**НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ**

**ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ ІМ. Г.Є. ПУХОВА**


# НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ «КІБЕРБЕЗПЕКА ЕНЕРГЕТИКИ»

**Матеріали**

**29 травня 2024 року**

Київ – 2024

УДК [621.3+620.9]::[004[056.53+42+94] + 504.06]
ББК 31
Б-39

Рекомендовано до друку Вченою радою Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України (протокол № 06 від 30 травня 2024 р.)

Б-39 **Кібербезпека енергетики,** науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України : матеріали, 29 травня 2024 р. Київ : ІПМЕ ім. Г.Є.Пухова НАН України, 2024. 121 с.

В-39 **Cybersecurity of energy**, scientific-practical conference of the G.E. Pukhov Institute for Modeling in Energy Engineering National Academy of Sciences of Ukraine : materials, May 29, 2024. Kyiv: PIMEE NAS of Ukraine, 2024. 121 p.

## *ОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ*

Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України
(м. Київ)

## *ПРОГРАМНИЙ КОМІТЕТ*

**Мохор Володимир Володимирович**
член-кореспондент НАН України, доктор технічних наук, професор,
**директор Інституту, голова програмного комітету**

**Чемерис Олександр Анатолійович**
доктор технічних наук, старший науковий співробітник
заступник директора з наукової роботи

**Чьочь Вікторія Володимирівна**
кандидат технічних наук,
заступник директора з науково-технічної роботи

**Артемчук Володимир Олександрвич**
доктор технічних наук, старший науковий співробітник
заступник директора з науково-організаційної роботи

## *ОРГАНІЗАЦІЙНИЙКОМІТЕТ*

**Артемчук Володимир Олександрвич**
доктор технічних наук, старший науковий співробітник
заступник директора з науково-організаційної роботи

**Клименко Тетяна Михайлівна**
Завідувачка науково-організаційного відділу

**Цуркан Оксана Володимирівна**
молодший науковий співробітник

A.V. Boychenko, V.R. Senchenko

# AN APPROACH TO DEVELOPMENT OF CYBERATTACK SCENARIOS FOR DIGITAL SUBSTATIONS

After the full-scale Russian military invasion of Ukraine in 2022, energy industry security becomes an urgent issue. Meanwhile power grids are gradually abandoning analog control in favor of intelligent digital networks technology. It allows to Ukrainian power industry to burst efficiency of power supply [1]. For this reason, cybersecurity of smart grid substation automation systems are receiving more and more attention [2, 3].

IEC 61850 "Communication networks and systems for power utility automation" is an international standard defining communication protocols for intelligent electronic devices at electrical substations. [4]. It was adopted as national standards of Ukraine [5, 6].

IEC 61850 uses SCL (System Configuration description Language), which is based on the XML markup language to configurate intellectual electrical devices (IEDs) and smart grid substations. SCL defines several file formats: ICD (IED Capability Description), CID (Configured IED Description), SSD (System Specification Description), SED (System Exchange Description) and SCD (Substation Configuration Description).

Figure 1 shows a fragment of a digital substation data model using the SCL language

| | Detail |
|---|---|
| COM Communication | |
| SVR IED ServerIED - C1 | Сервер 1 |
| AP AccessPoint - TemplateAP1 | Точка доступу 1 |
| SVR Server | |
| LD LDevice - LD1 | ІЕП 1 |
| LN0 LN0 - LLN0 | Вузол 1.1 |
| LN LN - LPHD0 | Інформація про фізичний пристрій |
| LN LN - ARCO0 | Вузол контролю 2 |
| SVR IED ServerIED - C2 | Север 2 |
| AP AccessPoint - TemplateAP1 | Точка доступу 1 |
| SVR Server | |
| LD LDevice - LDevice2 | ІЕП 2 |
| LN0 LN0 - LLN0 | Вузол 2.1 |
| LN LN - 2SOPM0 | Вузол контролю 2 |
| LN LN - ANCR0 | Вузол регулювання 2 |

Figure 1 – Displaying the structure of the .SCD file in the ICD Designer program

In work [7] we proposed an approach to modeling scenarios using knowledge-oriented technology using the Neo4j graph database. This technology includes, in particular, mechanisms for forming graph models from data contained in XML files.

SCD (Substation Configuration Description) file encompasses the complete configuration of the substation, integrating all individual device configurations and their interactions, while the other formats (ICD, CID, SSD, and SED) focus on specific aspects or components within the substation automation system. Therefore,

we used to extract information about the configuration of the substation automation system, including all IEDs, their connections and settings.

This allows you to get a graphical representation of the complete configuration of the substation in the Neo4j database with an SCD file as an input. then, using Cypher queries, you can simulate a cyber-attack scenario.

Figure 2 shows a part of the graph of the elements of the network of digital substations, where "IEP 1" and "IEP 2" are intelligent electronic devices (IED), "PM 1" and "PM 2" are subnets, "TD 1" and "TD 2" – access points, “Sv 1” and “Sv 2” – servers, “LP 1” and “LP 2” – logical devices (LD), “LV 1” and “LV 2” – logical nodes (LN).

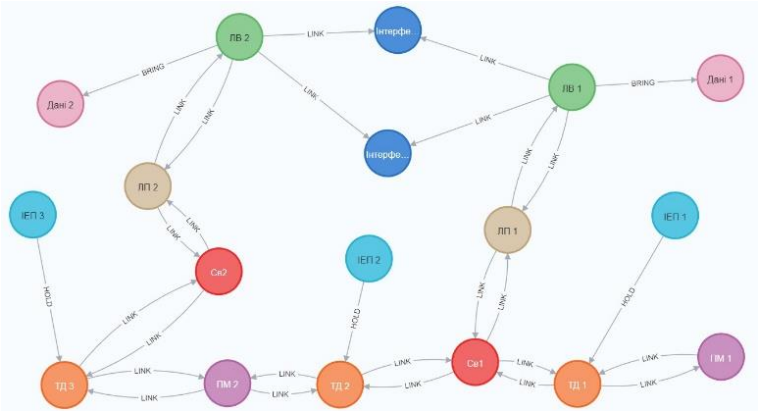



Figure 2 – Rendering part of a digital substation in Neo4j

Suppose the target of a cyberattack is the LN2 control node, and the attacker has access to the PM1 subnet. The following query allows you to check the reachability of this node:

***MATCH p=(a)-[:LINK*]-(c) WHERE a.label='SUBNET1' AND c.label='LN2' RETURN p LIMIT 1***

If the request did not receive results, it means that the attacker has no opportunity to influence the target node. On the other hand if a path between the attack source and the target node is extracted the attack is potentially successful, and the constructed graph (Figure 3) is the attack scenario.

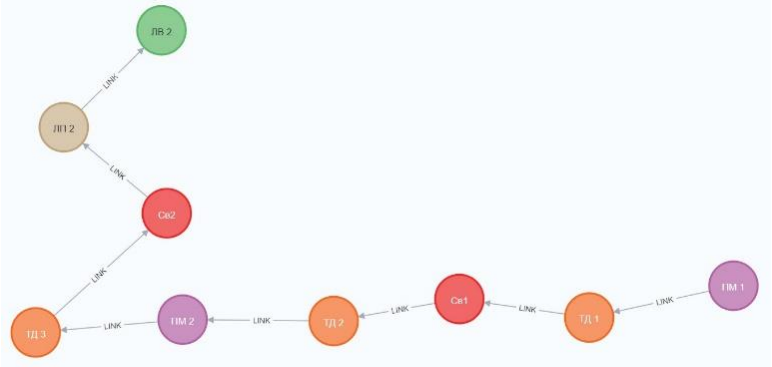



Figure 3 – Cyber-attack scenario in Neo4j

Smart grid resilience and development of new simulation methods for cyber

security analysis are becoming urgent. Building a cyber-attack scenario using the capabilities of a graph database allows to evaluate possible attack paths that attackers may try to penetrate, based on files in SCD format. This will ensure a reduction in the time needed to identify potential threats by building scenarios of attacks on digital substations, and ultimately contribute to strengthening the security of domestic critical infrastructure.

## REFERENCES


1. Кириленко, О. В., Блінов, І. В., Денисюк, С. П., Зайцев, Є. А., & Васильченко, В. І. (2022). Впровадження базових міжнародних стандартів Smart Grid в Україні: сучасний стан справ. Енергетика: економіка, технології, екологія: науковий журнал, 2022,№ 4.
2. Гільгурт, С. Я., Кіслов, О. Г., & Попова, В. М. (2023). Багаторівневі системи виявлення вторгнень для цифрових підстанції Вступ. ББК 31 Б-39, 34.
3. Gaspar, J., Cruz, T., Lam, C. T., & Simões, P. (2023). Smart substation communications and cybersecurity: A comprehensive survey. IEEE Communications Surveys & Tutorials.
4. Communication networks and systems for power utility automation, 2.0. IEC 61850, IEC, 2013.
5. ДСТУ IEC 61850-3:2018 Комунікаційні мережі та системи для автоматизації електроенергетичних підприємств. Частина 3. Загальні технічні вимоги (IEC 61850-3:2013, IDT).
6. ДСТУ EN 61850-6:2022 Комунікаційні мережі та системи для автоматизації електроенергетичних підприємств. Частина 6. Мова опису конфігурації для комунікації інтелектуальних електронних пристроїв на електричних підстанціях (EN 61850-6:2010, IDT; IEC 61850-6:2009, IDT).
7. Додонов, О. Г., Сенченко, В. Р., Путятін, В. Г., Бойченко, А. В., & Коваль, О. В. (2023). Методологічні та технологічні аспекти комп'ютерного моделювання сценаріїв прийняття рішень. Математичні машини і системи, 3, 65-88. DOI: 10.34121/1028-9763-2023-3-65-88.

Г.О. Кравцов

# ЛЮДИНА І ШТУЧНИЙ ІНТЕЛЕКТ В КОНТЕКСТІ УПРАВЛІННН РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

NIST Risk Management Framework (RMF) забезпечує комплексний, гнучкий, повторюваний і вимірний 7-етапний процес, який може використовувати будь-яка організація для управління інформаційною безпекою, а також містить посилання на набір стандартів і рекомендацій NIST для підтримки впровадження програм управління ризиками [1].

29 квітня 2024 року NIST опублікував чернетку публікації AI Risk Management Framework (AI RMF) як розвиток NIST RMF, щоб допомогти керувати ризиками інформаційної безпеки, створеними або посиленими за допомогою генеративного штучного інтелекту (ШІ) [2].

Проект AI RMF Generative AI Profile [3] призваний допомогти організаціям визначити унікальні ризики, пов'язані з генеративним ШІ, і запропонувати дії для управління зазначеними ризиками, які найкраще відповідають їхнім цілям і пріоритетам.

Управління ризиками систем ШІ, призначених для розширення або заміни людської діяльності, наприклад прийняття рішень, потребує певної метрики порівняння. Розробка такої метрики є вкрай складною науково-інженерною проблемою через складність систематизації знань та вмінь людини і ШІ, оскільки системи ШІ виконують різні завдання і виконують їх не так, як люди [3].

Порівнюючи людський інтелект із штучним загальним інтелектом (AGI), слід враховувати кілька ключових показників і характеристик [4]:

1. Швидкість обробки: AGI може обробляти інформацію з неймовірно високою швидкістю, яка часто вимірюється в обчисленнях за секунду. Ця швидкість набагато перевищує швидкість людського мозку, який працює на середній швидкості близько 20-30 Гц.

2. Ємність пам'яті: системи AGI зазвичай мають великий об'єм пам'яті, здатний зберігати та відновлювати великі обсяги даних із точністю. Хоча людська пам'ять вражає, вона обмежена такими факторами, як ємність і швидкість пошуку.

