеки.

Метою роботи є аналіз відомих підходів до проведення пентестингу інформаційних ресурсів та особливостей їх практичної реалізації. На практиці пентестинг передбачає моделювання реальних атак з боку потенційного зловмисника. Це дозволяє не тільки імітувати техніки проникнення, а й перевірити готовність організації до реагування на кіберінциденти. Найбільш поширеними є три підходи: тестування «чорної скриньки» (без попередніх знань про систему), «білої скриньки» (з повною інформацією про інфраструктуру) та «сірої скриньки» (часткова обізнаність про систему). Такий поділ дозволяє обрати оптимальний сценарій перевірки залежно від мети дослідження та рівня доступу, наданого тестувальникам.

Загальний алгоритм тестування на проникнення в мережеві системи можна розділити на чотири основні етапи. Перший етап являє собою збір інформації, який у результаті дає докладне уявлення про можливі напрямки атаки цілі. На другому етапі проводиться цілеспрямоване проникнення, завданням якого є отримати несанкціонований доступ до скомпрометованих цілей за допомогою слабких місць безпеки або вразливостей, виявлених на попередньому етапі. Третій реалізує постексплуатацію, тобто дії зловмисника після того, як він скомпрометував вразливу ціль. У ньому представлені три основні концепції: забезпечення надійного повторного входу, збір облікових даних і горизонтальний перехід до нових доступних систем. Четвертий етап завершує проникнення написанням звіту про результати.

Особливої уваги заслуговують активні методи пентестингу, що включають використання спеціалізованих інструментів. Вони дозволяють проводити сканування портів, виявляти уразливості, експлуатувати знайдені недоліки та проводити постексплуатаційні дії. При цьому важливим елементом залишається етична сторона процесу: усі дії мають бути санкціонованими й проводитися в рамках правового поля, що особливо актуально в контексті українського законодавства та міжнародних стандартів ISO/IEC 27001:2022, PCI DSS, Penetration Testing Execution Standard (PTES).

Відповідно до кращих практик і рекомендацій міжнародних організацій із кібербезпеки, регулярне проведення тестування на проникнення має стати обов’язковим елементом стратегії безпеки будь-якої критичної інфраструктури. Це стосується не лише технологічної складової, а й людського фактору, який часто є найслабшою ланкою в системі захисту. Навчання персоналу, перевірка на фішингову вразливість, соціальна інженерія – усе це може бути частиною комплексного пентесту.

У роботі проведено аналіз використання інструментів, які можуть бути застосовані під час тестування. Результати аналізу свідчать про те, що для кожного окремого завдання можуть знадобитися різні інструменти. Тому впровадження широкого спектра інструментів, таких як сканери вразливостей, тестери на проникнення та інші засоби аналізу, дозволяє отримати

більш повну картину стану безпеки мережі. Найбільш інформативними та зручними у використанні показали себе такі інструменти, як: Nmap, Metasploit Framework і CrackMapExec.

Визначення цілей тестування на проникнення – це першочергове завдання, що вимагає чіткого розуміння мети та обсягу робіт. Перед початком тестування важливо провести зустрічі з керівництвом і технічними експертами, щоб визначити, які саме аспекти мережі будуть піддані аналізу та яка інформація про мережу буде надана. Це може включати ідентифікацію критичних активів, оцінку потенційних загроз і визначення конкретних цілей, таких як зниження ризиків або підвищення рівня безпеки.

У процесі проведеного на основі INPT (Internal Network Penetration Test) тестування було проведено дослідження безпеки мережі та порівняння ефективності методів виявлення вразливостей безпеки мережевих вебсервісів і баз даних. Із використанням останніх було отримано доступ до хостів, на яких вони працювали, та отримано можливість віддаленого виконання коду. Проведене тестування дало змогу провести аналіз і випробування загальної методики тестування безпеки мереж на проникнення та отримання оцінки загальних мережевих вразливостей.

У якості загальних рекомендацій можна зазначити, що для проведення тестування мереж слід ретельно підготуватись, зокрема визначити чіткі цілі та обсяг тестування. Необхідно використовувати різноманітні інструменти та методи для виявлення вразливостей, включаючи як автоматизовані сканери, так і ручні перевірки. Важливо імітувати реальні умови функціонування мереж, щоб отримати об’єктивну картину стану їх безпеки. Після виявлення вразливостей необхідно детально задокументувати всі знайдені проблеми та надати рекомендації щодо їх усунення. Регулярне повторне тестування допоможе оцінити ефективність впроваджених заходів безпеки та підтримати необхідний рівень захищеності мережі.

Таким чином, пентестинг є не просто технологічним процесом, а стратегічним компонентом загальної системи кіберзахисту. Він дозволяє не лише виявляти та усувати поточні вразливості, а й формувати культуру інформаційної безпеки, яка охоплює всі рівні функціонування організації. Подальше вдосконалення практик тестування на проникнення, підвищення рівня співпраці між державою, бізнесом та освітніми установами є важливим аспектом створення стійкої цифрової екосистеми України в умовах гібридної війни та глобальних загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Royce Davis. The Art of Network Penetration Testing: How to take over any company in the world - Simon and Schuster, 2020. 304 p.

2. Study Guide to Penetration Testing: A Comprehensive Guide to Learn Penetration Testing – Cybellium Ltd, 2024. 225 p.

3. Живило Є. О. Тестування на проникнення: навч. посіб. Ч. 2. Полтава: Національний університет імені Юрія Кондратюка, 2024. 239 с.

УДК 004.056

аспірант **Бородавка В. В.** ORCID: 0009-0002-3885-1364 (ХНУ імені В. Н. Каразіна)
д-р техн. наук, професор **Єсін В. І.** ORCID: 0000-0003-1977-7269 (ХНУ імені В. Н. Каразіна)

ВИКОРИСТАННЯ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ДЛЯ МОНІТОРИНГУ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВА З АРХІТЕКТУРОЮ НУЛЬОВОЇ ДОВІРИ

Актуальність. В умовах стрімкої цифрової трансформації, переходу бізнесу в онлайн, прискорених пандемією та війною, а також зі зростанням загроз та їх складністю у кіберпросторі, актуальність питань організації кібербезпеки підприємств набуває особливої значущості. Переважна частина підприємств досі використовує традиційні методи захисту на основі периметру, які виявляються неефективними перед сучасними кіберзагрозами, що при цьому не обмежуються виключно зовнішніми суб’єктами. Їх джерелом можуть бути як зовнішні, так і внутрішні користувачі, які можуть випадково або навмисно скомпрометувати свої облікові дані, що призводить до витоку конфіденційної інформації, її знищення або несанкціонованого розповсюдження. Це може бути обумовлено не тільки технічними вразливостями, але й людським фактором, зокрема особистими упередженнями, емоційним станом працівника, соціальним тиском або фінансовими труднощами. Окремо варто зазначити ризики, пов’язані з використанням пристроїв для віддаленої роботи, які можуть стати вектором для поширення шкідливого програмного забезпечення у внутрішнє середовище підприємства, що призводить до серйозних збитків для бізнесу як через втрату даних, так і внаслідок погіршення довіри з боку клієнтів і партнерів через тривалі репутаційні наслідки. У відповідь на такі виклики підприємства схиляються до нової концепції та архітектури захисту, а саме до парадигми безпеки під назвою «нульова довіра». Окремі принципи моделі нульової довіри самі собою не нові, новим є той факт, що всі ці принципи використовуються комплексно в рамках архітектури для захисту ресурсів підприємства. Ця модель ґрунтується на принципі «ніколи не довіряй, завжди перевіряй» і передбачає, що жоден користувач, пристрій або процес не повинен автоматично вважатися безпечним, навіть якщо вони знаходяться всередині корпоративної мережі. Разом із тим, ефективність впровадження архітектури нульової довіри (Zero Trust Architecture, ZTA) значною мірою залежить від здатності своєчасно виявляти вразливості, перевіряти дієвість політик керування доступом і забезпечувати стійкість до внутрішніх загроз. У зв’язку з цим, особливої актуальності набуває використання підприємствами тестування на проникнення (penetration testing) як засобу для перевірки реалізованої моделі безпеки та своєчасного виявлення слабких місць і вдосконалення ZTA. Тестування на проникнення дозволяє імітувати дії зловмисника з метою виявлення вразливих місць у механізмах захисту, оцінити їхній рівень ефективності та визначити потенційні шляхи обходу політик нульової довіри. Тому інтеграція тестування на проникнення у модель розгортання ZTA є необхідним етапом перевірки її ефективності на всіх рівнях і дозволяє адаптувати системи безпеки до реальних умов функціонування підприємства та своєчасно виявляти недоліки архітектури до того, як вони будуть використані зловмисниками.

Постановка задачі. Провести аналіз можливості впровадження ZTA на підприємстві з використанням методів тестування на проникнення для виявлення та нейтралізації вразливостей і кіберзагроз з метою підвищення загального рівня безпеки підприємства й забезпечення більш ефективного захисту.

Основні положення. Тестування на проникнення в межах ZTA є ключовим інструментом оцінки ефективності засобів захисту шляхом моделювання реальних сценаріїв кібератак. Одним із пріоритетних завдань тестування на проникнення є виявлення вразливостей у системах контролю доступу. Під час контрольованих атак перевіряється, чи здатен зловмисник обійти механізми автентифікації або скористатися надмірними або неналежно налаштованими правами доступу. Окрема увага приділяється оцінці ефективності впровадження мікросегментації, а саме проводиться моделювання бічного переміщення (lateral movement) в мережі, що дозволяє оцінити здатність архітектури до ефективного

стримування та локалізації інцидентів. Тестуванню на проникнення підлягають також системи керування ідентифікацією та контролю доступу, де перевіряються потенційні шляхи підвищення привілеїв, недоліки у механізмах автентифікації та помилки в обробці сеансів доступу. У контексті гібридних і хмарних середовищ, де ZTA реалізується між локальними та хмарними компонентами, важливо оцінити рівень безпеки при передачі даних між середовищами. Крім того, з огляду на постійну перевірку справжності/ідентифікації суб’єкта, а також виконання автентифікації та авторизації суб’єктів в рамках ZTA, тестуванню на проникнення підлягають кінцеві пристрої та застосунки, включно з виявленням вразливостей, пов’язаних із неправильними налаштуваннями або застарілим програмним забезпеченням.

З іншого боку, слід мати на увазі, що впровадження тестування на проникнення в ZTA супроводжується низкою викликів. Зокрема, динамічні політики безпеки, які адаптуються залежно від поведінки користувача та контексту, ускладнюють створення постійної методології тестування. Мікросегментація й посилений контроль доступу обмежують можливості традиційного тестування на проникнення, яке покладається на бічне переміщення, а засоби безперервного моніторингу з підтримкою штучного інтелекту можуть розцінювати дії при тестуванні як реальну загрозу, активуючи автоматизовані механізми реагування, що перешкоджає проведенню тестування на проникнення. Ще одним викликом є інтеграція тестування на проникнення в процеси DevSecOps протягом циклу розгортання ZTA, а команда тестування на проникнення повинна тісно співпрацювати з командою впровадження ZTA.