3. Швидкість навчання та адаптивність: AGI може швидко навчатися на величезних масивах даних і швидко адаптуватися до нових ситуацій. Люди можуть ефективно навчатися, але їхній процес навчання часто передбачає поєднання досвіду, освіти та методу проб і помилок, що може бути повільнішим порівняно з AGI.

4. Узагальнення проти спеціалізації: людський інтелект, як правило, перевершує узагальнення, абстрагування та креативність, тоді як AGI спочатку може перевершувати спеціалізовані завдання, але його можна навчити узагальнювати в різних областях.

5. Емоційний інтелект: люди володіють емоційним інтелектом, включаючи емпатію, соціальне розуміння та емоційну регуляцію, яких бракує AGI, якщо вони не запрограмовані явно.

6. Енергоефективність: людський мозок надзвичайно енергоефективний, споживаючи лише близько 20 Вт електроенергії. Системи AGI, особливо великомасштабні, потребують значних обчислювальних ресурсів і потужності, що робить їх менш енергоефективними, ніж біологічні мізки.

7. Сенсорне введення та обробка: Органи чуття людини забезпечують багатий потік інформації в мозок, включаючи зорові, слухові, тактильні, нюхові та смакові дані. AGI може покладатися на різні датчики та джерела даних для введення, але якість і багатство сенсорного досвіду все ще непорівнянні з людським сприйняттям.

8. Креативність та інтуїція: людський інтелект часто включає елементи креативності, інтуїції та суб'єктивного судження, які може бути складно відтворити в AGI. Хоча системи AGI можуть створювати нові рішення та результати, їм може бракувати глибини та нюансів людської творчості.

9. Упередження та етичні міркування: як людський інтелект, так і AGI можуть проявляти упередження, але походження та наслідки цих упереджень відрізняються. Людські упередження часто виникають через культурні, суспільні та когнітивні фактори, тоді як упередження AGI можуть виникати через упереджені навчальні дані або алгоритми. Усунення упередженості в AGI є активною сферою досліджень і розробок.

10. Свідомість і самосвідомість: людський інтелект пов'язаний зі свідомістю і самосвідомістю, що призводить до суб'єктивних переживань і відчуття ідентичності. AGI на поточний момент не володіє свідомістю або самосвідомістю так само, як люди, хоча дискусії щодо потенційної появи цих якостей у AGI тривають.

Аналіз показників порівняння людини і ШІ [4] доводить надзвичайну складіть наукової проблеми розробки адекватної метрики, яка повинна інкапсулювати всі зазначені показники, серед яких є такі, що виглядають як якісні і не піддаються вираженню у цифрах, і бути пригідною для засовування в оцінці ризиків інформаційної безпеки.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. NIST Risk Management Framework | CSRC. NIST Computer Security Resource Center | CSRC. https://csrc.nist.gov/projects/risk-management/about-rmf.
2. Artificial Intelligence Risk Management Framework (AI RMF 1.0) . NIST. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf
3. NIST AI 600-1 «Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile», https://airc.nist.gov/docs/NIST.AI.600-1.GenAI-Profile.ipd.pdf
4. Pogla, M. (2024, 10 лютого). Artificial Intelligence vs Human Intelligence. AutoGPT Official. https://autogpt.net/artificial-intelligence-vs-human-intelligence/

Y. Kotukh

# QUANTUM CRYPTOANALYSIS OF PROSPECTIVE ASYMMETRIC CRYPTOSYSTEMS

Cryptography is a key factor in maintaining the stability of the national economy. It plays a crucial role in ensuring the confidentiality, integrity, and authenticity of information, providing protection against cyber attacks, and meeting regulatory requirements for the security of energy systems [1]. In a world where cyber threats are increasingly complex, the adoption of post-quantum cryptographic methods is essential to ensure the uninterrupted operation of energy infrastructure [2]. The transition to post-quantum standards arises from the development of effective quantum cryptanalysis algorithms, which hold potential applications, including within the energy sector [3].

The security analysis of several widely utilized symmetric ciphers and hash functions, when subject to the potential threat of distributed quantum computers, reveals significant insights. Under scenarios where the cryptographic function is treated as a "black box," a brute force search emerges as the optimal attack strategy against SHA and AES. We successfully calculated the security parameter, execution time, and memory size for each cryptographic primitive. Our attack model hinged on a brute-force approach employing a distributed version of Grover's algorithm, under the assumption of a fault-tolerant architecture. Certain symmetric key algorithms demonstrate vulnerability to "superposition attacks" [4]. Although these attacks are typically impractical in most realistic scenarios, they provide valuable perspectives on the vulnerabilities of specific defense mechanisms. Notably, recent cryptanalysis results [5, 6] have attempted to simplify the compromise of some symmetric algorithms by reducing them to the resolution of a system of nonlinear equations. This reduction enables attacks on the outcomes of solving nonlinear equations using a modified version of the algorithm that addresses quantum linear equations [7]. The effectiveness of these results largely depends on specific conditions within the nonlinear system, which pose challenges in their computation. If the number of conditions is relatively small, an advantage can be achieved over the brute force search performed by grover's algorithm. However, achieving practical results is currently constrained by the absence of sufficiently powerful quantum computers capable of executing such calculations.

Our analysis also extended to the security of asymmetric cryptography, specifically rsa and ecc. Incorporating advancements in fault-tolerant quantum error correction using surface code lattice methods, we calculated the spatiotemporal coordination required to attack each cryptographic scheme, considering physical error rates of $10^3$ and $10^5$ respectively. The study highlighted in paper [8] compared data with a third-degree polynomial, leading to an analytical formula for estimating the number of qubits necessary to breach the cryptographic circuit as a function of time. Table 1 presents a detailed analysis of the total number of physical qubits required to break rsa schemes within 24 hours, including the necessary number of t-gates, the corresponding number of surface code cycles, and the bit rate comparison with classical cryptography.

Table 1 – Results of quantum cryptanalysis of classical algorithms

| Algorithm | A physical footprint | The number of T-gates | Number of cycles | Classic security, bit |
|---|---|---|---|---|
| RSA-1024 | $3.01*10^{7}$ | $3.01*10^{11}$ | $5.86*10^{13}$ | 2TDEA-80 |
| RSA-2048 | $1.72*10^{8}$ | $2.41*10^{12}$ | $4.69*10^{14}$ | 3TDEA-112 |
| RSA-3072 | $6.41*10^{8}$ | $8.12*10^{12}$ | $1.58*10^{15}$ | AES-128 |
| RSA-4096 | $1.18*10^{9}$ | $1.92*10^{13}$ | $3.75*10^{15}$ | AES-156 |
| RSA-7680 | $7.70*10^{10}$ | $1.27*10^{14}$ | $2.64*10^{16}$ | AES-192 |
| RSA-15360 | $4.85*10^{12}$ | $1.01*10^{15}$ | $2.24*10^{17}$ | AES-256 |
| NIST P -160 | $1.81*10^{7}$ | $2.08*10^{11}$ | $4.05*10^{13}$ | 2TDEA-80 |
| NIST P -1 92 | $3.37*10^{7}$ | $3.71*10^{11}$ | $7.23*10^{13}$ | 3TDEA-96 |
| NIST P - 224 | $4.91*10^{7}$ | $5.90*10^{11}$ | $1.15*10^{14}$ | 3TDEA-112 |
| NIST P - 256 | $6.77*10^{7}$ | $8.82*10^{11}$ | $1.72*10^{14}$ | AES-128 |
| NIST P - 384 | $2.27*10^{8}$ | $3.16*10^{12}$ | $6.17*10^{14}$ | AES-192 |
| NIST P - 521 | $6.06*10^{8}$ | $7.92*10^{12}$ | $1.56*10^{15}$ | AES-256 |

The analysis corroborates the findings of [8], specifically that breaking RSA schemes demands a greater quantum resource allocation compared to schemes based on elliptic curves, given an equivalent level of classical security. Recent advancements in fault-tolerant quantum error correction significantly influence the evaluation of the effective strength of cryptographic schemes against quantum attacks. The fault tolerance aspect of quantum computing represents the most resource-intensive phase in the implementation of a quantum algorithm. Although effective quantum cryptanalysis algorithms have not yet been clearly defined for the candidates identified by NIST as finalists in the post-quantum cryptography standards competition, it remains of practical interest to analyze and compare the security of Key Encapsulation Mechanisms (KEMs), asymmetric encryption, and digital signatures against classical security levels, as detailed in Table 2.

Table 2 – Security levels of post-quantum algorithms

| Algorithm | Security level | The size of the public key | The size of the encrypted message | Classic security, bit |
|---|---|---|---|---|
| CRYSTALS-KYBER | Level 1 (AES-128) | 800 | 768 | RSA-3072, ECC-256 |
| CRYSTALS-KYBER | Level 3 (AES-192) | 1184 | 1088 | RSA-7680, ECC-384 |
| CRYSTALS-KYBER | Level 5 (AES-256) | 1568 | 1568 | RSA-15360, ECC-521 |
| NTRU | Level 1 (AES-128) | 699 | 699 | RSA-3072, ECC-256 |

| | | | | |
|---|---|---|---|---|
| NTRU | Level 3 (AES-192) | 930 | 930 | RSA-7680, ECC-384 |
| NTRU | Level 5 (AES-256) | 1230 | 1230 | RSA-15360, ECC-521 |
| SIKE | Level 1 (AES-128) | 330 | 346 | RSA-3072, ECC-256 |
| CRYSTALS-DILITHIUM | Level 1 (AES-128) | 1312 | 2420 | RSA-3072, ECC-256 |
| CRYSTALS-DILITHIUM | Level 3 (AES-192) | 1952 | 3293 | RSA-7680, ECC-384 |
| CRYSTALS-DILITHIUM | Level 5 (AES-256) | 2592 | 4595 | RSA-15360, ECC-521 |
| FALCON | Level 1 (AES-128) | 897 | 690 | RSA-3072, ECC-256 |
| FALCON | Level 5 (AES-256) | 1793 | 1330 | RSA-15360, ECC-521 |
| SPHINCS+ | Level 1 (AES-128) | 32 | 8080 | RSA-3072, ECC-256 |
| SPHINCS+ | Level 3 (AES-192) | 32 | 8080 | RSA-7680, ECC-384 |
| SPHINCS+ | Level 5 (AES-256) | 32 | 8080 | RSA-15360, ECC-521 |

Thus, the analysis of the data presented in the table suggests the need to increase the size of cryptographic keys. The transition to post-quantum cryptography necessitates the use of significantly larger key and ciphertext sizes, particularly for achieving higher levels of security. This requirement is a crucial factor to consider in the design of systems and the specification of application requirements.

## REFERENCES


1. Котух, Є. В. (2020). Основні виклики врядування у сфері кібербезпеки/Є. Котух, В. Ободяк. *Теорія та практика державного управління*, (4), 71.
2. Kotukh , Y. (2019). CYBER SECURITY PROBLEMS IN MODERN WORLD. *Pressing Problems of Public Administration*, (2(56), 33-38. https://doi.org/10.34213/ap.19.02.03.
3. G. Khalimov, O. Sievierinov, S. Khalimova, Y. Kotukh, S. -Y. Chang and Y. Balytskyi, "Encryption Based on the Group of the Hermitian Function Field and Homomorphic Encryption," *2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)*, Kharkiv, Ukraine, 2021, pp. 465-469, doi: 10.1109/PICST54195.2021.9772219.
4. M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia, “Breaking symmetric cryptosystems using quantum period finding,” E-print arXiv:1602.05973 [quant-ph].
5. Y.-A. Chen and X.-S. Gao, “Quantum Algorithms for Boolean Equation Solving and Quantum Algebraic Attack on Cryptosystems,” (2017), arXiv:1712.06239 [quant-ph].
6. Y.-A. Chen, X.-S. Gao, and C.-M. Yuan, “Quantum Algorithms for Optimization and Polynomial Systems Solving over Finite Fields,” (2018), arXiv:1802.03856 [quant-ph]

7. Harrow, A. W., Hassidim, A., & Lloyd, S. (2009). Quantum algorithm for linear systems of equations. *Physical review letters*, *103*(15), 150502.
8. M. Roetteler, M. Naehrig, K. M. Svore, and K. Lauter, “Quantum resource estimates for computing elliptic curves discrete logarithms,” (2017), arXiv:1706.06752 [quant-ph], 1706.06752.