Тому, з метою усунення зазначених викликів, варто дотримуватися низки запропонованих практик. Передусім, необхідно чітко визначати цілі тестування, які повинні узгоджуватися зі специфікою архітектури, а саме перевіркою механізмів автентифікації, ефективності сегментації мережі, політик контролю доступу, налаштувань безпеки гібридної або хмарної інфраструктури. При цьому варто застосовувати механізми штучного інтелекту та засоби автоматизації для ефективного аналізу великих обсягів даних та моделювання сценаріїв атак. У свою чергу, використання підходів «червоної команди» (red team) і «блакитної команди» (blue team) у форматі взаємодії (purple team) дає змогу не лише моделювати реальні кібератаки, але й узгоджено перевіряти ефективність заходів безпеки. Також, особливу увагу слід приділити перевірці механізмів керування доступом, де ключовими аспектами при тестуванні на проникнення є потенційні методи обходу багатофакторної автентифікації, ризики перехоплення сеансів користувачів, перевірка політики паролів, а також вразливість до атак соціальної інженерії. У цьому контексті важливо враховувати, що взаємодія в межах ZTA дедалі частіше реалізується через API-з’єднання та хмарні провайдери. Відтак, актуальним стає тестування механізмів автентифікації для API, виявлення неправильних налаштувань хмарних сервісів, а також оцінка відповідності вимогам галузевих стандартів безпеки (наприклад, NIST 800-207, CIS Benchmarks). Однак ZTA передбачає наявність загроз не лише ззовні, тому важливим елементом є моделювання дій інсайдера. Зокрема, це можуть бути спроби ексфільтрації даних, підвищення привілеїв чи зловживання легітимними обліковими записами. Тому, з огляду на постійний розвиток концепції нульової довіри та ускладнення цифрового середовища підприємств, стратегії тестування на проникнення повинні регулярно оновлюватися. Це дає змогу своєчасно виявляти нові вектори атак і підтримувати належний рівень кібербезпеки підприємства.

Висновок. ZTA є ефективною моделлю кібербезпеки підприємства, однак її ефективність безпосередньо залежить від постійної перевірки та моніторингу, вдосконалення та розвитку відповідно до змін характеру загроз, завдань, технологій і нормативних документів. В результаті аналізу виявлено, що проведення тестування на проникнення має ключову роль при впровадженні ZTA і дозволяє не лише оцінити ефективність наявних засобів захисту та дотримання принципів нульової довіри, але й виявити слабкі місця, що можуть бути використані для компрометації корпоративної інфраструктури, а також встановити пріоритети для вдосконалення реалізації ZTA. Такий підхід забезпечує обґрунтовану й цілеспрямовану оптимізацію політик безпеки, орієнтовану на запобігання несанкціонованому доступу та зміцнення загальної кіберстійкості підприємства.

УДК 004.056.53

д-р техн. наук **Зайцев О. В.** ORCID: 0000-0003-2475-3800 (ВА ім. Євгенія Березняка)
д-р техн. наук **Попов М. О.** ORCID: 0000-0003-1738-8227 (НЦАКДЗ ІГН НАН України)
канд. техн. наук **Стефанцев С. С.** ORCID: 0000-0002-7629-7563 (ВА ім. Євгенія Березняка)

МЕТОД ВИЯВЛЕННЯ КІБЕРАТАК НА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ СИСТЕМИ З УРАХУВАННЯМ ЧИННИКА КОГНІТИВНОСТІ

Вступ. Сучасні інформаційно-комунікаційні системи (ІКС) зазнають кіберзагроз, які зростають кількісно і стають більш складними для виявлення. Традиційні методи кіберзахисту, основані на сигнатурному та поведінковому аналізі, часто не забезпечують достатньої ефективності через високу варіативність атак, адаптивність зловмисників та обмеження алгоритмічних підходів.

Одним із перспективних напрямів удосконалення методів виявлення кіберзагроз є врахування чинників когнітивності, які впливають на процес прийняття рішень у сфері кібербезпеки. Людський фактор, зокрема експертні оцінки, інтуїтивне розпізнавання аномалій та евристичні методи аналізу можуть суттєво підвищити ефективність систем виявлення атак. Водночас когнітивні особливості операторів та аналітиків можуть як сприяти точності виявлення загроз, так і створювати додаткові виклики, пов’язані з когнітивними упередженнями, перевантаженням інформацією та обмеженістю ресурсів уваги.

Таким чином, постає проблема розробки підходу до виявлення кібератак на ІКС, який би вдосконалив автоматизовані алгоритми аналізу загроз з урахуванням когнітивних чинників, що впливають на ефективність прийняття рішень у сфері кібербезпеки. Вирішення цієї проблеми дасть можливість підвищити рівень кіберзахисту та зменшити ймовірність успішних атак на критично важливі системи.

Метою дослідження є розробка методу виявлення кібератак на ІКС з урахуванням чинника когнітивності.

Виклад основного матеріалу. Виявлення кібератак розглядається крізь призму аналізу як технологічних, так і когнітивних аспектів. Досліджено сучасні підходи до виявлення атак у зарубіжній і вітчизняній практиці. Зокрема, проаналізовано позиції Майкла П. Кройцера щодо багатовимірності простору бойових дій, а також дослідження українських науковців: С. Толюпи, Ю. Самохвалова, П. Хусаінова, С. Штаненка, О. Мазулевського та Н. Жолобовича щодо оцінки кіберстійкості технологічних систем [1–3]. Проте в наявних роботах недостатньо враховано когнітивний аспект.

У Законі України “Про захист інформації в інформаційно-комунікаційних системах” наведено визначення терміну інформаційно-комунікаційна система – це сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле [4]. Ці системи різняться між собою функціоналом, архітектурою побудови та рівнем підготовки операторів із протидії кіберзагрозам. Логіко-обчислювальний блок обробки й аналізу інформації про інцидент кібербезпеки в кожній з цих систем може бути побудовано на базі байєсівських мереж [5; 6].

Зважаючи на можливу неоднозначність і неповноту даних, що надаються операторами з протидії кіберзагрозам, як математичну платформу методу автори обрали інструментарій теорії Байєса, що дає можливість не лише формально оцінювати ймовірність кібератак, але й інтегрувати когнітивні аспекти процесу прийняття рішень. До основних переваг застосування цієї теорії слід віднести такі:

гнучкість і адаптивність – система постійно оновлює свої оцінки на основі нових даних, що дає змогу виявляти нові загрози й адаптуватися до мінливого кіберсередовища;

інтеграція різних джерел даних – байєсівський підхід дає змогу брати до уваги одночасно декілька ознак і джерел інформації, зокрема експертні оцінки, що підвищує точність прогнозування загроз.

Чинник когнітивності відіграє важливу роль у процесі оцінювання ймовірностей, оскільки експерти (аналітики) схильні до певних когнітивних упереджень (наприклад, ефекту доступності або упередженості підтвердження). Застосовуючи байєсівський підхід, можна мінімізувати вплив таких упереджень, формалізуючи процес оновлення оцінок на основі об’єктивних статистичних залежностей.

Використання теорії Байєса для виявлення кібератак допомагає не лише оцінити ймовірність загрози на основі відомих даних, а й підвищити ефективність прийняття рішень завдяки систематичному врахуванню як емпіричних даних, так і експертних суджень. Це сприяє формуванню більш надійної системи кіберзахисту, що адаптується до нових викликів і враховує як технологічні, так і когнітивні аспекти аналізу загроз. Алгоритм виявлення кібератак на ІКС з урахуванням чинника когнітивності наведено на рисунку 1.

Рис. 1. Алгоритм виявлення кібератак на ІКС з урахуванням чинника когнітивності

Крок 1. Формування гіпотез.

Розглянути стан ІКС як дві можливі гіпотези:

$H1$ – на ІКС здійснено кібератаку;

$H0$– кібератаки немає, ІКС працює в нормальному режимі (система у справному стані).

На цьому етапі когнітивний чинник впливає на формування гіпотез, оскільки експерти можуть мати певні упередження (наприклад, недооцінювати або переоцінювати ймовірність атак залежно від попереднього досвіду).

Крок 2. Визначення апріорної ймовірності кібератак.

Апріорна ймовірність – це початкова оцінка ймовірності того, що в цей момент відбувається кібератака. В основі оцінки можуть бути попередні дані про кількість кібератак за певний період. Наприклад, якщо кібератаки є рідкісним явищем – ймовірність $P(H1)$ здійснення кібератаки на ІКС буде низькою, а ймовірність $P(H0)$ нормальної роботи ІКС – високою.

Відповідно до байєсівського підходу приймемо, що апріорно всі гіпотези щодо можливого стану ІКС однаково ймовірні.

$$P^{pr}(H_1) = P^{pr}(H_2) = \ldots = P^{pr}(H_N) = 1/N, \quad (1)$$

де $P^{pr}(H_i)$ – апріорна ймовірність гіпотези H_i.

Проте цю оцінку може бути скориговано відповідно до експертного аналізу та суб’єктивного досвіду, що є важливим аспектом когнітивного сприйняття ризику.

Крок 3. Збір свідчень (інформації про інцидент кібербезпеки). Збір нових даних чи сигналів про можливу кібератаку, які можуть включати виявлені аномалії в мережевій активності або невідповідності в поведінці користувачів чи в роботі ІКС.

Очевидно, що після надходження кожного чергового свідчення E^i значення ймовірностей гіпотез можуть змінюватися. Ймовірності гіпотез $P(H_1)\ldots P(H_N)$ за підсумками розгляду поточного свідчення E^i обчислюють за формулою [7]:

$$P^i(H_n) = P(H_n|E^i) \cdot d^i + P(H_n|\neg E^i) \cdot (1 - d^i), \quad (2)$$

де $P(H_n|E^i)$ – ймовірність гіпотези H_n, з урахуванням свідчення E^i;

$P(H_n|\neg E^i)$ – ймовірність гіпотези H_n до надходження свідчення E^i;

d^i – ймовірність $P(H1)$ здійснення кібератаки на ІКС;

$(1 - d^i)$ – ймовірність $P(H0)$ того, що кібератаки на ІКС немає;

$n = 1,2,\ldots,N$.

Роль чинника когнітивності полягає в тому, як експерти інтерпретують дані. Наприклад, можуть виникати такі когнітивні упередження:

ефект доступності – переоцінка ризику на основі кількості нещодавніх атак;

консерватизм – недооцінка нових загроз через прив’язаність до старих даних.

Схему розрахунків за формулою (2) зображено на рисунку 2.

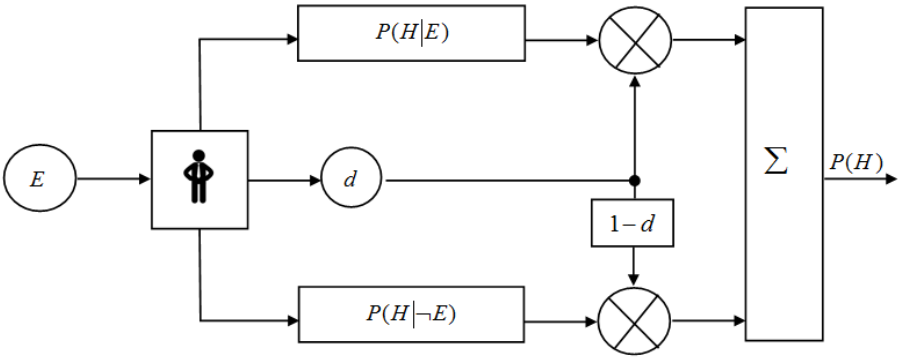

Рис. 2. Схема розрахунків за формулою (2)

Крок 4. Обчислення апостеріорної ймовірності.

Для обчислення апостеріорної ймовірності того, що кібератака відбувається, можна застосувати теорему Байєса, враховуючи нові дані (свідчення):

$$P^i_{aps}(H_n) = \frac{P(H_n|E^i) \cdot d^i}{P^i(H_n)}, \quad (3)$$

де $P^i_{aps}(H_n)$ – апостеріорна ймовірність.

Беручи до уваги нові дані, а також історичні патерни загроз, можна більш обґрунтовано оцінити ризик кібератаки.