В.В. Зубок, Р.С. Драгунцов, В.Ю. Зубок

# РЕЗИЛЬЄНТНІСТЬ ERP-СИСТЕМ В УМОВАХ ЕНЕРГЕТИЧНОЇ КРИЗИ

**Актуальність.** Впродовж російсько-української війни агресор застосовує атаки на цивільну енергетичну інфраструктуру. Спричинена ними енергетична криза впливає на усі галузі. В рамках завдань забезпечення безперервності бізнес-процесів багато підприємств переглянули ставлення до безпеки чутливих даних накористь їх збереження. Це вплинуло, зокрема, на системи планування ресурсів підприємства (ERP), які є класом інтегрованих інформаційних систем, розроблених для автоматизації та оптимізації управління різними аспектами діяльності підприємства. Ці системи інтегрують фінанси, облік, управління виробництвом та ланцюжками постачання, кадровими ресурсами та іншими процесами. Незамінність ERP-системи для забезпечення безперервності бізнес процесів, а також чутливість даних, які обробляються в них, робить максимально актуальним завдання забезпечення стійкості ERP-систем у світлі зростаючих загроз кібератак і природних лих, а також в умовах мілітарних загроз, спрямованих на руйнування критичної інфраструктури та, як наслідку, проблем з електропостачанням. Збій чи відмова ERP-системи призводить до серйозних втрат для підприємства через порушення виробничих процесів, руйнування ланцюгів постачання та інших втрат.

**Загрози функціонуванню ERP-систем підчас відключень.** Для ERP-систем традиційними є два архітектурні рішення – розгортання системи на власному програмно-апаратному обладнанні підприємства чи «в хмарі». SWOT-аналіз з порівнянням цих двох рішень виконано в [1]. Попри розвиток хмарних рішень, багато компаній використовують локальні (in-premise, або in-house) рішення ERP, оскільки так, на думку власників систем, найкраще зберігається контроль над чутливими даними: дані зберігаються, передаються та обробляються всередині інфраструктури, повний контроль над якою належить підприємству. Але вимоги безперервності бізнесу вимагають перегляду пріоритетів. Втім, розгортання in-premise ставить додаткові завдання забезпечення безпечного функціонування ERP-системи, що включає в себе, зокрема, і завдання з підвищення кіберрезильєнтності [2]:

– забезпечення автономного живлення на сучасних акумуляторних батареях великої ємкості чи та генераторах;
– географічний розподіл основних та резервних серверів для уникнення впливу однієї області на іншу у разі серйозних перебоїв з електропостачанням;
– модифікація процедур відновлення після аварійних ситуацій (disaster recovery) з урахуванням реально досяжних підчас тривалих відключень точки відновлення в часі та точки відновлення в даних;
– встановлення систем моніторингу та управління, які дозволяють віддалено контролювати стан системи та інфраструктури навіть під час

перебоїв з електропостачанням, щоб швидко реагувати на будь-які проблеми та забезпечити оптимальний час відновлення.

Слід зауважити, що широкомасштабні систематичні відключення електропостачання мають істотний вплив на спостережність інформації в інформаційно-комунікаційній системі. Зменшення спостережності інформації призводить до збільшення невизначеності в ситуації та відповідно зумовлює ряд характерних атрибутів таких інцидентів. До таких належать:

– Неповнота отримуваної інформації – в умовах, коли можливість фізичного відключення того чи іншого компоненту інфраструктури та, зокрема, систем безпеки розглядається як високоімовірна в будь-який момент часу, перерва в надсиланні журнальної інформації певним інформаційним активом стає нормальною ситуацією.

– Знижені гарантії достовірності отримуваної інформації – ситуація, коли не вся журнальна інформація надсилається з інформаційного активу до центру керування кібербезпекою зумовлює збільшення толерантності до неповноти отримуваних даних та, відповідно, зменшує рівень довіри співробітників кібербезпеки до отримуваної інформації.

– Розширені можливості порушника безпеки для маніпуляції інформацією, отримуваною командою реагування – враховуючи дві попередні тези, порушник має змогу маніпулювати даними, що надаються для аналізу команді кібербезпеки – вилучаючи певні компоненти та додаючи інакші.

Основну складність в розслідуванні інцидентів кібербезпеки високого рівня ризику та імовірності в умовах масових відключень електропостачання становить різнорідний рівень довіри до інформації, що поступають від компонентів системи та відсутність достатньої прозорості цих компонентів. Для усунення даних складностей можливе використання алгоритму послідовної ізоляції та кластеризованого розслідування активності компонентів системи, що дозволяє здійснити декомпозицію задачі першочергової ізоляції та пріоритизації розслідування інциденту [3].

**Аналіз шляхів пом’якшення ризиків.** Зниженню ризиків, пов’язаних з невизначеністю стану системи через можливе відключення може сприяти розгортання ERP-системи в спеціалізованому приміщенні постачальника послуг центру обробки даних (ЦОД), але на обладнанні власника ERP-системи. Ця послуга ЦОД має назву “colocation” і попит на неї відновився з початком пандемії COVID-19 [4]. Розміщення власних апаратних серверів в ЦОД усуває загрози, пов’язані з хмарною інфраструктурою під стороннім керуванням, залищаючи лише ризики фізичного доступу до обладнання. Втім, ЦОД, які пройшли сертифікацію за Tier Certification [5] чи за ISO/IEC TR 22237 [6], за визначенням забезпечують такий рівень фізичного захисту та енергетичної автономності, досягнення якого індивідуальному власникові ERP-системи коштуватиме значних капіталовкладень, які можуть бути не виправданими з точки зору ризику, якого треба уникнути. Аргументуємо це.

Відповідно до [5] ЦОД оцінюється за чотирма рівнями (tiers) – стандартизованою системою рейтингу, яка вказує на надійність інфраструктури

ЦОД. Вищий рівень означає вищу оцінку. Сертифікується окремо проєкт ЦОД, побудований за проєктом об'єкт, а також операційна сталість (operational sustainability). Найбільш поширеною є сертифікація рівня Tier III. На цьому рівні ЦОД забезпечує резервування (N+1) для всіх основних компонентів, що що дозволяє одночасно проводити, наприклад, планове обслуговування однієї з двох систем, не втрачаючи доступності послуг. Зокрема, резервування N+1 забезпечує:

– не менш ніж два незалежних і повністю резервованих шляхи живлення (1+1). Це означає, що при виході з ладу однієї лінії живлення інша лінія автоматично вмикається, забезпечуючи безперебійне електропостачання;

– наявність резервної системи охолодження, яка забезпечує стабільний температурний режим, запобігає перегріву обладнання та забезпечує оптимальну роботу обчислювальної техніки.

Рівень доступності ЦОД Tier III – не менше 99,982% (приблизно 1,6 години недоступності на рік).

Серія технічних специфікацій ISO/IEC 22237 [6], присвячена проектуванню та оцінці об'єктів центрів обробки даних та інфраструктури. Перший документ із серії представляє та описує чотири класи доступності, за якими можна класифікувати центри обробки даних. Найбільш новий документ серії – частина 31 – представляє прості, але чіткі визначення резильєнтності інфраструктури ЦОД, визначенню рівня резильєнтності на основі доступності, стійкості до відмов, доступності в умовах відмов, частоти відмов, надійності та інших. У всіх серіях 22237 використовується термін «резильєнтність», щоб визначити взаємозв'язок між відмовостійкістю (яка визначається кількістю та побудовою ланцюжків постачання) та доступністю інфраструктури ЦОД.

Отже, з урахуванням особливостей побудови ЦОД, переваги та недоліки компромісного варіанту побудови ERP-системи на власному обладнанні підприємства, розміщеному в ЦОД, з точки зору кіберстійкості можна зобразити так (табл.1). Кількість плюсів є зворотною по відношенню до рівня ризику, пов'язаного з категорією оцінювання (більше плюсів – нижче ризик).

Таблиця 1 – Аналіз переваг та недоліків побудови ERP-системи в ЦОД

| **Категорія оцінювання** | **ЦОД хмара** | **ЦОД colocation** | **In-premise** |
|---|---|---|---|
| Захист чутливих даних | + | +++ | +++++ |
| Енергозабезпечення підчас тривалих відключень | +++++ | +++++ | + |
| Резервування інфраструктури ERP-системи | +++++ | + | + |
| Фізичний захист обладнання | +++ | +++ | +++++ |
| Connectivity | +++++ | +++++ | + |
| Моніторинг систем кіберзахисту | +++++ | +++++ | + |

Проаналізувавши фреймворк інженерії кіберрезильєнтності [2] можна побачити, що кожна з категорій має відношення до завдань кіберрезильєнтності (cyber resiliency objectives). Безумовно, будь-який з поодиноких плюсів може бути розвинутий до кількох плюсів, але це потребуватиме часу та капітальних витрат, а отже - окремого розрахунку та обгрунтування. З іншого боку, така візуалізація характеристик різних архітектур демонструє, що компромісний варіант перенесення обладнання ERP-системи в ЦОД може бути привабливим як завдяки достатньо високому рівню забезпечення конфіденційності чутливих даних підприємства, так і завдяки уникненню ускладнень, пов'язаних з виявленням та реагуванням на інциденти кібербезпеки в умовах масових відключень електропостачання.

**Висновки**. За результатами проведеного аналізу визначено загрози функціонуванню ERP-систем підчас масових довготривалих відключень електроенергії, вплив відключень на ландшафт загроз для таких об'єктів, та запропоновано моделювання зміни ландшафту загроз з переміщення ERP-системи в ЦОД з використанням двох архітектурних рішень – хмарного та colocation.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Зубок В.В. Побудова резильєнтних ERP-систем. XLII Науково-технічна конференція молодих вчених та спеціалістів ІПМЕ ім. Г.Є. Пухова НАН України (присвячена Дню науки в Україні) : Збірник тез конференції (Київ, 15 травня 2024 р).– К.: ІПМЕ ім. Г.Є. Пухова НАН України. – 2024. – С.14-17
2. Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., and McQuaid, R. (2021), NIST Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD. DOI:10.6028/NIST.SP.800-160v2r1
3. В. Ю. Зубок, Р. С. Драгунцов. Особливості розслідування та реагування на інциденти кібербезпеки в умовах масових відключень електропостачання. Безпека енергетики в епоху цифрової трансформації, V наук.-практ. конф. ІПМЕ ім. Г.Є. Пухова НАН України : матеріали, 22 листопада 2023 р. Київ : ІПМЕ ім. Г.Є.Пухова НАН України, 2023. – с.38-44.
4. Cloud services fuels rise of data center colocation in Europe – MissionCritical [online]. URL: https://www.missioncriticalmagazine.com/articles/95049-cloud-services-fuels-rise-of-data-center-colocation-in-europe (accessed 12 May 2024)
5. Tier Certification Overview – Uptime Institute [online]. URL: https://uptimeinstitute.com/tier-certification (accessed 12 May 2024).
   ISO/IEC 22237 Site/Facilities Certification (DCCC) [online]. URL: https://www.epi-ap.com/services/9/31/150/ (accessed 12 May 2024.)

Я.О. Каряка, А.Д. Данилов

# АДАПТАЦІЯ МІЖНАРОДНИХ СТАНДАРТІВ ІСО/ІЕС 27001 У НАЦІОНАЛЬНИХ КОМПАНІЯХ

У сучасному світі, де інформаційна безпека критично важлива для захисту даних, стандарт ІСО/ІЕС 27001 відіграє ключову роль. Ці міжнародні стандарти визначають рамки для систем управління інформаційною безпекою (ISMS). Адаптація цих стандартів у національних компаніях потребує не лише розуміння технічних вимог, а й урахування культурних, економічних та законодавчих особливостей кожної країни.

Метою доповіді є оцінка процесів адаптації міжнародних стандартів ІСО/ІЕС 27001 в українських компаніях, аналіз основних викликів, які виникають під час цього процесу, і визначення переваг, які компанії можуть отримати від їхньої імплементації та сертифікації. Ця доповідь дозволить глибше зрозуміти, як національні реалії впливають на впровадження глобальних стандартів і як можна ефективно подолати ці бар'єри для підвищення загальної інформаційної безпеки.

Процес імплементації міжнародного стандарту ІСО/ІЕС 27001 в національних компаніях можна розділити на кілька ключових етапів, кожен з яких має свої специфічні завдання та виклики:

1 підготовка: першим кроком є розуміння потреб організації та визначення обсягу ISMS. Цей етап включає збір інформації про існуючі процеси безпеки та їх аналіз. Важливо встановити високий рівень залучення керівництва та забезпечити, що вони повністю розуміють вигоди та зобов'язання, пов'язані з сертифікаціє;

2 оцінка ризиків: центральна частина процесу імплементації полягає в оцінці ризиків, які можуть вплинути на інформацію та IT-інфраструктури компанії. Використовуючи методологію оцінки ризиків, визначену в ІСО/ІЕС 27001, компанії повинні ідентифікувати потенційні загрози та вразливі місця, а також впровадити контрольні заходи для їх мінімізації або усунення;

3 розробка політик та процедур: на основі оцінки ризиків, компанія розробляє специфічні політики та процедури управління інформаційною безпекою. Ці документи стають основою для впровадження ISMS і повинні бути чітко зрозумілі та доступні всім співробітникам;

4 навчання та освіта: одним із ключових аспектів успішної імплементації ISMS є навчання персоналу. Всі співробітники повинні бути обізнані про політики та процедури безпеки, що впроваджуються, та розуміти свою роль у забезпеченні інформаційної безпеки;

5 впровадження та експлуатація: після розробки політик і процедур, наступний крок полягає у впровадженні необхідних технологій та процесів. Це може включати оновлення програмного забезпечення, встановлення шифрування даних, впровадження фізичних заходів безпеки та інші технічні рішення;

6 моніторинг та перегляд: імплементація ISMS не закінчується введенням системи в дію. Важливо постійно моніторити і переглядати систему для забезпечення її ефективності. Це включає регулярні аудити, перегляд політик та процедур, а також оновлення заходів контролю згідно з новими загрозами чи вразливостями;

7 сертифікація: останній крок полягає у формальній сертифікації системи згідно ICO/IEC 27001, що включає оцінку зовнішніми аудиторами. Успішна сертифікація підтверджує, що система управління інформаційною безпекою відповідає міжнародним стандартам.

Адаптація міжнародних стандартів, таких як ICO/IEC 27001, в національних компаніях часто супроводжується рядом викликів, які можуть ускладнити процес імплементації. Розглянемо ключові з них:

1 культурні та організаційні бар'єри. В різних країнах існують свої організаційні культури, які можуть впливати на прийняття міжнародних стандартів. Наприклад, в компаніях, де немає культури постійного дотримання формальних процедур, впровадження строгих вимог ICO/IEC 27001 може зустрічати опір з боку співробітників;

2 недостатність ресурсів. Часто компанії стикаються з обмеженими ресурсами, як фінансовими, так і людськими, для належного впровадження та підтримки ISMS. Вкладення в навчання, технології та персонал може бути значним, і не всі компанії готові до таких витрат;

3 технічні труднощі. Інтеграція стандарту ICO/IEC 27001 з існуючими IT-системами може виявитися складною, особливо якщо ці системи застарілі або не сумісні з новими вимогами безпеки. Оновлення та модернізація IT-інфраструктури може вимагати значних зусиль і інвестицій;

4 законодавчі розбіжності. У різних країнах можуть діяти різні закони щодо інформаційної безпеки, які можуть конфліктувати або не повністю корелюватися з вимогами ICO/IEC 27001. Це вимагає додаткової роботи для адаптації стандарту під місцеве законодавство;

5 внутрішній спротив. Співробітники можуть сприймати нові процедури як додаткове навантаження або обмеження їхньої звичної роботи. Побудова спільного розуміння важливості інформаційної безпеки та активне включення персоналу в процес є ключовими для подолання цього виклику;

6 підтримка з боку керівництва. Недостатня підтримка проєкту з боку вищого керівництва може призвести до слабкої імплементації стандарту. Керівництво повинне активно залучатися в процес, встановлюючи приклад та забезпечуючи необхідні ресурси.

Адресація цих викликів вимагає комплексного підходу, який включає стратегічне планування, адаптацію під культурні особливості та вдосконалення внутрішніх комунікацій. Подолання цих бар'єрів не тільки сприяє успішній імплементації ICO/IEC 27001, але й загалом підвищує рівень інформаційної безпеки в компанії.

Сертифікація за стандартом ICO/IEC 27001 пропонує компаніям низку стратегічних переваг, що покращують їхнє управління інформаційною безпекою та зміцнюють їхній імідж на ринку.

Переваги сертифікації за стандартом ICO/IEC 27001:

1 підвищення довіри з боку клієнтів і партнерів: Сертифікація свідчить про відповідність компанії міжнародним стандартам безпеки, що викликає більшу довіру з боку клієнтів і бізнес-партнерів. Це особливо важливо в індустріях, де безпека даних є критичним аспектом, наприклад, у фінансових послугах, охороні здоров'я або електронній комерції;

2 покращення управління ризиками. Стандарт вимагає регулярного перегляду та оцінки інформаційних ризиків, що дозволяє компанії ефективно управляти потенційними загрозами. Реалізація вимог ICO/IEC 27001 допомагає ідентифікувати вразливі місця та запровадити контрольні заходи для їхнього усунення або зменшення;

3 забезпечення відповідності законодавству. Дотримання ICO/IEC 27001 допомагає компаніям відповідати місцевим та міжнародним законодавчим вимогам щодо захисту даних. Це знижує ризик юридичних санкцій та покращує загальну юридичну впевненість компанії;

4 зміцнення репутації компанії. Впровадження і підтвердження дотримання міжнародно визнаного стандарту в області інформаційної безпеки позитивно впливає на імідж компанії. Це може відіграти ключову роль у залученні нових клієнтів та утриманні існуючих;

5 покращення бізнес-процесів. Процес сертифікації часто вимагає від компаній перегляду та оптимізації їхніх бізнес-процесів. Це може призвести до загального підвищення ефективності роботи, зниження витрат і покращення якості послуг;

6 міжнародне визнання. ICO/IEC 27001 є міжнародно визнаним стандартом, що дозволяє компаніям легше входити на нові ринки та співпрацювати з міжнародними партнерами, які також визнають цей стандарт як маркер надійності.

Адаптація та сертифікація за міжнародним стандартом ICO/IEC 27001 мають істотне значення для підвищення рівня інформаційної безпеки у національних компаніях. Цей процес не тільки зміцнює довіру з боку клієнтів та партнерів, але й покращує управління ризиками та допомагає відповідати законодавчим вимогам. Однак, імплементація стандарту супроводжується рядом викликів, таких як культурні та організаційні бар'єри, нестача ресурсів, технічні труднощі, законодавчі розбіжності, внутрішній спротив та потреба в активній підтримці з боку керівництва.

Рекомендації, щодо адаптаціъ міжнародних стандартів ICO/IEC 27001 у національних компаніях:

1 залучення керівництва. Забезпечити активну участь та підтримку вищого керівництва в процесі адаптації та імплементації стандарту, оскільки їхнє залучення критично важливе для успішного впровадження змін;

2 підвищення обізнаності та навчання. Організувати регулярні тренінги та семінари для співробітників з метою підвищення обізнаності про важливість інформаційної безпеки та роль кожного у цьому процесі;

3 ресурсне забезпечення. Виділити достатньо ресурсів для оновлення технічної інфраструктури та забезпечення необхідного фінансування для впровадження необхідних змін у відповідності до вимог ICO/IEC 27001;

4 адаптація під місцеві умови. Гнучко підходити до впровадження стандартів, адаптуючи їх під культурні та законодавчі особливості країни та конкретної організації;

5 постійний моніторинг та оцінка. Встановити систему регулярного моніторингу та оцінки ефективності ISMS для своєчасного виявлення та усунення можливих проблем;

6 міжнародне співробітництво. Налагоджувати співпрацю з міжнародними організаціями та партнерами, що мають досвід у впровадженні ICO/IEC 27001, для обміну знаннями та кращими практиками.

З урахуванням цих рекомендацій компанії зможуть не тільки ефективно впровадити міжнародні стандарти інформаційної безпеки, але й підвищити свою конкурентоспроможність на глобальному ринку, забезпечивши надійний захист важливих даних.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Міжнародна організація стандартизації (ISO). (2013). ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements. Geneva: International Organization for Standardization.
2. Smith, J. (2020). Challenges in Implementing ISO/IEC 27001 in National Companies. Journal of Information Security, 34(2), 112-119.
3. Brown, A., & Davis, E. (2021). Understanding Risk Assessment Practices at Manufacturing Companies: A Collaborative Initiative for the Department of Homeland Security. Boston: WIT Press.
4. Український інститут стандартизації. (2019). Гід по впровадженню систем управління інформаційною безпекою згідно ISO/IEC 27001. Київ: УкрІнСтандарт.
5. Johnson, L. (2019). Cultural and Organizational Impacts on Implementing International Security Standards. International Journal of Information Management, 39, 45-53.
6. Міністерство цифрової трансформації України. (2021). Національна стратегія в сфері кібербезпеки України. Київ.

К.О. Боскін

# СУЧАСНА ПРАКТИКА ПОБУДОВИ ТА СЕРТИФІКАЦІЇ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

В умовах воєнного стану та зміні зовнішніх обставин в контексті російської агресії розробка та впровадження систем управління інформаційною безпекою на об'єктах критичної інфраструктури є важливим завданням, спрямованим на забезпечення цілісного захисту інформаційних ресурсів, які обслуговують енергетичні об'єкти.

Варто дати означення таким термінам як “Система управління безпекою” та “Управління інформаційною безпекою”

Система управління безпекою (СУІБ) – це “та частина системи загальної системи управління організації заснованої на оцінці ризиків для бізнесу, яка створює, реалізує, використовує, виконує функцію моніторингу, перегляд, супровід і вдосконалення інформаційної безпеки” [1] відповідно до міжнародного стандарту в галузі IT ISO/IEC 27001 [2], який описує вимоги до безпеки в інформаційних системах.

Управління інформаційною безпекою – це процес, який повторюється циклічно, що включає важливі етапи і заходи як зі сторони людини так і технічні, в тому числі з обробки даних [3], а саме:

усвідомлення всіма ключовими особами ступеня необхідності захисту інформації та постановку завдань;

збір та аналіз даних про стан інформаційної безпеки в організації; оцінку інформаційних ризиків;

планування заходів з обробки ризиків;

реалізацію та впровадження відповідних механізмів контролю, розподіл ролей і відповідальності, навчання і мотивацію персоналу, оперативну роботу з здійснення заходів захисту;

впровадження систем для моніторингу функціонування механізмів контролю, оцінку їх ефективності та відповідні коригувальні дії.;

Розробка та використання системи управління інформаційною безпекою (СУІБ) здійснюється за допомогою методу, схожого на той, що застосовується до інших управлінських систем. Згідно зі стандартом ISO 27001, підхід до СУІБ включає неперервний цикл заходів, який складається з планування, реалізації, перевірки та дії (ПРПД).