Крок 5. Аналіз ризиків на основі отриманих результатів. Прийняття рішення.

Апостеріорна ймовірність $P^i_{aps}(H_n)$ вказує, наскільки ймовірно те, що атака відбувається. Якщо $P^i_{aps}(H_n)$ перевищує певний поріг (який визначається відповідно до політики безпеки), можна вважати атаку ймовірною і вжити відповідних заходів.

На цьому етапі когнітивні чинники можуть впливати на поріг сприйняття загрози таким чином:

надмірна обережність може призвести до великої кількості хибних спрацювань;

недооцінювання ризику може спричинити несвоєчасне реагування на атаку.

Отже, поєднання байєсівського підходу та чинника когнітивності дає можливість удосконалити систему виявлення кібератак, зробивши її більш адаптивною та ефективною.

Приклад. Припустимо, що на ІКС здійснено DDoS-атаку (атака на комп’ютерні системи органу, організації, установи з метою порушення доступності вебресурсів) [8].

Виконуємо дії згідно з розробленим методом:

Крок 1. Формулювання гіпотез.

$H1$ – на ІКС здійснена DDoS-атака;

$H0$ – кібератаки немає, ІКС працює в нормальному режимі.

На цьому кроці когнітивні чинники можуть впливати на формування гіпотез. Наприклад, якщо оператор у минулому часто стикався з хибними спрацюваннями, він може несвідомо занижувати ймовірність атаки (когнітивний ефект “втоми від тривоги”).

Крок 2. Визначення апріорної ймовірності кібератак.

На основі наявних даних припустимо, що DDoS-атаки відбуваються в середньому один раз на тиждень, а нормальний трафік спостерігається протягом решти часу. Оскільки в тижні 168 годин, ймовірність того, що в довільний момент часу здійснюється DDoS-атака $P(H1) = \frac{1}{168} = 0{,}006$, а ймовірність нормального стану системи $P(H0) = 1 - P(1) = 0{,}994$.

Чинник когнітивності проявляється в оцінюванні апріорних ймовірностей. Експерти можуть надавати перевагу власному досвіду над статистичними даними, що може призводити до зміщення оцінок.

Крок 3. Збір свідчень (інформації про інцидент кібербезпеки).

ІКС фіксує кількість запитів на сервер щохвилини. Виявлено 2000 запитів за хвилину, що суттєво перевищує середнє значення.

Припустимо, що ймовірність отримання 2000 запитів за хвилину за умови DDoS-атаки становить $P(H_n|E^i) = 0{,}9$.

Якщо кібератаки немає і система працює нормально ($H0$), ймовірність отримання 2000 запитів за хвилину дуже низька, $P(H_n|\neg E^i) = 0{,}1$.

На цьому кроці когнітивний чинник може впливати на трактування даних. Наприклад, оператор може вважати, що аномальна активність пов’язана з технічними збоями, а не атакою (ефект “помилкової кореляції”).

Крок 4. Обчислення апостеріорної ймовірності.

За формулами (2) і (3) обчислюємо апостеріорну ймовірність:

$$P^i_{aps}(H_n) = \frac{0{,}9 \times 0{,}006}{0{,}9 \times 0{,}006 + 0{,}1 \times 0{,}994} = \frac{0{,}0054}{0{,}0054 + 0{,}0994} = 0{,}052.$$

Тобто після отримання нового свідчення ймовірність атаки зросла з 0,6 % до 5,2 %, однак усе ж залишається низькою.

Крок 5. Аналіз ризиків на основі отриманих результатів. Прийняття рішення.

Припустимо, що система безпеки встановлює поріг реагування на рівні 30 %. Оскільки апостеріорна ймовірність 5,2 % не перевищує цього порогу, система не активує механізми захисту.

Однак якщо надходять додаткові свідчення (наприклад, затримка відповідей сервера або одночасне надходження запитів із великої кількості IP-адрес), то нові розрахунки можуть вказувати на вищу ймовірність атаки, що змусить приймати рішення щодо реагування.

У наведеному прикладі аномальна кількість запитів суттєво підвищила ймовірність DDoS-атаки, але не перевищила поріг, за якого система безпеки швидко вживає відповідних заходів. Врахування чинника когнітивності дозволяє зменшити ризики помилкових рішень та підвищити ефективність кіберзахисту системи.

Приймаючи рішення, слід враховувати вплив чинника когнітивності, а саме:

упередженість у сприйнятті загроз. Якщо оператор рідко стикається з DDoS-атаками, він може недооцінювати ризики та ігнорувати перші ознаки атаки;

ефект “втоми від тривог”. Велика кількість хибних спрацювань може призвести до того, що оператор не звертатиме увагу на критичні сигнали;

психологічний поріг реагування. Встановлення занадто високого порогу для виявлення атак може стати причиною затримки в прийнятті рішень.

Таким чином, байєсівський підхід у поєднанні з чинником когнітивності дає можливість не лише об’єктивно оцінювати загрози, а й враховувати психологічні аспекти, що впливають на прийняття рішень експертами.

Висновки. Застосування байєсівського підходу для аналізу інформаційно-комунікаційної системи дає можливість: динамічно оновлювати оцінки загроз на основі нових даних; інтегрувати різні джерела інформації для підвищення точності виявлення атак; ефективно працювати в умовах невизначеності та часткової чи суперечливої інформації.

Окрім математичної складової, важливим є вплив когнітивних чинників на прийняття рішень експертами, зокрема:

оператори можуть недооцінювати або переоцінювати ризики залежно від попереднього досвіду;

ефект “втоми від тривог” може призвести до ігнорування критичних загроз;

психологічний бар’єр реагування може вплинути на встановлення порогу виявлення атак.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Michael P. Kreuzer. Cyberspace is an Analogy, Not a Domain: Rethinking Domains and Layers of Warfare for the Information Age. *The Strategy Bridge*. 2021. URL: https://thestrategybridge.org/the-bridge/2021/7/8/cyberspace-is-an-analogy-not-a-domain-rethinking-domains-and-layers-of-warfare-for-the-information-age (дата звернення: 29.04.2025).

2. Толюпа С., Самохвалов Ю., Хусаінов П., Штаненко С. Самодіагностування як спосіб підвищення кіберстійкості термінальних компонентів технологічної системи. *Кібербезпека: освіта, наука, техніка*. 2023. № 2 (22). С. 134–147. URL: https://doi.org/10.28925/2663-4023.2023.22.134147 (дата звернення: 28.04.2025).

3. Мазулевський О., Жолобович Н. Оцінка поточного стану кіберстійкості з урахуванням ситуації у кіберпросторі. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2024. № 3 (51). С. 34–40. URL: https://doi.org/10.33099/2311-7249/2024-51-3-34-40 (дата звернення: 28.04.2025).

4. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР: зі змінами від 28 черв. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр (дата звернення: 28.04.2025).

5. Moffat J., Witty S. Bayesian decision making and military command and control. *Journal of the Operational Research Society*, 2002. № 53 (7). P. 709–718. URL: https://doi.org/10.1057/palgrave.jors.2601347 (дата звернення: 28.04.2025).

6. Sutton C., Morrison C., Cohen P.R., Moody J., Adibi J. A Bayesian blackboard for information fusion / Proc. 7th Int. Conf. on Information Fusion, Stockholm, Sweden, June 2004. P. 1111–1116.

7. Farmer M. E. Integrating Temporal Streams of Image Classifications Using Evidential Reasoning for Smart Airbag Applications / Proc. of the IEEE Conference on Electro-information Technology, 2006. P. 360–365.

8. Що таке DDoS-атака? Державна служба спеціального зв’язку та захисту інформації України. URL: https://cip.gov.ua/ua/faqs/sho-take-ddos-ataka (дата звернення: 28.04.2025).

Колєсніков О. Є. (ХНУ імені В. Н. Каразіна)
канд. техн. наук, доцент **Єсіна М. В.** (ХНУ імені В. Н. Каразіна)

МЕХАНІЗМИ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ У МОБІЛЬНИХ ЗАСТОСУНКАХ

Вступ

Із розвитком мобільних технологій та зростанням обсягів обробки конфіденційних даних значно зросли вимоги до механізмів автентифікації у мобільних застосунках. Одним із найбільш ефективних рішень є впровадження багатофакторної автентифікації, що базується на TOTP-кодах та біометрії.

Мета

Метою дослідження є аналіз сучасних підходів до реалізації багатофакторної автентифікації в мобільних застосунках, зокрема за допомогою одноразових паролів (TOTP) і біометричних методів, а також вивчення можливостей інтеграції таких механізмів у безпечну архітектуру мобільних інформаційних систем із урахуванням сучасних загроз.

TOTP та біометрія в мобільній автентифікації

У сучасності, методи та засоби автентифікації у мобільних застосунках здебільшого визначають загальну захищеність інформаційних систем, що працюють із чутливими даними користувачів. Майже всі люди кожен день користуються своїми гаджетами для проведення операцій в онлайн-банкінгу, зберігання особистих документів або виконання хмарних обчислень, внаслідок чого вимоги до надійності автентифікації зростають.

Одним із численних надійних методів автентифікації є використання одноразових кодів доступу, а саме TOTP (Time-based One-time Password). TOTP відповідає документу із серії пронумерованих документів Інтернету – RFC 6238 [1]. Коди у зазначеному методі генеруються на основі симетричного ключа та поточного світового часу із застосуванням криптографічної геш-функції HMAC-SHA1, HMAC-SHA256 або HMAC-SHA512. Використовувана комбінація засобів у методі забезпечує унікальність кожного створеного коду в заданий момент часу, із чого можна зробити висновок, що неможливо повторно використати один і той самий код. Генерація такого роду є ефективним захистом від атак типу replay (повторення).

Основною вимогою при використанні подібних рішень є надійне та безпечне збереження секретного ключа. У середовищі Android для досягнення цих цілей можна застосовувати Keystore API – систему, яка дозволяє зберігати криптографічні ключі у контейнері та ускладнює їх витяг із пристрою. Як тільки секрет (ключ) попадає у сховище, його використання звужується до меж системи і експорт стає недоступним. Також, система збереження дає змогу обмежити використання ключів і усередині системи, визначивши які саме дії повинні виконуватися та хто може їх виконувати [2]. Зберігання ключа в апаратному модулі (Hardware-Backed Keystore) додатково захищає його навіть у разі ескалації привілеїв або наявності шкідливого ПЗ на пристрої.

У моделі багатофакторної автентифікації важливим є не тільки фактор – знання (секретного ключа), а й інші два – володіння (фізичний доступ до пристрою) та властивості (те, ким є користувач). Фактор властивості найкраще розкривається у виді біометричної автентифікації. Сучасні пристрої та платформи підтримують використання біометричних даних, а саме: відбитків пальців, райдужних оболонок ока або розпізнавання обличчя. У мобільних операційних системах обробка біометричних даних відбувається у захищених середовищах – Trusted Execution Environment (TEE), Secure Enclave або Secure Element [3]. Вони забезпечують ізоляцію процесу верифікації та запобігають доступу до біометрії навіть з боку ОС. В Android, інтерфейси, такі як BiometricPrompt, дозволяють застосункам викликати автентифікацію без обробки самих біометричних даних – програма отримує лише результат (вдало/невдало), що у результаті значно знижує ризики витоку чутливих даних. Зазначений підхід відповідає принципам GDPR, NIST SP 800-63 та інших стандартів приватності.

У поєднанні двох розглянутих методів автентифікації у багатофакторну архітектуру ми отримуємо систему, яка схематично визначена на рисунку 1.

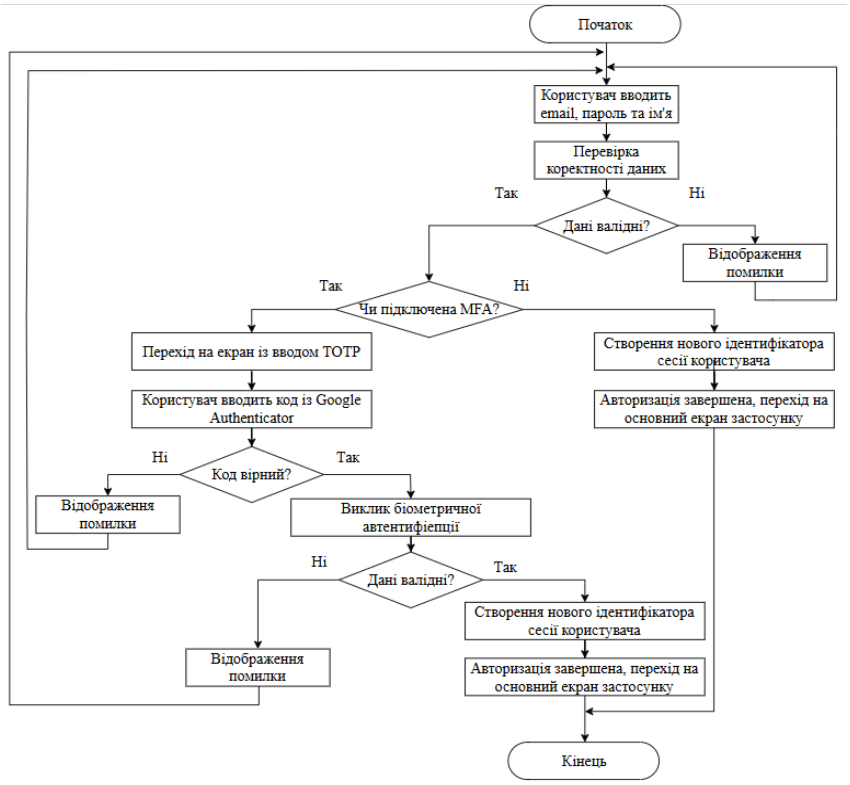

Рис. 1. Схема процесу автентифікації із використання комбінації TOTP та біометрії

Зазначена багатофакторна архітектура може протистояти широкому спектру загроз, а саме:

- атаки фішингу (phishing);
- атаки повторного відтворення (replay attacks);
- атаки грубої сили (brute-force) або атаки за словником (dictionary) на паролі;
- компрометація пристрою;
- перехоплення даних у мережі.

Додаткову стійкість системі можна забезпечити через запровадження механізмів обмеження – кількість спроб входу, довжина та використання спеціальних символів під час створення паролів, час затримки після великої кількості невдалих спроб входу та ін.

Розглянуті системи можуть бути масштабовані для корпоративного середовища, державного використання, фінансових застосунків та електронного документообігу. Впровадження багаторівневих систем автентифікації з використанням криптографічно стійких алгоритмів і біометричних даних є передовим чинником у забезпеченні безпеки кіберпростору.

Висновки

TOTP і біометрична автентифікація є ключовими складовими надійної багатофакторної системи доступу. Їх використання у мобільних середовищах сприяє підвищенню рівня захисту користувачів і відповідає сучасним стандартам кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. TOTP: Time-Based One-Time Password Algorithm // URL: https://datatracker.ietf.org/doc/html/rfc6238.

2. Developers. Android Keystore system // URL: https://developer.android.com/privacy-and-security/keystore.

3. Mobile device forensics: comparison of mobile encryption hardware and software // URL: https://www.researchgate.net/publication/387479483_MOBILE_DEVICE_FORENSICS_COMPARISON_OF_MOBILE_ENCRYPTION_HARDWARE_AND_SOFTWARE.

УДК 004.056

Ластовець О. С. ORCID: 0009-0008-3739-1849 (ВІТІ ім. Героїв Крут)

МЕТОДОЛОГІЯ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ: ПРИНЦИПИ ПОБУДОВИ ЕФЕКТИВНИХ ПРОЦЕДУР РЕАГУВАННЯ

Актуальність теми. У сучасних умовах стрімкого зростання кіберзагроз своєчасне та ефективне реагування на кіберінциденти є критично важливим для забезпечення безпеки інформаційних систем. Організації стикаються з новими видами атак, що вимагають не лише технічних рішень, а й чітко розроблених процедур реагування. Відсутність стандартизованих підходів до реагування суттєво підвищує ризики для бізнесу та державних структур.

Мета роботи. Розробити методологічні принципи побудови ефективних процедур реагування на кіберінциденти, що забезпечують мінімізацію наслідків атак, швидке відновлення діяльності та безперервне удосконалення систем безпеки.

Виклад основного матеріалу.

Кіберінцидент – це будь-яка подія, яка має потенціал або вже призвела до порушення конфіденційності, цілісності чи доступності інформації або IT-інфраструктури. Інциденти можуть бути спричинені як зовнішніми атаками (наприклад, фішинг, DDoS, зловмисне ПЗ), так і внутрішніми загрозами (недбалість співробітників, інсайдери). Для ефективного реагування важливо класифікувати інциденти за рівнем критичності:

- Критичні – впливають на основні сервіси або призводять до витоку важливої інформації.
- Серйозні – порушують окремі функції, але не призводять до катастрофічних наслідків.
- Незначні – локалізовані події, що не впливають на загальний стан безпеки.

Стандарти NIST SP 800-61 та ISO/IEC 27035 описують реагування як процес, що охоплює кілька ключових етапів:

- Підготовка (Preparation). Цей етап включає: створення команди реагування на інциденти (IRT/CSIRT), розробку політик та процедур реагування, налаштування систем моніторингу та сповіщення, забезпечення навчання персоналу.
- Виявлення та аналіз (Detection and Analysis). Інциденти мають бути виявлені якомога швидше за допомогою SIEM-систем, логування, IDS/IPS. Після виявлення важливо провести: початкову оцінку інциденту, аналіз джерела, типу загрози та уразливостей, визначення масштабу впливу.
- Реагування та стримування (Containment, Eradication and Recovery). Мета – мінімізувати збитки та відновити нормальну роботу: ізоляція уражених систем, видалення зловмисного ПЗ або користувача, оновлення систем безпеки та резервне відновлення даних.
- Постінцидентна діяльність (Post-Incident Activity). Після інциденту слід: провести розслідування причин, оновити політики та процедури, підготувати звіт та провести навчання на основі інциденту, перевірити ефективність заходів реагування.

Команда CSIRT має чітко визначені ролі та повноваження. Її функції включають: моніторинг подій, координацію дій під час інциденту, комунікацію із зовнішніми структурами (CERT, правоохоронні органи), формування звітності для керівництва.

Важливу роль в автоматизації процесів реагування на кіберінциденти відіграють інструменти SOAR (Security Orchestration, Automation, and Response). Вони дозволяють: скоротити час реагування, автоматизувати рутинні дії (наприклад, блокування IP, створення тикетів), підвищити точність аналізу даних. Використання машинного навчання та аналітики допомагає прогнозувати інциденти й аналізувати тенденції атак.

Періодичні тренування персоналу (tabletop exercises, Red Team/Blue Team симуляції) дозволяють перевірити готовність до реальних інцидентів і вдосконалити взаємодію між підрозділами.

Висновок. Ефективне реагування на кіберінциденти неможливе без чіткої методології, що охоплює підготовку, виявлення, нейтралізацію загроз і навчання. Важливими умовами успішної реалізації є наявність професійної команди реагування, актуальних процедур, використання інструментів автоматизації та постійне вдосконалення на основі аналізу попередніх інцидентів. Побудова такої системи дозволяє зменшити наслідки атак, забезпечити кіберстійкість організації та підтримувати довіру користувачів і партнерів.

Логачова Є. О. (ХНУ імені В. Н. Каразіна)
канд. техн. наук, доцент **Єсіна М. В.** (ХНУ імені В. Н. Каразіна)

ІНФОРМАЦІЙНА МОДЕЛЬ РЕГУЛЮВАННЯ БЕЗПЕКИ ШТУЧНОГО ІНТЕЛЕКТУ В УКРАЇНІ

Вступ. Розумні технології, що ґрунтуються на штучному інтелекті (ШІ), стрімко поширюються в різних сферах життя – від повсякденного використання до медицини та сфери безпеки. Водночас зростає потреба в забезпеченні належного рівня безпеки цих технологій. У відповідь на це в Європейському Союзі та низці інших країн вже з’явилися перші нормативно-правові акти, спрямовані на регулювання ШІ. В Україні ж поки що відсутнє єдине бачення щодо необхідності запровадження подібних регулювань, хоча перші кроки у цьому напрямі вже зроблено.

1. Класифікація ризиків, пов’язаних із використанням штучного інтелекту

Перші спроби створення ШІ були ще у 90-х роках минулого століття, та найбільшим моментом прогресу вважається 2023 рік, у якому відбувся випуск GPT-3 та його наступників. А вже у 2024 році ці розробки показують неабиякий прогрес у генеруванні зображень, текстів, аудіо й іншого. До того ж було помічено прогрес у навчанні ШІ, завдяки якому помічники на основі ШІ здатні брати участь у природних, контекстних розмовах, а також допомагати з різноманітними завданнями [1].

ШІ несе за собою не менший список загроз і ризиків, наприклад: проблеми з конфіденційністю, алгоритмічна упередженість, неетичне використання, можливі втрати робочих місць, автоматизація кібератак, проблеми довіри та контролю, використання ШІ для атак соціальної інженерії, атаки на самі алгоритми штучного інтелекту та багато іншого. У документі EU AI Act проводиться поділ ШІ за рівнями ризиків, відповідно до яких мають бути задіяні різні правила. За цим розподілом ризики, які несуть за собою технології ШІ, поділяють на три типи: неприйнятний, високий і мінімальний [2].

2. Міжнародні регуляторні заходи з безпеки використання штучного інтелекту

Одним із перших органів, що висловив занепокоєння щодо потенційних ризиків, пов’язаних із ШІ, став Конгрес США. У 2023 році генеральний директор компанії OpenAI Сем Альтман закликав Конгрес запровадити регулювання в цій сфері. Яскравим прикладом таких зусиль стало ухвалення 17 травня 2024 року в штаті Колорадо першого в США комплексного закону про ШІ – Колорадського закону про штучний інтелект. Цей нормативний акт визначає обов’язки як для розробників, так і для користувачів систем ШІ. Основна увага приділяється автоматизованим системам ухвалення рішень. Зокрема, під поняття «високоризикована система ШІ» підпадають ті, що під час використання ухвалюють рішення або суттєво впливають на остаточне рішення. Закон набуде чинності у 2026 році [3]. Ще одним стандартом у цій галузі є NIST AI Risk Management Framework [4]. Це методичний посібник, створений для організацій, які використовують або розробляють генеративний ШІ (GAI). Він допомагає: визначити та зрозуміти ризики, пов’язані з GAI (наприклад, deepfakes, порушення приватності, токсичний контент тощо); розробити політики, стратегії та дії для ефективного управління цими ризиками; дотримуватись міжнародних стандартів і принципів довіри, безпеки та прозорості ШІ [4].