Так само, експлуатація високоспеціалізованих систем в конкретних галузях, таких як енергетика, здійснюється як і інші більш загальні системи управління.

Ефективність інформаційної безпеки можна оцінювати за допомогою різних показників – від кількості заблокованих повідомлень до виконання повідомлення про потенційні системні ризики. Для аналізу ефективності СУІБ можна застосовувати такі показники, як кількість безпекових інцидентів в організації за відведений період часу, кількість повідомлених інцидентів системою управління інформаційною безпекою, оцінені ризики, які були

мінімізовані заходами безпеки, та інше. Це допомагає забезпечити більш глибоке розуміння ситуації для ключових осіб.

Варто відзначити, однією з ключових цілей імплементації СУІБ, крім забезпечення ефективного управління організацією, є отримання сертифікатів, що підтверджують відповідність сучасним стандартам інформаційної безпеки, наприклад ISO2700x. Процес сертифікації включає проведення зовнішнього аудиту корпоративної системи безпеки для перевірки її відповідності до встановлених стандартів. Щоб збільшити шанси на успішний зовнішній аудит, організації часто використовують практику проведення внутрішнього аудиту безпеки перед початком сертифікації. Ефективне зберігання та обробка ключових даних оцінки безпеки в СУІБ може істотно спростити проведення внутрішнього аудиту, а також покращити шанси на успішне проходження зовнішнього аудиту і отримання сертифікату.

Якщо важливі дані зберігаються несистемно і неструктуровані, один із можливих наслідків – це складність у регулюванні доступів до таких файлів через складність їх пошуку та контролю. Такий наслідок може створити безпекові інциденти пов`язані із неправильним контролем доступу до певної інформації і призводити до витоку ключової інформації для широкого кола користувачів або навіть поза організацію.

В сучасному світі актуальним залишається побудова систем у вигляді веб-рішень з використанням API. Таким чином, слід відзначити проект OWASP (Open Web Application Security Project) – відкритий проєкт з безпеки вебзастосунків [4]. OWASP щорічно випускає так званий OWASP TOP 10 – стандартний документ для розробників щодо безпеки веб-додатків [5]. OWASP TOP 10 представляє широкий консенсус щодо найбільш критичних ризиків для безпеки веб-додатків. Він був започаткований у 2003 році, щоб допомогти організаціям і розробникам створити відправну точку для безпечної розробки систем, з роками він перетворився на псевдостандарт, який використовується як маркер якості, а також корисний під час проектування і імплементації систем.

Відповідно до документу видання 2023 року (випускається щорічно у вересні), ключовими вразливостями OWASP API [6] було визнано:

**API1:2023 - Broken Object Level Authorization** – загальне API системи відкриває користувачам із недостатнім рівнем привілеїв кінцеві точки (endpoints), які обробляють ідентифікатори об’єктів, що створює можливість для вектору атак пов`язаних із керуванням доступом на рівні об’єктів. Перевірки авторизації на рівні об’єкта слід враховувати в кожній функції, яка отримує доступ до джерела даних за допомогою ідентифікатора користувача.

**API2:2023 - Broken Authentication** – Механізми автентифікації часто реалізуються неправильно, що дозволяє зловмисникам скомпрометувати токени автентифікації або використовувати недоліки реалізації, щоб тимчасово або назавжди присвоїти ідентифікаційні дані інших користувачів. Порушення здатності системи ідентифікувати клієнта/користувача порушує загальну безпеку API.

**API3:2023 - Broken Object Property Level Authorization** – Ця категорія об’єднує дві раніше представлені у документі 2019 року – API3:2019 Excessive

Data Exposure (Надмірний доступ до даних) та API6:2019 – Mass Assignment (масове перевизначення), зосереджуючись на першопричині: відсутність або неправильна перевірка авторизації на рівні властивості об’єкта. Це призводить до викриття інформації або маніпулювання неавторизованими сторонами.

**Ключовими вразливостями OWASP Web було визнано:**

**A01:2021 - Broken Access Control.** Контроль доступу забезпечує регулювання доступів до інформації таким чином, щоб користувачі не могли діяти поза межами призначених ролей. Збої зазвичай призводять до несанкціонованого розголошення інформації, модифікації, знищення всіх даних або виконання бізнес-функцій недоступних для користувача, враховуючи обмеження.

**A02:2021 - Cryptographic Failures.** Збої пов’язаних із криптографією (або її відсутністю). Часто призводить до розкриття конфіденційних даних. До відомих загальних слабких місць: використання жорстко засписаного пароля в коді, скомпрометований або ризикований криптоалгоритм.

**A03:2021 - Injection.** Програма вразлива до атак, коли:

дані, надані користувачем, не перевіряються, не фільтруються або не очищаються програмою;

динамічні запити або непараметризовані виклики без контекстно-залежного екранування використовуються безпосередньо (нема обробки в коді).

Можливість використання даних в параметрах запиту, з метою пошуку об’єктно-реляційного відображення та схеми бази даних. Як наслідок - отримання додаткових конфіденційних записів.

Повний перелік вразливостей публічно доступний на сайті OWASP.

Отже, під час проектування та побудови СУІБ слід не тільки спиратися на міжнародні стандарти, але також враховувати потенційні загрози, які є переліку OWASP. Таким чином, слід передбачати функціональні можливості моніторингу, повідомлення, а також, автоматизовані компоненти, які би надавали можливість уникати загрози, які є найвідомішими на даний час. Для сертифікування варто спиратися на визнані міжнародні стандарти, такі як ISO 27001.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Комаров, М. Ю., Гончар, С. Ф., & Ониськова, А. В. (2018). Нормативний аспект побудови та впровадження системи управління інформаційною безпекою на об’єктах критичної інфраструктури. Моделювання та інформаційні технології, (82), 40-48.
2. ISO/IEC 27001:2022. Information technology — Security techniques — Information security management systems — Requirements.
3. Комаров, М. Ю., & Гончар, С. Ф. (2017). Методика побудови системи управління інформаційною безпекою на об’єктах критичної інфраструктури. Моделювання та інформаційні технології, (81), 12-19.
4. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. (б. д.). OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. https://owasp.org/.

5. OWASP Top Ten | OWASP Foundation. (б. д.). OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. https://owasp.org/www-project-top-ten/.
6. OWASP Top 10 API Security Risks – 2023 - OWASP API Security Top 10. (б. д.). OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. https://owasp.org/API-Security/editions/2023/en/0x11-t10/.
7. Домарєв, В. В., Домарєв, Д. В., & Гордієнко, С. Б. (2012). Обгрунтування основних функцій системи управління інформаційною безпекою. Вісник Державного університету інформаційно-комунікаційних технологій, (10,№ 2), 102-104.
8. Sharma, P. (2023). A Deep Dive into OWASP Top 3 Security Risks.

В.І. Ботвінчук, А.Д. Данилов

# АНАЛІЗ ОСОБЛИВОСТЕЙ ПОБУДОВИ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Сьогодні інформація стала одним з найцінніших активів для організацій, і її захист є критично важливим. Зі зростанням цифровізації суспільства, використанням Інтернету речей, хмарних технологій та інших сучасних IT-рішень, значно збільшується обсяг даних, що потребують надійного захисту. Кіберзагрози постійно еволюціонують, стаючи все більш складними та небезпечними. Від хакерських атак, вірусів до витончених методів соціальної інженерії — все це створює серйозні ризики для бізнесу. Водночас, регуляторні вимоги до захисту інформації також стають більш жорсткими. Законодавство вимагає від компаній впровадження серйозних заходів безпеки для захисту персональних даних та іншої конфіденційної інформації. Невдачі в захисті інформації можуть призводити до значних економічних втрат, втрати репутації та юридичних наслідків. Тому інвестиції в побудову ефективних систем управління інформаційною безпекою є пріоритетом для багатьох організацій.

З кожним днем зростає усвідомлення необхідності захисту приватності та персональних даних серед користувачів. Розвиток нових технологій, таких як штучний інтелект та машинне навчання, відкриває нові можливості для захисту інформації, але водночас створює нові виклики. Аналіз особливостей побудови систем управління інформаційною безпекою дозволяє краще розуміти ці виклики та розробляти ефективні стратегії для їх подолання, що робить цю тему надзвичайно важливою в умовах швидкоплинного технологічного прогресу.

Системи управління інформаційною безпекою (СУІБ) є комплексними структурами, що включають процеси, технології та людей для захисту інформаційних ресурсів організації. Основні особливості побудови СУІБ можна розглянути в таких аспектах:

1. Визначення цілей та політик безпеки

Цілі безпеки повинні бути визначені на основі бізнес-цілей організації. Вони включають захист конфіденційності (запобігання несанкціонованому доступу до інформації), цілісності (запобігання несанкціонованій зміні інформації) та доступності (забезпечення доступу до інформації для авторизованих користувачів). Цілі безпеки повинні бути конкретними, вимірюваними, досяжними, реалістичними та обмеженими в часі (SMART).

Політики безпеки документують правила, які визначають, як організація захищає свої інформаційні ресурси. Вони включають такі аспекти, як контроль доступу, управління користувачами, управління паролями, захист мережі, шифрування, резервне копіювання, управління інцидентами та відповідальність співробітників за дотримання політик.

2. Ризик-менеджмент

Процес ідентифікації ризиків включає виявлення всіх можливих загроз, які можуть вплинути на інформаційні активи організації. Це можуть бути як

зовнішні загрози (хакерські атаки, природні катастрофи), так і внутрішні (помилки персоналу, внутрішні загрози).

Оцінка ризиків включає визначення ймовірності виникнення загроз та потенційного впливу на організацію. Оцінка може використовувати як кількісні методи (математичні моделі, статистичні дані), так і якісні (експертні оцінки, сценарії).

Управління ризиками передбачає розробку та впровадження заходів для зниження ймовірності та впливу ризиків до прийнятного рівня. Це може включати запобіжні заходи (контроль доступу, фаєрволи), заходи зниження впливу (резервне копіювання, плани відновлення), перенесення ризиків (страхування) та прийняття ризиків (усвідомлене прийняття ризику в разі, якщо він незначний).

3. Організаційна структура та відповідальність

Чітке визначення ролей і обов'язків необхідне для забезпечення відповідальності за інформаційну безпеку. Це включає призначення керівника з інформаційної безпеки (CISO), команд з безпеки, адміністраторів систем та користувачів.

Комітет з інформаційної безпеки координує всі заходи щодо безпеки в організації. Він включає представників різних підрозділів та забезпечує узгодженість політик безпеки з бізнес-цілями організації.

4. Технологічні заходи захисту

Технічні засоби включають фаєрволи, системи виявлення та запобігання вторгнень (IDS/IPS), антивірусне програмне забезпечення, системи управління ідентифікацією та доступом (IAM), системи шифрування даних, захист електронної пошти та інші.

Шифрування захищає дані як при зберіганні (на жорстких дисках, у базах даних), так і при передачі (через мережу). Використання сильних алгоритмів шифрування (AES, RSA) та належне управління ключами є критично важливими для забезпечення захисту даних.

Постійний моніторинг інформаційних систем дозволяє виявляти та реагувати на інциденти безпеки в режимі реального часу. Аудит систем безпеки допомагає перевіряти відповідність політикам безпеки та виявляти потенційні вразливості.

5. Навчання та підвищення обізнаності персоналу

Регулярні тренінги з інформаційної безпеки допомагають співробітникам зрозуміти важливість дотримання політик безпеки, розпізнавати загрози (фішинг, соціальна інженерія) та діяти відповідно до встановлених процедур.

Формування культури безпеки передбачає створення середовища, в якому всі співробітники усвідомлюють свою роль у забезпеченні безпеки та активно дотримуються політик та процедур безпеки.