Регулювання, введені у ЄС, мають дещо інший характер. У країнах ЄС закликають вводити певні регулювання і обмеження не тільки на рівні держав у контексті ШІ, а й на приватному громадському рівні. Регламент ЄС 2024/1689 є важливим правовим документом Європейського Союзу, який встановлює гармонізовані правила для використання ШІ у різних сферах. Його основною метою є створення єдиного правового поля для регулювання ШІ у країнах-членах ЄС. Регламент зобов’язує розробників і постачальників ШІ забезпечувати можливість людського контролю, мінімізувати дискримінаційні ризики та захищати права людини. Документ також вносить зміни до кількох існуючих європейських регламентів, таких як транспорт, захист даних і безпека продукції, щоб узгодити вимоги ШІ з чинним законодавством. Наступним важливим рішенням стала директива NIS2, яка не фокусується

безпосередньо на регулюванні ШІ, але одним із ключових аспектів є те, що NIS2 розширює вимоги до кібербезпеки для критичних інфраструктур і послуг, включаючи ті, де використовуються технології ШІ [5].

3. Інформаційна модель регулювання безпеки штучного інтелекту в Україні

Попри відсутність активної публічної дискусії щодо регулювання ШІ в Україні, певні ініціативи в цьому напрямку вже реалізуються. Зокрема, Україна приєдналася до Декларації Bletchley, підписаної під час Саміту з безпеки ШІ у 2023 році. Крім того, була розроблена так звана Біла книга, яка має на меті сприяти конкурентоспроможності українського бізнесу, забезпечити захист прав людини та підтримати процес євроінтеграції. У документі пропонується етапний підхід: від використання позазаконодавчих інструментів та ініціатив у найближчі роки – до ухвалення спеціального закону про ШІ на завершальному етапі. Водночас запропонована модель прагне вибудувати систему регулювання безпеки ШІ в Україні більш узгоджено та інтегровано із міжнародними практиками [5].

У моделі пропонується додати більше суб’єктів діяльності, пов’язаної з ШІ, а також інтегрувати вже відомий з EU AI Act розподіл за рівнями ризику. Запропоновану модель наведено на рисунку 1.

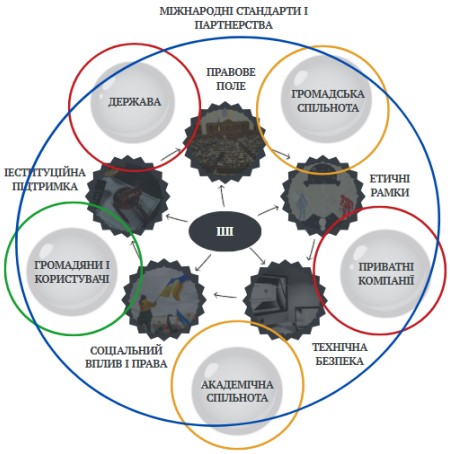

Рис. 1. Модель регулювання безпеки ШІ в Україні

Висновки. Швидкий розвиток технологій ШІ вимагає від держав комплексного підходу до безпеки і регулювання, з урахуванням міжнародного досвіду та національних реалій. Україна, попри відсутність усталеного законодавчого поля у сфері ШІ, уже робить кроки у напрямку гармонізації з європейськими стандартами. Запропонована інформаційна модель регулювання дозволяє систематизувати ризики, окреслити ролі ключових суб’єктів і сформувати адаптивну систему, орієнтовану на захист прав людини, кібербезпеку та інноваційний розвиток.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What is artificial intelligence (AI)? // ISO. 2024. URL: https://www.iso.org/artificial-intelligence/what-is-ai-v3.

2. EU AI Act: first regulation on artificial intelligence. European Parliament, 2025. URL: https://surl.li/abxfru.

3. AI Watch: Global regulatory tracker – United States. White & Case LLP, 2024. URL: https://surl.li/snkzfd.

4. Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile, U.S. Department of Commerce Gina M. Raimondo, Secretary NIST Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology, 2024. URL: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf.

5. Логачова Є. О, Єсіна М. В. Штучний інтелект: сучасні загрози та безпека. 2024.

УДК 004

д-р філософії **Марченко В. В.** ORCID: 0000-0003-4271-3132 (ДУІКТ)
д-р техн. наук, професор **Гайдур І. І.** ORCID: 0000-0003-0591-3290 (ДУІКТ)
Кушнір Д. І. ORCID: 0009-0007-2284-4625 (КПУ)

ВИКОРИСТАННЯ OSINT-ІНСТРУМЕНТІВ ДЛЯ СТВОРЕННЯ ПРОФІЛЮ ДЕРЖАВНИХ СЛУЖБОВЦІВ

1. Вступ

Технології збору інформації стали невід’ємною частиною діяльності урядів, правоохоронних органів, розвідувальних агенцій, а також підприємств, що намагаються ефективно оцінювати потенційні ризики і приймати обґрунтовані рішення. Одним із таких потужних інструментів є Open Source Intelligence (OSINT), який визначається як дані, отримані шляхом збору, оцінки та аналізу загальнодоступної інформації з відкритих джерел [1]. Особливе місце серед застосувань OSINT займає створення профілю осіб, зокрема державних службовців, що включає аналіз їхньої публічної діяльності, соціальних мереж, професійної кар’єри, контактів та інших доступних даних для оцінки потенційних загроз або корупційних ризиків. Однак використання таких інструментів пов’язане з етичними питаннями щодо конфіденційності та прав особистості.

2. Методологія створення профілю державних службовців

OSINT, або розвідка з відкритих джерел, включає процес збору, аналізу і поширення інформації, яка доступна публічно та відкрита самою особою в публічному просторі, тобто не є засекреченою. Це можуть бути інформаційні ресурси, такі як:

– соціальні мережі (Twitter, Facebook, LinkedIn, Instagram);

– публічні записи (урядові звіти, судові документи, законодавчі акти);

– медіа (новинні портали, блоги, форуми);

– наукові статті, конференції, презентації.

Державні службовці, як публічні особи, залишають велику кількість інформації в доступних джерелах, що може бути використано для побудови їхнього профілю.

Процес створення профілю державного службовця включає кілька етапів:

1. Збір даних: пошук інформації з відкритих джерел, таких як соціальні мережі, профілі на професійних платформах, новини, публікації тощо.

2. Аналіз даних: систематизація і класифікація зібраної інформації для майбутнього використання. Аналіз може охоплювати профіль освіти, кар’єрного шляху, публічних заяв, взаємодії з іншими державними та приватними особами.

3. Визначення ризиків: на основі зібраної інформації можуть бути виявлені потенційні загрози, такі як конфлікти інтересів, зв’язки з корупційними схемами або інші проблеми, що ставлять під загрозу доброчесність службовця.

3. Інструменти OSINT для створення профілю

Для створення профілю державного службовця використовуються різні інструменти збору та аналізу даних. Деякі з них включають [2]:

– Maltego: потужний інструмент для картографування зв’язків між людьми, організаціями та ресурсами;

– Social Media Monitoring Tools: інструменти для моніторингу активності в соціальних мережах (Hootsuite, Brandwatch, Sprout Social);

– Pipl: інструмент для пошуку інформації про людей через інтернет;

– Shodan: інструмент для пошуку інформації про пристрої, підключені до Інтернету, які використовуються для збору даних про особу.

Після збору даних, наступним кроком є їхній аналіз і візуалізація:

– Tableau або Power BI для візуалізації великих обсягів даних і побудови звітів;

– Gephi для візуалізації мережевих зв’язків між особами та організаціями;

– IBM i2 Analyst’s Notebook для складного аналізу і візуалізації зв’язків і даних.

4. Застосування OSINT для виявлення ризиків у діяльності державних службовців

Конфлікт інтересів є серйозною проблемою для державних службовців, адже вони можуть приймати рішення, що впливають на їхні особисті чи бізнесові інтереси. Використання OSINT може допомогти виявити й оцінити ці ризики шляхом аналізу зв’язків державного службовця з приватними компаніями, іншими політиками, членами родини чи іншими впливовими особами.

Вивчення кар’єрного шляху особи та її професійних зв’язків може виявити потенційні конфлікти інтересів. Наприклад, службовець, який працював у приватному секторі в тій самій галузі, де він зараз приймає державні рішення, може бути схильний до впливу цієї галузі.

Дослідження бізнесових зв’язків службовця (наприклад, через відкриті декларації про доходи або перевірку власності) дозволяє виявити можливі конфлікти між його професійними обов’язками та приватними інтересами. Зокрема, за допомогою інструментів для моніторингу корпоративних реєстрів можна виявити участь службовця у приватних компаніях, що може бути підозрілим у випадку, якщо ці компанії виграють тендери чи контракти з державними установами.

Державні службовці можуть мати контакти з представниками бізнесу або політичними діячами, що може бути неприпустимим, якщо ці зв’язки суперечать інтересам держави або порушують принципи доброчесності. OSINT дозволяє виявити такі зв’язки через аналіз публічних профілів у соціальних мережах або в медіа [2].

Збір відкритої інформації допомагає не тільки виявити конфлікти інтересів, але й оцінити потенційні загрози, які можуть виходити від окремих державних службовців. Це включає:

- **зв’язки з корупційними мережами.** Аналізуючи публічну діяльність службовця, можна виявити ознаки його причетності до корупційних схем. Наприклад, якщо службовець часто відвідує зустрічі або заходи, організовані сумнівними компаніями, це може бути індикатором підозрілої діяльності;
- **виявлення зв’язків із міжнародними загрозами.** OSINT дозволяє проводити моніторинг публічної активності службовців за кордоном, що може вказувати на можливі загрози національній безпеці, якщо службовець має підозрілі зв’язки з іноземними урядами, організаціями чи політичними групами.

Стан репутації державного службовця є важливим фактором для оцінки його здатності ефективно виконувати свої обов’язки. Аналіз репутації включає:

- **моніторинг публічних заяв та публікацій.** Процес профілювання включає не лише аналіз особистої кар’єри, а й оцінку публічних заяв службовця, його участь у скандалах, дискусіях чи конфліктних ситуаціях, що можуть вплинути на громадську думку;
- **вивчення медіа та новин.** Збір інформації з новинних порталі й медіа допомагає визначити рівень довіри громадськості до певного державного службовця. Якщо службовець часто потрапляє в заголовки новин у контексті скандалів або негативних публікацій, це вказує на проблеми з його репутацією.

В останні роки Україна активно використовує інструменти OSINT для підвищення прозорості державних органів та виявлення загроз на всіх рівнях державного управління. Два важливі приклади застосування OSINT у національній безпеці і боротьбі з корупцією висвітлюються в публікаціях на офіційних вебресурсах, а саме:

1. Застосування OSINT у діяльності Верховної Ради України

В одній із останніх статей, опублікованих на сайті Верховної Ради України, йдеться про те, як відкриті дані та інструменти OSINT допомагають виявляти корупційні зв’язки та моніторити діяльність публічних осіб. Інформація, доступна у відкритих джерелах, дозволяє значно покращити антикорупційну політику, відслідковувати зміни в активностях держслужбовців та навіть прогнозувати ймовірні ризики для національної безпеки. Це також дає можливість громадськості та медіа більше залучатися до процесів контролю за діяльністю державних органів, підвищуючи рівень прозорості та відповідальності публічних службовців. На практиці це означає, що інформація з відкритих джерел стає важливим інструментом для законодавчого контролю і забезпечення державного нагляду за діяльністю службовців [3].

2. Робота OSINT-агенції “Molfar”

Ще одним важливим прикладом використання OSINT є діяльність агенції “Molfar”, яка займається збором і аналізом відкритих даних із різних джерел для створення аналітики, що має ключове значення для національної безпеки України. Як зазначено в інтерв’ю з засновником агенції Артемом Старосійцем, ця організація активно застосовує передові інструменти OSINT для дослідження інформаційних потоків, виявлення загроз на державному рівні та забезпечення безпеки в умовах гібридної війни. Принцип роботи “Molfar” полягає у поєднанні технологій автоматизації збору даних та експертного аналізу, що дозволяє максимально ефективно виявляти потенційні загрози і надавати оперативну аналітичну підтримку органам державної влади та силовим структурам. Діяльність таких агентств відіграє важливу роль в інформаційній боротьбі, а також у створенні безпечного середовища для громадян [4].

5. Етичні та правові аспекти використання OSINT

Незважаючи на те, що дані, які використовуються для OSINT, є відкритими, їхнє використання має бути етично виправданим і не порушувати права особистості на приватність. Це особливо актуально, коли мова йде про профілювання публічних осіб.

Збір інформації та її використання для створення профілю державних службовців має відповідати законодавству. У різних країнах існують різні закони, що регулюють використання OSINT, і важливо дотримуватись принципів прозорості, добросовісності та законності.

6. Висновки

Використання OSINT для створення профілю державних службовців надає нові можливості для підвищення прозорості та відповідальності в управлінні. Однак це також пов’язано з етичними та правовими викликами, які потребують уваги та ретельного регулювання. Майбутній розвиток інструментів OSINT, а також удосконалення законодавчої бази можуть зробити цей процес більш ефективним і відповідальним.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Gill R. What is OSINT (Open-Source Intelligence?) / SANS Institute. Cyber Security Training // SANS Courses, Certifications & Research. URL: https://www.sans.org/blog/what-is-open-source-intelligence/ (дата звернення: 23.04.2025).

2. Ланде Д. В. OSINT у кібербезпеці: навч. посіб. / Д. В. Ланде. Київ: ТОВ «Інжиніринг», 2024. 522 с. ISBN 978-966-2344-97-4.

3. Навчіться перевіряти інформацію та аналізувати дані за допомогою інструментів OSINT // Комітет з питань цифрової трансформації. Верховна рада України. URL: https://www.rada.gov.ua/news/news_kom/252968.html (дата звернення: 23.04.2025).

4. Кліщук Л. Як працює OSINT-агенція Molfar: інтерв’ю АрміяInform із засновником Артемом Старосєком // АрміяInform – Інформаційне агентство АрміяInform. URL: https://armyinform.com.ua/2024/09/02/yak-praczyuye-osint-agencziya-molfar-intervyu-armiyainform-iz-zasnovnykom-artemom-starosyekom/ (дата звернення: 23.04.2025).

УДК 004.7

канд. техн. наук, ст. наук. співр. **Масесов М. О.** ORCID: 0000-0003-4537-4295 (ВІТІ ім. Героїв Крут)

МОДЕЛЬ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ ПОБУДОВІ ГЕТЕРОГЕННОЇ СИСТЕМИ ЗВ’ЯЗКУ

Активне протиборство у кіберпросторі під час відбиття повномасштабної збройної агресії російської федерації лише підтвердило актуальність та необхідність створення ефективних систем для захисту критично важливої інформації в Україні. Зазначене стосується як органів управління Державою, так і установ (організацій, підприємств, компаній) різних форм власності.

Збройні Сили України, як і інші складові Сил оборони, не є виключенням у наведеній тенденції. Саме тому забезпечення захисту інформації є загальною вимогою при створенні та функціонуванні будь-яких систем сектору безпеки і оборони Держави, в тому числі – системи зв’язку Збройних Сил України.

Систему зв’язку Збройних Сил України слід відносити до критичних систем, порушення безпеки інформації якої може нанести вагому шкоду. Тому одним із ключових питань побудови системи зв’язку є реалізація вимог щодо захисту інформації від несанкціонованого доступу (НСД).

Захист інформації вимагає врахування ряду специфічних особливостей, які додають множину нових можливостей порушення безпеки інформації до існуючих при “ручній” технології побудови системи зв’язку. Для більшості таких критичних систем необхідний індивідуальний підхід до захисту інформації, що обумовлений залежністю можливостей порушення інформаційної безпеки від їх архітектури і режимів роботи, гетерогенністю і слабкою уніфікацією, складністю, різноманітністю носіїв і способів перетворення інформації, необхідністю заміни програмного та апаратного забезпечення внаслідок морального старіння і т. д. Існуюче протиріччя між необхідністю збільшення ефективності процесу побудови системи зв’язку шляхом автоматизації (інформатизації) і збільшенням риску порушення безпеки інформації повинна вирішувати система захисту інформації (СЗІ), що створюється окремо в якості підсистеми забезпечення в процесі планування та побудови системи зв’язку. Тому актуальним завданням є розробка сукупності моделей захисту інформації від НСД, що визначатимуть СЗІ при побудові системи зв’язку.

Із цією метою на підставі аналізу каналів НСД і можливостей використання існуючих методів і засобів захисту інформації запропоновано модель СЗІ при побудові системи зв’язку, відповідно до якої визначено вимоги до СЗІ, проведено декомпозицію СЗІ на функціональні підсистеми.

Відповідно до розробленої моделі, СЗІ повинна включати в себе наступні підсистеми: 1) розмежування доступу (що складається з підсистем дискреційного і мандатного розмежування доступу); 2) виявлення НСД; 3) автентифікації; 4) криптографічний захист; 5) управління. Кожна функціональна підсистема СЗІ, крім системи управління, повинна мати множину структурних компонентів за кількістю АРМ і систем колективного користування (серверів) в розподіленій структурі. Для адміністраторів захисту створюється свій АРМ, що включає всі функціональні підсистеми СЗІ, при чому на АРМ адміністратора повинен створюватися базовий компонент системи виявлення НСД.

Запропонована модель дозволяє представити загальну модель системи захисту інформації частковими моделями підсистем захисту інформації, а також розробити моделі підсистем захисту інформації, реалізація яких у сукупності з комплексом організаційних заходів спроможна забезпечити створення СЗІ, яка реалізує вимоги щодо захисту інформації від НСД.

Прийма О. О. ORCID: 0009-0008-6991-1773 (ВІТІ ім. Героїв Крут)
Бродовський А. П. ORCID: 0009-0006-9118-7465 (ВІТІ ім. Героїв Крут)

ВПЛИВ КВАНТОВИХ ОБЧИСЛЕНЬ НА БЕЗПЕКУ КРИПТОГРАФІЧНИХ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

Генератори псевдовипадкових чисел (ГПВЧ) є фундаментальною складовою сучасних криптографічних систем. Вони забезпечують генерацію ключів і випадкових послідовностей, що безпосередньо впливає на стійкість алгоритмів шифрування. Надійність ГПВЧ базується на складності математичних задач, таких як факторизація цілих чисел або дискретне логарифмування – задач, важкорозв’язуваних для класичних обчислювальних пристроїв. Проте розвиток квантових технологій істотно змінює уявлення про криптографічну безпеку.

Алгоритм Шора [1] є найвідомішим прикладом квантового загрозливого інструмента, здатного ефективно вирішувати задачі, на яких базується безпека RSA та DSA. Теоретично він дозволяє виконати факторизацію великих цілих чисел значно швидше, ніж класичні методи. Для ілюстрації можливих наслідків у майбутньому наведено теоретичні оцінки швидкості у таблиці 1.

Таблиця 1

Таблиця порівняння швидкості факторизації RSA-ключів

Розмір ключа (біт)	*Класичні обчислення*	*Квантові обчислення*
1024	~2,3 × 10^4 років	~5 секунд
2048	~6,4 × 10^17 років	~20 хвилин
3072	~3,4 × 10^32 років	~2 години

Примітка: Наведені значення є гіпотетичними та базуються на симуляціях і теоретичних моделях за умов наявності великомасштабного квантового комп’ютера з тисячами стабільних кубітів. На 2025 рік практичне застосування алгоритму Шора до ключів RSA-2048 залишається недосяжним.

Для симетричних шифрів, як AES, застосовують алгоритм Гровера [2], який знижує складність повного перебору ключа з $O(2^n)$ до $O(2^{\frac{n}{2}})$ завдяки квадратичному прискоренню, характерному для цього квантового алгоритму. Теоретичні оцінки наведено в таблиці 2.

Таблиця 2

Таблиця порівняння складності перебору AES-ключів

Розмір ключа AES (біт)	*Класичні обчислення*	*Квантові обчислення*
128	2^128	2^64
192	2^192	2^96
256	2^256	2^128

Отже, навіть квантовий комп’ютер вимагає експоненційного часу для зламу AES, хоча і в значно меншому обсязі, ніж класичний.

Ці фактори підкреслюють важливість переходу до постквантової криптографії – криптографічних методів, що залишаються стійкими як до класичних, так і до квантових атак. Перспективні підходи базуються на задачах, які не піддаються ефективному квантовому розв’язанню: криптографія на решітках, кодах корекції помилок, багатовимірних поліномах і ізогеніях еліптичних кривих [3; 4].

Наприклад, алгоритм SIKE (Supersingular Isogeny Key Encapsulation) [4] заснований на складності знаходження ізогеній між суперсингулярними еліптичними кривими. Попри початкову перспективність і компактні розміри ключів, у 2022 році він був зламаний класичним методом і виключений із фінального етапу конкурсу NIST.

Національний інститут стандартів і технологій США (NIST) проводить стандартизацію постквантових алгоритмів. На завершення третього раунду конкурсу (2022 рік) було відібрано кілька алгоритмів-кандидатів [3]. Результати наведено в таблиці 3.

Таблиця 3

Таблиця результатів третього раунду конкурсу NIST

Алгоритм-кандидат	*Тип задачі*	*Основа алгоритму*	*Статус*
CRYSTALS-Kyber	Шифрування ключів	Решітки	Фіналіст
CRYSTALS-Dilithium	Цифровий підпис	Решітки	Фіналіст
Falcon	Цифровий підпис	Решітки	Фіналіст
SPHINCS+	Цифровий підпис	Хеш-функції	Фіналіст

Попри квантову стійкість, деякі з них мають обмеження: Falcon – складний у реалізації через високу чутливість до числових похибок, SPHINCS+ – малопридатний для пристроїв із обмеженими ресурсами через великі розміри підписів та низьку швидкодію.

Окрему увагу слід приділити квантовим генераторам випадкових чисел (Quantum Random Number Generators, QRNG). Вони використовують фізичні квантові явища, такі як суперпозиція або шум фотонів, для створення дійсно випадкових чисел, які не залежать від алгоритмічних структур і є недоступними для передбачення навіть за допомогою квантових комп’ютерів [5].

Висновок

Квантові технології стрімко розвиваються, і хоча повноцінна реалізація алгоритмів Шора або Гровера ще залишається теоретичною, вікно для підготовки до криптографічної трансформації звужується. Впровадження квантово-стійких протоколів, участь у глобальних стандартизаційних ініціативах і перехід на QRNG є критично необхідними кроками для захисту інформації у квантову епоху.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Шор П. Алгоритми квантового обчислення дискретного логарифма і факторизації // SIAM J. Computing. Computing. 1997. Т. 26, № 5. С. 1484–1509.

2. Grover L. A fast quantum mechanical algorithm for database search // Proceedings of the 28th Annual ACM Symposium on the Theory of Computing. 1996. P. 212–219.