6. Інцидент-менеджмент

План реагування на інциденти визначає кроки, які необхідно виконати у разі виникнення інциденту безпеки, включаючи виявлення інциденту, оцінку його впливу, повідомлення зацікавлених сторін, усунення наслідків та відновлення нормальної роботи.

Система реєстрації інцидентів дозволяє документувати всі інциденти безпеки для аналізу, покращення процесів та запобігання повторенню.

7. Оцінка та вдосконалення

Регулярний аудит дозволяє оцінювати відповідність системи управління інформаційною безпекою встановленим стандартам та політикам, виявляти недоліки та області для покращення.

На основі результатів аудиту та змін у зовнішньому середовищі постійно вдосконалюються політики, процедури та технічні засоби захисту для забезпечення високого рівня інформаційної безпеки.

8. Відповідність стандартам та законодавству

Відповідність міжнародним стандартам, таким як ISO/IEC 27001, допомагає організації встановити, впровадити, підтримувати та постійно вдосконалювати систему управління інформаційною безпекою. Стандарт визначає вимоги до оцінки та обробки ризиків інформаційної безпеки, а також до впровадження належних заходів безпеки.

Організації повинні дотримуватися національних та міжнародних законодавчих вимог щодо захисту інформації, таких як GDPR (Загальний регламент захисту даних) для Європейського Союзу, HIPAA (Закон про переносимість і підзвітність страхування здоров'я) для США та інших відповідних нормативно-правових актів.

Таким чином, система управління інформаційною безпекою є комплексним механізмом, який вимагає ретельного планування, постійного моніторингу та вдосконалення для забезпечення надійного захисту інформаційних активів організації.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. МЕТОДИ УПРАВЛІННЯ КОРПОРАТИВНОЮ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ. *Головна*. URL: https://economyandsociety.in.ua/index.php/journal/article/view/1732/1675 (дата звернення: 16.05.2024).
2. *Про видання*. URL: https://pag-journal.iei.od.ua/archives/2019/11-2019/35.pdf (дата звернення: 16.05.2024).
3. *Scientific specialized edition "Printing and Publishing". Ukrainian Academy of Printing*. URL: http://pvs.uad.lviv.ua/static/media/2-74/11.pdf (дата звернення: 16.05.2024).

О.А. Владимирський, І.А. Владимирський, Д.М. Семенюк.

# УСУВАННЯ КОРЕЛЬОВАНИХ ЗАВАД З ХАРАКТЕРНОЮ ЗАТРИМКОЮ ПРИ ПОШУКУ ВИТОКІВ

Для підвищення достовірності результатів пошуку витоків у кореляційних течешукачах застосовується статистичне накопичення та усереднення оцінок взаємних кореляційних функцій (ВКФ). Це дозволяє мінімізувати статистичну похибку остаточної оцінки ВКФ, знизити вплив на координату витоку не корельованих, тобто статистично не пов'язаних одина з одною завад у двох сигналах, що обробляються. Однак це не дозволяє усунути так звані корельовані перешкоди (КП).

Ознакою присутності у ВКФ впливу потужної КП часто є характерне положення локального чи глобального максимумів ВКФ вздовж осі затримок.

У практиків зазвичай виникає недовіра до сплеску ВКФ при нульовій або близькій до нуля затримці, – у середині діагностованої ділянки. Це пов'язано з поширеним видом КП, об'єднаних загальною особливістю. Швидкості поширення цих завад значно перевищують швидкість поширення корисних акустичних сигналів у трубопроводі, що призводить до появи відповідного максимуму кореляції при малих затримках між сигналами, що корелюються приладом.

Іншими характерними точками є місця встановлення датчиків. Незважаючи на відсутність у цих місцях витоку (інакше її не потрібно довго шукати) їх координатам може відповідати максимум ВКФ, викликаний присутністю на сусідній ділянці трубопроводу потужного джерела вібросигналів, наприклад, працюючої компресорної установки чи протікаючого сальникового компенсатора. При цьому величина затримки між оброблюваними сигналами близька до часу поширення одного з них крізь всю ділянку трубопроводу між двома датчиками. Начебто джерело цих сигналів знаходиться біля датчика, ближчого до джерела завади. Крім того, іноді максимуми ВКФ внаслідок КП можуть відповідати джерелам реальних шумів у межах секції трубопроводу, що діагностується. Їх координати часто відомі, наприклад відгалуження трубопроводів з потужними відборами, звуження на трубопроводах з великою витратою.

Проблема полягає в тому, що на тлі максимумів ВКФ, викликаних потужними КП, кореляційні піки шуканих витоків виявляються невиразними. Штучне посилення ВКФ (наприклад з "обрізанням" зверху найбільших завадових екстремумів) зазвичай не призводить до виявлення витоку внаслідок багатьох бічних завадових сплесків ВКФ, породжених КП.

Ефективним інструментом усунення КП є частотна фільтрація. Щоб сформулювати методику частотного усування цих перешкод, представимо ВКФ як вектор $\mathbf{r}$ [1]

$$\mathbf{r} = \mathbf{r}_{ss} + \mathbf{r}_{s\alpha} + \mathbf{r}_{\gamma s} + \mathbf{r}_{\alpha\gamma}, \qquad (1)$$

де $\mathbf{r}_{ss}$ - вектор ВКФ шумів витоку; $\mathbf{r}_{\gamma s}$ і $\mathbf{r}_{s\alpha}$ - вектори ВКФ сигналів і адитивних завад; $\mathbf{r}_{\alpha\gamma}$ - вектор ВКФ завад.

Оскільки шуми витоку і завад у даному випадку статистичне не пов'язані, (1) можно записать в виді

$$\mathbf{r} \approx \mathbf{r}_{ss} + \mathbf{r}_{\alpha\gamma},$$

причому $\mathbf{r}_{\alpha\gamma}$ відповідає інтервал $[\tau_1..\tau_2]$ найбільшої кореляції.

У тих випадках, коли розподіл основної частини спектральної щільності потужності завади або витоку відомий, можна синтезувати відповідні селективні фільтри для підвищення відношення сигнал-завада. Однак часто подібна інформація відсутня. Усунути або суттєво зменшити вплив КП на приладову оцінку ВКФ у таких випадках можна в такий спосіб. Представимо $\mathbf{r}$ у вигляді

$$\mathbf{r} \approx \mathbf{\Theta A}, \qquad (2)$$

де $\mathbf{A}$ – вектор-стовпець коефіцієнтів передачі вузькосмугових цифрових фільтрів (ВЦФ) , $\mathbf{\Theta} = (\mathbf{\Theta}(0), \mathbf{\Theta}(1),..., \mathbf{\Theta}(M-1))$ - матриця розміром $M \times N$, $\mathbf{\Theta}(i)$ - вектор-стовпець результату лінійної фільтрації ВКФ ВЦФ з *i*-тою резонансною частотою. Причому $\mathbf{\Theta}(i)$ для всіх $i \in [0..M-1]$ є нормованими

$$\|\Theta(i)\|^2 = 1, \qquad \mathbf{\Theta}(i) = \begin{pmatrix} \Theta(0,i) \\ \Theta(1,i) \\ \vdots \\ \Theta(N-1,i) \end{pmatrix}, \qquad [\tau_1..\tau_2] \in [0..N-1] \ .$$

де символом $\| \|$ позначається евклідова норма.

Визначимо $\{\mathbf{\Theta}(j)\} \in \{\mathbf{\Theta}(i)\}$ для всіх $i \in [0..M-1]$ на підставі умови $\Theta(l, j) = \max\{\Theta(m, j)\}$ для всіх $m \in [0..N-1]$ при $l \in [\tau_1..\tau_2]$. Для кожного $\mathbf{\Theta}(j)$ знайдемо його показник екстремальності

$$Q(j) = \frac{\Theta(l, j)}{f(\mathbf{\Theta}(j))},$$

де $f$ - деяка функція, наприклад $f(\mathbf{\Theta}(j)) = \|\mathbf{\Theta}(j)\|$.

У реальній обстановці частотні діапазони, які займають $\mathbf{r}_{ss}$ і $\mathbf{r}_{\alpha\gamma}$, перекривають один одного. Тому на форму $\mathbf{\Theta}(j)$ різною мірою впливають як $\mathbf{r}_{ss}$ так і $\mathbf{r}_{\alpha\gamma}$. Однак, оскільки максимум $\mathbf{\Theta}(j)$ знаходиться в інтервалі кореляції завади, то відповідний параметр екстремальності $Q(j)$ характеризує ступінь її впливу на форму $\mathbf{\Theta}(j)$. Таким чином, обнуляючи коефіцієнти передачі (2) при $\{\mathbf{\Theta}(j)\}$ з найбільшими показниками екстремальності в області $[\tau_1..\tau_2]$, можна зменшити вплив $\mathbf{r}_{\alpha\gamma}$ на $\mathbf{r}$ до прийнятного рівня. Даний рівень можна визначити адаптивно шляхом визначення

$$\frac{1}{N - \tau_2 + \tau_1 - 1}\left[\sum_{i=0}^{\tau_1 - 1} |r_m(i)| + \sum_{i=\tau_2+1}^{N-1} |r_m(i)|\right]$$

де $r_m(i)$- елементи вектора **r** після m-того обнулення.

**Висновок.** Одною з характерних рис різноманітності акустичної обстановки при пошуку витоків у міських мережах водо та теплопостачання населення є випадки з потужними акустичними завадами. Часто, тимчасово, джерела цих завад вдається відключити. Але не завжди. Це трапляється не тільки внаслідок зносу обладнання – засувок, компенсаторів, повітряників тощо. Не можливо,

наприклад, відключити шумний насос, якщо саме він забезпечує необхідний для пошуку витоку тиск у трубопроводі. У таких та подібних їм випадках запропонований спосіб надає додаткові можливості для точного визначення місць витоків.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Владимирский А.А., Владимирский И.А. О некоторых способах подавления коррелированных помех при поиске утечек. Зб. наук. праць. ІПМЕ НАНУ., Черкаси, 1998. Вип. 6. С.73-76.

С.Я. Гільгурт

# ОГЛЯД МОЖЛИВОСТЕЙ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ КІБЕРЗАХИСТУ ЦИФРОВИХ ПІДСТАНЦІЙ

Електричні підстанції є одними з найчисленніших об'єктів енергетики та відіграють вирішальну роль у всій енергосистемі, виконуючі важливі функції з розподілу та перетворення енергії. Складнощі, що виникають під час цифрової трансформації їх обладнання, пов'язані в першу чергу зі стандартизацією. Якщо життєвий цикл силового обладнання, такого як трансформатори, комутаційні апаратні роз'єднувачі тощо складає близько 40 років, то керуючі системи оновлюються в середньому втричі швидше. В результаті змушені спільно взаємодіяти пристрої декількох поколінь, не сумісні між собою.

Для вирішення цих проблем під час побудові електричних цифрових підстанцій (ЦПС) було розроблено стандарт МЕК 61850 "Мережі та системи зв'язку на підстанціях" [1]. Головне призначення стандарту – створити єдині специфікації, які дозволили б, з одного боку, захистити фінансові вкладення в енергетичне обладнання, з іншого – використовувати передові обчислювальні та мережеві технології. Відповідно до стандарту МЕК 61850 система автоматизації інформаційного обміну на енергооб'єкті за схемою ЦПС складається з трьох рівнів: станційний (Station Level) – найвищій рівень, рівень приєднання (Bay Level) та рівень процесу (Process Level) або "польовий" (Field Level) – найнижчий рівень. Кожен рівень виконує притаманні йому функції, за які відповідають певні типи пристроїв. Комунікації можливі як всередині рівнів (горизонтальні), так і між рівнями (вертикальні).