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

4. Costello C. Supersingular isogeny key exchange for beginners. 2019. URL: https://eprint.iacr.org/2019/050.pdf.

5. IBM Quantum Experience. URL: https://quantum-computing.ibm.com.

6. Qiskit: An Open-source Framework for Quantum Computing. URL: https://qiskit.org.

УДК 629.735.45-519:004.032.26:531.383

д-р філософії **Фесенко О. Д.** ORCID: 0000-0002-2114-5327 (ВІТІ ім. Героїв Крут)

МЕТОД УПРАВЛІННЯ ПОЗИЦІОНУВАННЯМ МІКРО-БпЛА НА ОСНОВІ НЕЙРОМЕРЕЖЕВОЇ АРХІТЕКТУРИ КОЛМОГОРОВА – АРНОЛЬДА

На сьогодні забезпечення точної оцінки орієнтації БпЛА мікрокласу в просторі в умовах невизначеності та під час зникнення сигналів глобальної навігаційної системи є фундаментальною задачею для виконання всієї місії польоту. Традиційні підходи на основі алгоритмів фільтрації навігаційних даних (EKF, Маджвік), які обмежені вимогами до апріорних моделей, обчислювальною складністю та субоптимальністю при впливі нелінійних чи негаусових шумів. Таким чином, пропонується концепція гібридного методу синтезу системи орієнтації та керування мікрокласу БпЛА, що використовує універсальні апроксимаційні властивості нейронних мереж, обґрунтовані теоремою Колмогорова – Арнольда, та переваги кватерніонної алгебри для репрезентації поворотів у групі SO(3).

Теорема Колмогорова – Арнольда (КА), також відома як теорема про суперпозицію, показує, що для апроксимації довільної багатовимірної залежності достатньо одного прихованого рівня нейромережі, що містить $2n + 1$ нейрон (де n – розмірність входу), за умови що нейрони мають довільні монотонні функції активації. У контексті нейронних мереж таке представлення називають колмогоровською структурою мережі. На відміну від класичних багаторівневих архітектур, наприклад, персептрона (MLP), мають фіксовану форму функцій активацій (ReLU, сигмоїда тощо), тому для досягнення потрібної гнучкості відповідно збільшується кількість прихованих рівнів і нейронів.

Сучасні дослідження в галузі нейромережевих структур розвивають ідеї Колмогорова через імплементацію унімерних функцій у міжнейронних зв’язках. Архітектура (КА) пропонує інноваційний підхід до побудови нейромереж, де замість класичних вагових коефіцієнтів використовуються сплайнові функції, що дозволяє досягти підвищеної точності порівняно з традиційними нейромережами.

У контексті задачі оцінки просторової орієнтації БпЛА мікрокласу в умовах невизначеності, цільова функція системи може складатися із двох елементів:

1. Моделювання переходу від поточного стану (q_t, ω_t, a_t) до наступного (q_{t+1}) під впливом керуючого сигналу.

2. Встановлення прямої залежності орієнтації та координат від часу й профілю керування.

Нейромережа архітектури КА може забезпечити адаптивне налаштування функціональних залежностей на основі даних траєкторій, що виключає необхідність ручного конфігурування параметрів фільтрації. Необхідно зазначити, що для ефективної роботи з часовими послідовностями необхідно врахувати динамічну природу системи, оскільки класична колмогоровська мережа апроксимує статичну функцію від набору змінних.

Застосування нейромережевих структур для апроксимації руху квадрокоптера дозволяє ефективно оцінювати орієнтацію і позицію апарата у просторі.

Для кінематики орієнтації у нейромережі необхідно розробити функцію наближеного інтегрування кватерніона $q(t)$, що змінюється під впливом кутової швидкості згідно з рівнянням $\dot{q} = \frac{1}{2} q \otimes$. Мережа обчислює кватерніон на наступному кроці за формулою: $q_{t+\Delta t} = F_\theta(q_t, \omega_t, a_t, m_t)$, де θ – параметри мережі, а $\boldsymbol{a}, \boldsymbol{\omega}, \boldsymbol{m}$ – вимірювання сенсорів. Процес обробки даних акселерометра і магнітометра дозволяє автоматично корегувати дрейф гіроскопа, оскільки мережа навчається розпізнавати невідповідність між вимірюваним вектором прискорення та очікуваним для поточної орієнтації.

Для оцінки траєкторії нейромережа здатна прогнозувати зміну швидкості та позиції на основі прискорень, поточної орієнтації та швидкості. Колмогоровська архітектура забезпечує

теоретичну можливість апроксимації складних залежностей між керуванням, показниками IMU та переміщенням квадрокоптера.

Процес навчання такої мережі можливо здійснювати двома методами: із зовнішнім еталоном (за записаними траєкторіями з відомою орієнтацією) або адаптивно під час польоту (мінімізуючи розбіжність між виміряним та прогнозованим вектором гравітації). Перевагою нейромережевого підходу є можливість врахування нелінійних залежностей, які складно моделювати у традиційних фільтрах Калмана, а мінімальна архітектура зменшує кількість параметрів, покращуючи узагальнюючу здатність.

Висновок. Таким чином, нейромережева архітектура Колмогорова – Арнольда являє собою суттєвий прогрес у вирішенні задачі оцінки орієнтації БпЛА мікрокласу. Заміна стандартних вагових коефіцієнтів на сплайнові функції може забезпечити більш точну апроксимацію нелінійних залежностей, характерних для динаміки БпЛА в умовах невизначеності. Імплементація КА для оцінки орієнтації дозволить підвищити точність прогнозування стану системи при меншій обчислювальній складності.

Запропонований підхід відкриває перспективи для створення адаптивних систем керування БпЛА, що самостійно налаштовуються на характеристики конкретного апарата в реальному часі без необхідності ручного конфігурування параметрів фільтрації.

УДК 004.853

д-р філософії, доцент **Фесьоха В. В.** ORCID: 0000-0001-6612-1970 (ВІТІ ім. Героїв Крут)
Легкобит В. С. ORCID: 0000-0002-9118-4188 (ВІТІ ім. Героїв Крут)

ВАРІАНТ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ УПРАВЛІННЯ ЗНАННЯМИ В ІНТЕЛЕКТУАЛЬНИХ СИСТЕМАХ КІБЕРЗАХИСТУ

Фактична відсутність обмежень на використання передових технологій штучного інтелекту (ШІ) призводить до того, що протиборство в кіберпросторі все більше перетворюється на змагання між оборонним (Defensive AI) та наступальним (Offensive AI) штучними інтелектами. У даному контексті, одним з основних засобів захисту інформації, оборони інформаційно-комунікаційних систем та мереж по периметру є інтелектуальні системи кіберзахисту, в основу функціонування яких покладено методи, моделі та/або алгоритми машинного навчання, глибинного аналізу даних, аналізу багатовимірних структур і поведінкових моделей для прогнозування кібератак, виявлення аномалій, а також адаптивної протидії ще невідомим кібератакам.

Незважаючи на те, що доцільність застосування таких систем досить важко переоцінити, їх ефективність значною мірою залежить від якості навчальних даних і підходів до управління знаннями про кіберзагрози (оперативності оновлення, інтеграції, організації, використання), недостатня увага до яких істотно ускладнює своєчасне здійснення ефективних заходів протидії.

Аналіз публікацій за даною тематикою демонструє перевагу застосування моделей інтелектуальних систем кіберзахисту, архітектура яких передбачає використання формально верифікованого підходу до управління знаннями – забезпечення узгодженості, актуальності та цілісності даних про загрози засобами баз знань, онтологій, семантичних мереж, фреймів, оскільки дає змогу забезпечити прозорість і валідацію процесу прийняття рішень.

На основі викладеного запропоновано варіант підвищення ефективності управління знаннями в інтелектуальних системах кіберзахисту, який базується на використанні human-machine teaming підходу, згідно з яким передбачається оптимізація розподілу ролей в управлінні знаннями: експерти контролюють критичні рішення, тоді як інтегровані функціональні модулі мовних моделей штучного інтелекту прискорюють рутинні процеси отримання та інтеграції даних. У якості форми організації знань обрано онтологію, оскільки її здатність до концептуального відображення історичних знань з можливістю динамічного їх оновлення вдало поєднується зі зрозумілістю моделі знань для людини, що є важливою передумовою для ухвалення обґрунтованих рішень. Функціональне ядро модуля прийняття рішень використовує автоматично згенеровані продукційні Belief Rule Base (BRB) правила, які є розширенням класичних IF–THEN конструкцій, де кожне “THEN” супроводжується векторами ступенів довіри (belief degrees), що дає змогу враховувати неповноту, суперечливість і нечіткість досліджуваних даних. Додатково на онтологію покладено функції конструктора правил, де її концепти та їхні атрибути трансформуються в умови (antecedents), а відношення між ними – в наслідки (consequents). Експертний внесок дає змогу коригувати початкові ступені довіри та додавати контекстно-важливі правила в базу правил. Згенеровані правила додатково оцінюються засобами інструментів пояснювального ШІ (Explainable AI) за низкою метрик (детермінізм, імплементаційна інваріантність, точність імовірнісних оцінок), що підвищує довіру оператора до автоматизованих висновків у системі кіберзахисту, забезпечуючи прозорість та аудит прийнятих рішень.

Таким чином, запропонований варіант підвищення ефективності управління знаннями в інтелектуальних системах кіберзахисту характеризується високим ступенем структурованості, інтерпретованості та актуалізації, передбачає застосування формалізованих, адаптивних та інтероперабельних методів інтеграції нових знань, а також гарантує оперативність, масштабованість і передбачуваність оновлення знань про кіберзагрози.

УДК 004.853

д-р філософії, доцент **Фесьоха В. В.** ORCID: 0000-0001-6612-1970 (ВІТІ ім. Героїв Крут)
Унтілова О. О. ORCID: 0009-0003-8756-1889 (ВІТІ ім. Героїв Крут)

СПОСІБ МІНІМІЗАЦІЇ ХИБНОПОЗИТИВНИХ РЕЗУЛЬТАТІВ ПРИ ВИЯВЛЕННІ АНОМАЛІЙ СИСТЕМАМИ КІБЕРЗАХИСТУ НА ОСНОВІ ТОПОЛОГІЧНОГО АНАЛІЗУ ПОДІЙ

Виявлення аномалій системами кіберзахисту є ключовим процесом у забезпеченні кіберстійкості інформаційно-комунікаційних систем і мереж, оскільки належить до одного з найефективніших підходів щодо виявлення невідомих кібератак. Так, порівняно з прогнозуванням кібератак, біоінспірованим та декларативним підходами, виявлення аномалій має низку переваг:

виявлення нових або модифікованих кібератак без опори на попередні знання;

виявлення підозрілої активності на ранніх етапах (до нанесення шкоди);

можливість застосування до різних систем і мереж без значних змін;

незначна кількість хибнонегативних результатів.

Поряд із цим, такий підхід досить часто характеризується значною кількістю хибнопозитивних спрацьовувань, коли система помилково оцінює звичайну або нормальну поведінку як потенційну деструктивну (шкідливу) активність, що у свою чергу призводить до збільшення навантаження на аналітиків безпеки, значно сповільнює реакцію системи та може спричинити пропуск реальної кібератаки. Основними причинами високого показника хибнопозитивних результатів є висока варіативність нормальної поведінки користувачів і систем, недостатня адаптивність моделей виявлення, а також складність забезпечення чіткої (лінійної) сепарабельності легітимної та шкідливої активності.

Серед існуючих підходів до вирішення даного завдання є: поєднання традиційного (signature-based) і поведінкового (anomaly-based) аналізу, використання моделей машинного навчання на маркованих наборах даних (supervised Learning), напівконтрольованого навчання (semi-supervised Learning), фільтрації на основі контексту, зменшення розмірності простору ознак (dimensionality reduction). Найбільшої уваги заслуговують Risk Scoring Systems і User and Entity Behavior Analytics, функціональне ядро яких ґрунтується на додатковій оцінці загрози виявленої аномалії. Суть оцінки загрози виявленої аномалії полягає у реалізації таких етапів:

виявлення аномалії;

оцінка можливого її деструктивного впливу на основі множини ознак (критичність активів, привілеї користувача);

призначення ваги (коефіцієнту) загрозливості;

фільтрація та пріоритизація.