Але забезпечення сумісності обладнання різних рівнів не є єдиною проблемою ЦПС. Разом з перевагами цифрові технології привносять в роботу систем автоматики підвищення рівня кібернетичної небезпеки [2]. Покращити кіберзахист систем управління технологічними процесами енергетики в умовах цифровізації, в тому числі – в ЦПС, можливо шляхом дослідження та застосування сучасних досягнень технологій штучного інтелекту (ШІ), таких як smart-технології на основі машинного навчання, нейронні мережі, глибоке навчання, методи обробки великих даних тощо.

В даному дослідженні проведено аналіз сучасних технологій ШІ, які можуть бути використані для підвищення рівня кіберзахищеності систем автоматизованого управління технологічними процесами (АСУ ТП) та промислової автоматики, в тому числі – цифрових підстанцій. Головна увага при цьому приділяється таким засобам кібербезпеки, як мережеві системи виявлення/запобігання вторгнень (МСВВ/МСЗВ) [3].

Розглянемо спочатку основні загрози кібербезпеки інформаційним мережам цифровізованих промислових підприємств. В табл. 1 зведено типи потенційних загроз, описи наслідків (інцидентів), до яких вони можуть призвести, а також приклади відомих розробок шкідливого програмного забезпечення, здатного вказані загрози здійснювати [4].

Таблиця 1 – Можливі інциденти в промислових мережах

| Тип загрози | Потенційні інциденти | Приклади шкідливих програм |
|---|---|---|
| Зміни в системі управління | Придушення тривог.<br>Зміна поведінки процесів з непередбачуваними результатами. | Stuxnet, Black Energy, Crashoverrride |
| Зміни програмованої логіки | Пошкодження обладнання.<br>Зупинка технологічних процесів. | Stuxnet, Black Energy, Crashoverrride |
| Дезінформація операторів | Неадекватні дії операторів. | Shamoon, NotPetya |
| Фальсифікація системи керування або безпеки | Придушення засобів захисту та протиаварійних систем з непередбачуваними наслідками. | Triton |
| Зараження шкідливим програмним забезпеченням або DDoS-атаки | Вимушене переведення активів у автономний режим для криміналістичного аналізу.<br>Перехоплення керування з метою пошкодження системних файлів або компрометування системи.<br>Несанкціонований доступ до системних та мережевих ресурсів. | Night Dragon, Duqu/Flame/Gauss, Dragonfly, Dragonfly 2.0 |
| Крадіжка інформації | Несанкціонований доступ до конфіденційної інформації, наприклад, комерційної таємниці. | Night Dragon, Duqu/Flame/Gauss, Dragonfly, Dragonfly 2.0 |
| Зміна інформації | Викривлення значень важливих технологічних параметрів, конфігурацій, декалібрування датчиків. | Shamoon, NotPetya |

Для протидії згаданим загрозам застосовуються різні підходи, в тому числі такі, що використовують досягнення технологій ШІ. Розглянемо, які з них найчастіше застосовують для створення засобів кіберзахисту АСУ ТП, насамперед – інформаційних мереж промислових підприємств [5-9].

Сигнатурний підхід

Виявляє атаки, порівнюючи заздалегідь зібрану інформацію з ознаками атаки, наприклад, шляхом відшукування конкретних патернів в мережевих пакетах. Підходить для високоперіодичних мереж. Не виявляє принципово нові типи атак.

На основі знань

Використовує знання про конкретні атаки, щоб ідентифікувати відповідні загрози. Реалізується на основі правил, на основі логіки тощо. Базується на даних спостереження за набором попередньо визначених правил.

На основі статистики (частково контрольований)

Використовує тести логічного виведення для перевірки відповідності даних певній статистичній моделі мережевого трафіку, яка характеризує стохастичну поведінку мережі.

На основі аномалій (частково контрольований)

Аналізує поточний стан системи на відхилення поведінки від нормального стану, опис якого згенеровано заздалегідь, від такого, що виникає внаслідок вторгнення. Нормальний трафік використовується для навчання моделі ідентифікації штатного режиму. Профілі трафіку створюються за допомогою системних індикаторів, таких як завантаження процесора, помилки входу тощо з прив'язкою до часу доби та дня тижня. Повідомлення генерується коли поточні дані про трафік не відповідають заданим показникам.

На основі контрольованого машинного навчання

Створює математичні моделі, які навчаються та вдосконалюються з часом, щоб виявляти вторгнення. Може використовувати нейронні мережі або статистичні моделі (класифікація, кластеризація). Використовує встановлену модель для перевірки шаблонів на основі даних, зібраних раніше в процесі навчання. Зазвичай застосовує методи класифікації.

На основі неконтрольованого машинного навчання

Не потребує навчальних даних. Зазвичай використовують статистичні методи, такі як кластеризація.

Подальший аналіз інформаційних джерел дозволив виокремити з розглянутих класів підходів на основі ШІ напрями та конкретні технічні рішення, які виглядають більш прийнятними для застосування саме на ЦПС. Розглянемо нижче типові приклади реалізації засобів кіберзахисту відповідно до деяких зі згаданих підходів і не тільки.

В роботі [10] в якості типового прикладу реалізації ***сигнатурного підходу*** розроблено МСВВ із збереженням стану для мереж систем збору даних та диспетчерського управління (SCADA-систем – від англ. Supervisory Control And Data Acquisition) IEC 60870-5-104. Протокол IEC/104 моделюється як детермінований скінченний автомат. Доповнення системи методом білого списку дозволяє виявляти також невідомі атаки. Існують також реалізації МСВВ згідно даного підходу, які побудовані на основі правил для мереж SCADA-систем з використанням протоколу IEC 60870-5-104. Подібна розробка [11] використовує сигнатурний метод для виявлення зловживань та методи на основі моделі для опису очікуваної поведінки.

З метою пом'якшення головного недоліку сигнатурного аналізу – здатності запобігати лише вторгненням, для яких існує фіксований статичний опис – розробники використовують гнучке розпізнавання патернів, яке базується на використанні апарату регулярних виразів. В розробці [12] програмований пристрій на базі ПЛІС з використанням цього апарату реалізує модифікацію розширеної версії алгоритму Домёлкі–Бейза-Ятса–Гоннета для виявлення атак на протокол повідомлень GOOSE (Generic Object Oriented Substation Events), що використовується в ЦПС за стандартом МЕК 61850 для виконання критичних по часу операцій.

В роботі [13] згідно ***статистичного підходу*** розроблено метод виявлення аномалій для двох основних протоколів стандарту МЕК 61850: GOOSE і MMS (Manufacturing Message Specification). На етапі препроцесинга мережеві пакети фільтруються, релевантна інформація витягується та об’єднується з інформацією з пов’язаних пакетів для створення інформаційних потоків. Також

створюються набори даних на основі трафіку, які дозволяють виявляти DDOS-атаки, спостерігаючи за швидкістю передачі. Для тренування нормальної поведінки використовується алгоритм ***Support Vector Machine (SVM)***. Під час моніторингу MMS- і GOOSE-пакети з файлів журналу порівнюються з вивченою моделлю SVM і додаються до навчального набору даних для покращення моделі. В роботі [14] для опису аномалій розглядаються чотири параметри: спроби атак, зміни у файловій системі, зміни в конфігурації цільової системи та зміни стану системи в цільовій системі. За допомогою цих чотирьох атрибутів можна виявити зловмисну поведінку на всіх рівнях ЦПС та створити "відбиток" цієї поведінки. В роботі [15] використано метод виявлення аномалій, заснований на аналізі мережевих потоків даних, інформація з яких збирається з періодичними інтервалами, щоб постійно генерувати моделі та використовувати ці моделі для виявлення аномалій.

В якості прикладу реалізації підходу на основі ***машинного навчання*** можна навести розробку [16]. Моделі, що створюються для характеристики прийнятної поведінки SCADA-системи і дозволяють виявляти атаки, що призводять до відхилення поведінки, базуються на правилах MCBB Snort. Недоліком такого рішення є той факт, що побудовані на TCP-пакетах правила здатні виявляти лише відхилення від очікуваного шаблону зв’язку. Якщо зловмисник згенерує схожий шаблон зв’язку, атака може бути не виявлена. Інші метод застосування даного підходу аналізують поведінку центрального процесора та процесів доступу до пам'яті в комп'ютерах SCADA-системи [17] або використовують для виявлення аномалій властивість періодичності, притаманну мережевому трафіку у SCADA-системах.

***Підхід на основі моделі*** використовується, зокрема, в розробці [18] для кіберзахисту системи керування технологічним процесом. Тут модель-орієнтовний підхід використовується для виявлення порушень кібербезпеки на трьох рівнях. На найнижчому рівні він використовується для захисту мережевого протоколу TCP поверх польової шини Modbus, а також для створення правил Snort. На наступному рівні описуються моделі зв'язку між компонентами мережі. На третьому рівні модель, заснована на навчанні, може обчислювати ймовірності ненормальної поведінки за допомогою мережі Байєса. Модель-орієнтовна система виявлення вторгнень для мікромереж Smart Grid (Model-based Intrusion Detection for the Smart grid) [19] містить модель на основі мереж Петрі всієї ЦПС, включаючи всі пристрої та комунікації. Виявлення атак здійснюється шляхом порівняння поточного мережевого трафіку з моделлю. Результати цієї процедури виявлення потім використовуються як вхідні дані для подальшого аналізу на рівні системи, щоб також ідентифікувати скоординовані комплексні атаки.

З метою покращення кібербезпеки в мережах ЦПС в роботі [20] використано два методи моніторингу стану кібербезпеки SCADA-системи цифрової підстанції: з використанням ***нейронних мереж*** і такий, що базується на ***формальних методах***.

Додаткові приклади реалізацій систем кіберзахисту для ЦПС можна знайти в роботах [21-23].

**Висновки**

В дослідженні розглянуто підходи до побудови систем кіберзахисту цифровізованих систем АСУ ТП, SCADA та промислової автоматики, функціонування яких базується на використанні технологій штучного інтелекту. Проаналізовані підходи, які найбільш прийнятні для застосування в електричних цифрових підстанціях на базі стандарту МЕК 61850. Розглянуто типові рішення і конкретні розробки, що ілюструють відповідні ідеї, підходи, методи, техніки та практичні рішення.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. International Electrotechnical Commission. IEC 61850-1 ed. 2.0 Communication Networks and Systems for Power Utility Automation – Part 1. Introduction and Overview; IEC: Geneva, Switzerland, 2013.
2. Гільгурт С.Я. Підходи до побудови систем виявлення атак на протоколи цифрових електричних підстанцій / С.Я. Гільгурт // Кібербезпека енергетики: Матеріали наук.-практ. конф. Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, м. Київ, 28 травня 2021. – К.: ІПМЕ ім. Г.Є. Пухова НАН України, 2021. – С. 34-42.
3. Quincozes S.E., Albuquerque C., Passos D., Mossé D. A survey on intrusion detection and prevention systems in digital substations // Computer Networks. – 2021. – Vol. 184. – Article 107683.
4. R. Luis de Moura, V.N.L. Franqueira, G. Pessin, "Cybersecurity in Industrial Networks: Artificial Intelligence Techniques Applied to Intrusion Detection Systems," 2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE), Las Vegas, NV, USA, 2023, pp. 2235-2242.
5. J.E. Rubio, C. Alcaraz, R. Roman, J. Lopez, "Analysis of intrusion detection systems in industrial ecosystems," in SECRYPT, 2017, Conference Proceedings, pp. 116-128.
6. L. Tomlin, M.R. Farnam, S. Pan, "A clustering approach to industrial network intrusion detection," in Proceedings of the 2016 Information Security Research and Education (INSuRE) Conference (INSuRECon-16), 2016, Conference Proceedings.
7. L. Zhou, H. Guo, "Anomaly detection methods for IIOT networks," in 2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI). IEEE, 2018, Conference Proceedings, pp. 214-219.
8. A. Javaid, Q. Niyaz, W. Sun, M. Alam, "A deep learning approach for network intrusion detection system," in Proceedings of the 9th EAI International Conference on Bioinspired Information and Communications Technologies (formerly BIONETICS), 2016, Conference Proceedings, pp. 21-26.
9. W. Liang, K.C. Li, J. Long, X. Kui, A.Y. Zomaya An industrial network intrusion detection algorithm based on multifeature data clustering optimization model, IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 2063-2071, 2020.