У зв’язку з цим, запропоновано спосіб мінімізації хибнопозитивних результатів при виявленні аномалій системами кіберзахисту, заснований на топологічній оцінці їхньої потенційної загрозливості. Так, на відміну від традиційного підходу, де кожна аномалія аналізується окремо, передбачено оцінку множини одночасних подій в системі, враховуючи структурну форму їх розподілу в багатовимірному просторі ознак. Засобами основного інструменту топологічного аналізу даних – персистентних гомологій – виявляються стійкі приховані аномальні структури (топологічні об’єкти), зокрема кластерні петлі, розгалуження, діри та переходи, що дає змогу інтерпретувати ступінь їх персистентності як показника потенційної загрози. Наявність топологічної структури з множини (декількох) аномальних подій із високим ступенем достовірності свідчить про цілеспрямовану кібератаку.

Таким чином, запропонований спосіб дає змогу зменшити кількість хибнопозитивних спрацьовувань при виявленні аномалій системами кіберзахисту шляхом врахування не лише відхилення окремих подій від нормальної поведінки, а й їхнього взаємозв’язку та топологічної організації.

УДК 681.35

канд. техн. наук **Хусаінов П. В.** ORCID: 0000-0002-0675-0369 (ВІТІ ім. Героїв Крут)
канд. техн. наук **Штаненко С. С.** ORCID: 0000-0001-9776-4653 (ВІТІ ім. Героїв Крут)

МОДЕЛЬ ПРЕДМЕТНОЇ ОБЛАСТІ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ

Тестування на проникнення (penetration testing) уособлює комплекс заходів оцінки захищеності об’єкта кіберзахисту від кіберзагроз шляхом доведення або заперечення твердження про можливість компрометації системи із застосуванням способів та засобів здійснення демонстраційної кібератаки [1; 2].

Діяльність фахівця з тестування на проникнення характеризується деревом цілей. Дерево цілей є відображенням декомпозиції головної цілі в систему часткових цілей на основі застосування узагальнення та класифікації. Коренева вершина графу такого дерева асоціюється з головною ціллю, вузлові вершини – з проміжними цілями, кінцеві (термінальні) вершини є відображенням первинних (елементарних) цілей. Для структуризації знань в сценаріях класифікації найчастіше застосовуються відношення типу “причина – наслідок”, “ціль – підціль”, “частина – ціле”, “засіб – результат”, “інструмент – дія” і т. д. Під поняттям “узагальнення” розглядається процес здобуття нових знань, які пояснюють і класифікують вже відомі факти предметної області, а також можуть передбачувати нові. Узагальнення передбачає застосування моделей класифікації, формування понять, розпізнавання образів, виявлення закономірностей. Здатність людини до узагальнення є базисом будь-якого наукового дослідження, одержання нових знань.

Лінійно впорядковану послідовність дій людини, спрямовану на досягнення головної цілі, будемо називати траєкторією діяльності. Траєкторія діяльності утворюється сукупністю структурованих казуальних відношень, що визначають просування до головної цілі від первинних (елементарних) через проміжні. Така частково-впорядкована послідовність дій розпочинається від перебування у відомому стані початкової ситуації, подібна казуальному сценарію та може розглядатися у контексті застосування стереотипних знань.

Казуальний сценарій є типовою послідовністю дій (процедур), що підлягає структуризації у формі казуального ланцюжка (сценарію), в якому кожна чергова дія створює умови для здійснення наступної. Сценарій – формалізований опис стандартної послідовності взаємозв’язаних фактів типових ситуацій предметній області, послідовності дій або процедур досягнення цілей, стереотипних знань, таких як *The Unified Kill Chain, Ethical Hacking Methodology*. Сценарій тестування на проникнення уособлює казуальні відношення між тактиками (етапами досягнення тактичних цілей) та відповідними техніками (способами, методами) *Adversarial Tactics, Techniques & Common Knowledge (ATT&CK)* [3–5].

Висновки. Відношення між фактами предметної області тестування на проникнення є семантичною мережею казуальних та структурних відношень між етапами (фазами, кроками) демонстраційної кібератаки. Казуальні відношення відображають існуючу повноту експертних знань про типової послідовності варіантів дій, а структурні відношення визначають взаємозв’язок етапів досягнення тактичних цілей.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. NIST SP 800-115 Technical Guide to Information Security Testing and Assessment.
2. Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж: Постанова Кабінету Міністрів України від 16 травні 2023 року № 497.
3. The Unified Kill Chain. URL: https://www.unifiedkillchain.com.
4. Certified Ethical Hacker. URL: https://cert.eccouncil.org/certified-ethical-hacker.html.
5. Adversarial Tactics, Techniques & Common Knowledge. URL: https://attack.mitre.org.

УДК 004.056

Штонда Р. М. ORCID: 0000-0001-5986-0847 (ВІТІ ім. Героїв Крут)
Паламарчук С. А. ORCID: ORCID: 0000-0001-7483-9165 (ВІТІ ім. Героїв Крут)
Бокій О. В. ORCID: 0009-0006-3459-5665 (ВІТІ ім. Героїв Крут)

ВІЗУАЛІЗАЦІЯ КІБЕРЗАГРОЗ ЯК ІНСТРУМЕНТ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ АНАЛІТИКІВ SECURITY OPERATIONS CENTER

Масштабність подій, які відбуваються на сьогодні в кіберпросторі, настільки велика, що аналітики Security Operations Center стикаються з безмежним обсягом даних, а це, своєю чергою, призводить до ускладнення швидкого виявлення кіберзагроз і кіберінцидентів [1]. З огляду на це, візуалізація кіберзагроз стає все більш ефективним інструментом, що дозволяє відобразити дані у зрозумілому та більш доступному вигляді, покращуючи тим самим якість й оперативність прийняття рішень аналітиками Security Operations Center.

Зважаючи на проблему, необхідно дослідити роль візуалізації кіберзагроз під час підтримки прийняття рішень аналітиками Security Operations Center та проаналізувати основні функції, які будуть сприяти ефективній роботі Security Operations Center в умовах виникнення кібератак та кіберінцидентів.

Візуалізація кіберзагроз дозволяє аналітикам Security Operations Center у реальному часі здійснювати оперативний аналіз великих масивів даних, виявляти приховані аномалії, із відображенням аналітичних карт виявлених IP-адрес, геолокацією вебзагроз тощо та приймати швидкі та обґрунтовані рішення в умовах малої кількості часу на реагування.

Ключовими функціями візуалізації кіберзагроз є:

підвищення рівня обізнаності про оперативну обстановку;

виявлення та аналіз кібератак і кіберінцидентів;

пріоритизація кіберзагроз;

координація дій аналітиків всіх рівнів.

Підвищення рівня обізнаності про оперативну обстановку забезпечується за допомогою аналітичних панелей для відображення кіберзагроз у реальному часі (далі – аналітичні панелі) та дозволяє відстежувати загальний стан в інформаційно-комунікаційних системах організацій та установ, відокремлювати зони ризику, відслідковувати активність кіберзагроз.

Під час виявлення та аналізу кібератак і кіберінцидентів за допомогою теплових відображень, часових графіків та поведінкових моделей на аналітичних панелях, візуалізація дає можливість виявити непритаманну активність, що може бути підтвердженням кібератаки чи кіберінциденту.

Кольорове кодування та багаторівневе відображення кіберзагроз та кіберінцидентів на аналітичних панелях дозволить здійснити пріоритизацію кіберзагроз шляхом візуального відстеження найкритичніших подій аналітиками Security Operations Center та зосередити їх увагу саме на них.

Візуальні графічні елементи, що відображаються на аналітичній панелі, покращать координацію дій між аналітиками Security Operations Center всіх рівнів, особливо під час надзвичайних ситуацій.

Враховуючи вищезазначене, можна зробити висновок, що візуалізація кіберзагроз є сучасним і потужним інструментом підтримки прийняття рішень у сфері кібербезпеки. За допомогою неї врази підвищується ефективність роботи аналітиків Security Operations Center, зменшується час реагування на кіберінциденти та приймаються обґрунтовані рішення в умовах, коли відбуваються кібератаки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 2024. Річний звіт. Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. scpc.gov.ua. URL: https://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006 (дата звернення: 17.04.2025).

УДК 681.518.54

Шинкар Є. В. ORCID: 0009-0006-7371-003X (НАСВ імені гетьмана Петра Сагайдачного)
Зварич А. Я. ORCID: 0000-0003-4654-0216 (НАСВ імені гетьмана Петра Сагайдачного)

КОРОТКІ РЕКОМЕНДАЦІЇ ЩОДО ОРГАНІЗАЦІЇ КІБЕРЗАХИСТУ У СТРУКТУРІ БОЙОВИХ ПІДРОЗДІЛІВ ДЛЯ ШВИДКОЇ АДАПТАЦІЇ ВІЙСЬКОВОСЛУЖБОВЦІВ, ЯКІ ПРИБУВАЮТЬ В ЗОНУ ВЕДЕННЯ БОЙОВИХ ДІЙ

Російсько-українська війна показала, що питання захисту в інформаційному середовищі займає одне з ключових місць. Ефективне ведення бойових дій неможливе без швидкого реагування на ситуацію, яка склалась і своєчасного забезпечення необхідними інформаційними ресурсами підрозділів. Кібербезпека є одним із пріоритетів у системі безпеки. Реалізація зазначеного пріоритету здійснюється шляхом посилення спроможностей для протидії кіберзагрозам у сучасному безпековому середовищі. Це досягається забезпеченням надійності та безпеки цифрових послуг із моменту створення та протягом усього їхнього життєвого циклу. Аналіз показує достатньо високий рівень застосування в Збройних Силах України сучасних інформаційних технологій і систем, проте не всі військовослужбовці знають правила кібергігієни. Потрібно запровадження навчальних програм підготовки та проведення практичних навчань у сфері кібербезпеки. Тому до розгляду пропонуються короткі рекомендації, які доступно пояснюють, що потрібно робити і які виконувати заходи, та допоможуть швидко адаптуватися військовослужбовцям, які прибувають в зону ведення бойових дій для запобігання кіберінцидентам.

Відповідно до керівних документів існують правила щодо забезпечення кіберзахисту:

– всі мобільні пристрої та інші електронні пристрої на пункті управління, в розташуваннях повинні бути з вимкненою геолокацією, в режимі польоту та налаштовані відповідно до вимог;

– обов’язковим налаштуванням є подвійна автентифікація на месенджерах WhatsApp, Signal, Trima для запобіганню викрадення чи компроментації акаунтів;

– потрібно здійснювати постійний моніторинг створених робочих груп в месенджерах, шляхом перевірки користувачів;

– вводиться заборона на особисті мобільні пристрої, у визначених зонах використовуються спеціально налаштовані пристрої;

– обов’язкове встановлення антивірусного програмного забезпечення з актуальними базами оновлення на всіх пристроях і робочих місцях (навіть на особистих, якщо вони використовуються в робочих цілях);

– на пристроях, які знаходяться в мережі Інтернет, антивірусне програмне забезпечення зав’язується на консоль керування кіберцентру, залежно від регіону;

– обов’язковим в налаштуваннях є контроль пристроїв, які підключаються, а саме: контроль флеш-носіїв, підключення блютуз-пристроїв, модемів, портативних пристроїв та пристроїв зображення тощо;

– не стежити за всіма подіями, потрібно відключити всі непотрібні групи в месенджерах;

– велика кількість оповіщень від різних джерел, не переходити за посиланнями, які приходять від невідомих джерел;

– обов’язковим є розмежування доступу в локальних мережах, дозвіл на підключення здійснюється за mac-адресами.

Інциденти в кіберпросторі опрацьовуються за допомогою спеціалістів кіберцентрів. Реагування відбувається в найкоротші терміни, згідно із затвердженим алгоритмом дій.