10. Yang Y., McLaughlin K., Sezer S., Yuan Y., Huang W. Stateful intrusion detection for IEC 60870-5-104 SCADA security. In: 2014IEEE PES general meeting conference & exposition; 2014. pp. 1-5.
11. Y. Yang, K. McLaughlin, T. Littler, S. Sezer, H. Wang, Rule-based intrusion detection system for SCADA networks (2013).
12. Kim J., Park J. FPGA-based network intrusion detection for IEC 61850-based industrial network, Elesevier ICT Express, vol. 4, pp.1-5, 2018.
13. Yoo H., Shon T. Novel approach for detecting network anomalies for substation automation based on IEC 61850. Multimed Tools Appl 2015; 74:303-18.
14. Ten C.W., Hong J., Liu C.C. Anomaly detection for cybersecurity of the substations. IEEE Trans Smart Grid 2011; 2:865-73.
15. Barbosa R.R.R., Pras A. Intrusion detectionin SCADA networks. In: 2010. In: Mechanisms for Autonomous Management of Networks and Services, 4th International Conference on Autonomous Infrastructure, Management and Security, AIMS 2010, Zurich, Switzerland, June 23-25, 2010. p. 163-166.
16. Cheung S., Dutertre B., Fong M., Lindqvist U., Skinner K., Valdes A. Using model-based intrusion detection for SCADA networks. In: Proceedings of the SCADA security scientific symposium, 46; 2007. p. 1-12.
17. Gonzalez E., Stephen B., Infield D, Melero J.J. Usinghigh-frequencySCADA data for windturbine performancemonitoring:asensitivity study. RenewEnergy 2019; 131:841-53.
18. Yang D., Usynin A., Hines J.W. Anomaly-basedintrusion detectionfor SCADA systems. In: 5th intl. topical meeting on nuclear plant instrumentation, control and human machine interface technologies (npic&hmit 05); 2006. pp. 12-16.
19. HahnA, GovindarasuM. Model-based intrustion detection for the smart grid (MINDS). In: Proceedings of the eighth annual cyber security and information intelligence research workshop; 2013. No. 27, pp. 1-4.
20. Kreimel P., Eigner O., Mercaldo F., Santone A., Tavolato P. (2020). Anomaly detection in substation networks. Journal of Information Security and Applications, 54, 102527.
21. Yang Y., Xu H.-Q., Gao L., Yuan Y.-B., Sezer S. Multidimensional intrusion detection system for IEC 61850-based SCADA networks // IEEE Trans. Power Deliv, 2017. – Vol. 32, № 2. – pp. 1068-1078.
22. Hariri M.E., Youssef T.A., Habib H.F., Mohammed O. Online false data detection and lost packet forecasting system using time series neural networks for IEC 61850 sampled measured values. IEEE conf. on Innovative Smart Grid Technologies (ISGT), IEEE: 2017. – pp. 1-5.
23. Rouget P., Badrignans B., Benoit P., Torres L. FPGA Implementation of Pattern Matching for Industrial Control Systems // 2018 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW), Vancouver, BC, Canada, 2018. – pp. 210-213

В.М. Горбачук, Д.І. Ніколенко, М.М. Пустовойт, Д.О. Рибачок, Є.О. Сабадаш

# ДО ЦИФРОВОЇ ДЕЦЕНТРАЛІЗАЦІЇ ЕНЕРГЕТИКИ

За помітної тенденції розвитку систем генерації енергії та менеджменту енергією у напрямку до децентралізованих структур з використанням відновлюваних джерел енергії, необхідно застосовувати цифрові та інтелектуальні платформи для обміну інформацією і проведення фінансових трансакцій відповідними децентралізованими методами в одноранговій (peer-to-peer, P2P) моделі. Децентралізована верифікація трансакцій криптовалют дає змогу використовувати ці шифровані валюти та децентралізовані блокчейн-мережі в системах енергоменеджменту і виконувати фінансові операції, пов'язані з торгівлею вуглецевими викидами (carbon trading). Системи торгівлі викидами вуглецю та інших парникових газів (greenhouse gas, GHG) знижують конкурентоспроможність проектів з викопного палива на ринку і прискорюють інвестиції в джерела енергії з низьким вмістом вуглецю, такі як вітрові та фотоелектричні установки енергогенерації. Цей ринковий механізм дозволяє таким великим суб'єктам, як країни та компанії, що викидають GHGs в атмосферу, купувати та продавати ці гази. Для ринків з торгівлею вуглецевими викидами можна запропонувати блокчейн-рішення, пов'язані з проектуванням смарт-контрактів на платформі блокчейн, і відповідні спеціальні криптовалюти, що використовуються для трансакцій зеленої енергетики й торгівлі вуглецевими викидами [1]. Крім того, для енерготрейдингу можна застосовувати теорію ігор і штучний інтелект.

Дослідження різних блокчейн-схем для торгівлі вуглецевими викидами показує, що використання децентралізованих платформ у такій торгівлі може мати значний вплив на тренд у напрямку до заходів із низьким рівнем вуглецевих викидів, досягнення цілей Кіотського договору (підписаного 11 грудня 1997 р. і чинного з 16 лютого 2005 р.), збільшення вартості зелених криптовалют та обсягу трансакцій. Блокчейн-технології пропонують перспективний шлях до створення більш децентралізованої, ефективної та екологічно продуманої енергетичної екосистеми [2].

Блокчейн (ланцюг блоків), що іноді називають технологією розподіленої книги (distributed ledger technology, DLT), записує історію будь-якого цифрового активу (інвестиційний процес) за допомогою децентралізованої мережі та зв'язаних (chained) блоків через шифровані хеші [3].

Хеш-функція – це будь-яка функція, яка може бути використана для відображення вхідних даних довільного розміру в значення фіксованого розміру, хоча є деякі хеш-функції, які підтримують вихідні значення змінної довжини [4]. Значення, які повертає хеш-функція, – це хеш-значення (хеш-коди, хеш-дайджести, дайджести, хеші) [5]. Ці значення зазвичай використовуються для індексування таблиці фіксованого розміру, яка називається хеш-таблицею. Використання хеш-функції для індексування хеш-таблиці називається хешуванням або розсіяною адресацією сховища.

Ця децентралізована мережа, дещо подібна до Google Docs, є абсолютно непорушною і прозорою [6]. Користувач Google Docs може поділитися документом зі своїми колегами та разом з ними редагувати його в режимі реального часу. Кожен бачить найновішу версію документа і може вносити зміни, які інші можуть негайно помітити. Тоді в кожного є спільний і сумісний (consistent) з іншими погляд на реальний об'єкт, який називають істинним. До появи Google Docs хтось (колега 1) мав створити документ на своєму локальному комп'ютері за допомогою програми на зразок Microsoft Word і потім електронною поштою надіслати документ через Інтернет колезі 2. Цей колега згодом завантажував цей документ, вносив зміни, а потім передавав комусь іншому (колезі 3), хто вносив подальші зміни. При цьому генерувалися 3 версії одного й того самого документа, а зміни до крайньої версії могли вноситися лише після узгодження з колегами 1 і 2 та відповідного надсилання цим колегам версії документа. Оскільки колеги 1, 2, 3 є зв'язаними, але не синхронізованими (in-sync), то процес узгодження документа між ними не є ефективним. Такі продукти, як Google Docs, вирішують проблему синхронізації (syncing problem), щоб спрощувати, пришвидшувати, вдосконалювати співпрацю та обмін даними.

Синхронізовані мережеві обчислення в блокчейні подібні до використання Google Docs, але Google Docs потребує Google, позаяк технологія блокчейну є фактично самодостатньою. Коли у Google Docs документ створюється спільним для групи людей, то він розподіляється серед них, а не копіюється чи передається. Google для Google Docs діє як центральний посередник, який гарантує роботу всього необхідного ПЗ, верифікацію і синхронізацію кожного користувача. Коли всі користувачі довіряють такому посереднику, то Google Docs працює у штатному режимі. Коли не всі користувачі довіряють цьому посереднику чи незалежні організації користувачів намагаються працювати разом синхронізовано, то для Google Docs постають питання відповідного управління. Подібні питання не виникають для блокчейну з мережевими обчисленнями, де дані синхронізуються без довіреного централізованого регулятора [7].

Крім того, якщо Google Docs є текстовим процесором онлайн, то блокчейн потенційно може застосовуватися до будь-яких об'єктів. Ідею переходу від Microsoft Word до Google Docs для синхронізованого редагування тексту можна узагальнювати в глобальному масштабі до багатьох централізованих баз даних, на яких основані юридичні документи, медичні записи, банківські бухгалтерські книги (ledgers) тощо. Тоді можна очікувати суттєвого підвищення ефективності роботи з інформацією за рахунок швидшого і простішого обміну даними та їх використання в реальному часі.

Технологія блокчейну створює децентралізований ланцюг розподілу з послідовних блоків даних, дозволяючи кожному учаснику отримувати доступ до базового документа в один і той самий час. Кожний блок (даних) містить хеш попереднього блоку, мітку часу (timestamp), дані трансакції [8]. Криптографічні концепції використовуються для захисту кожного блоку та зв'язування кожного блоку з попереднім блоком і наступним блоком. Така

конструкція надзвичайно ускладнює зловмисникам (malicious actors) спроби змінювати історичні дані, забезпечуючи високий рівень довіри до інформації, що зберігається на блокчейні.

Девід Чаум здобув науковий ступінь доктора філософії з комп'ютерних наук Університету Берклі (заснованого у 1868 р.) у 1982 р., підготувавши дисертацію «Комп'ютерні системи, засновані, підтримувані та довірені взаємно підозрілими групами» − першу відому пропозицію інфраструктури з протоколом блокчейну, основаним на алгоритмі шифрування RSA [9].

RSA − це криптосистема з відкритим ключем, одна з найстаріших і найширше використовуваних для безпечної передачі даних, винайдена у 1977 р. і названа за першими буквами прізвищ її винахідників [10]. З 1991 р. проводяться конференції RSA. Еквівалентну систему (розсекречену у 1997 р.) розробив у 1973 р. для Штаб-квартири урядового зв'язку (Government Communications Headquarters, GCHQ), британського агентства сигнальної розвідки, Кліффорд Кокс (здобув науковий ступінь бакалавра Королівського коледжу Кембріджського університету (заснованого у 1441 р.) та навчався на докторській програмі з математики Оксфордського університету (заснованого у 1096 р.)).

У 1982 р. Чаум заснував Міжнародну асоціацію криптологічних досліджень (International Association for Cryptologic Research, IACR), яка організовує наукові конференції з досліджень криптографії. Чаум відомий як піонер у криптографії та технологіях збереження приватності, а також як широко визнаний винахідник цифрових грошей. Цифрова валюта (цифрові гроші, електронні гроші, електронна валюта) − це будь-яка валюта, гроші чи подібні до грошей активи, якими в основному управляють, які зберігаються, якими обмінюються на цифрових комп'ютерних системах, особливо на Інтернеті. Типи таких валют − криптовалюта, віртуальна валюта, цифрова валюта центральних банків. Така валюта може записуватися в розподілену базу даних на Інтернеті, централізовану електронну комп'ютерну базу даних у власності компанії чи банку, в цифрові файли або на картку збереженої вартості (stored-value card, SVC). SVC − це платіжна картка, монетарна вартість якої зберігається на самій картці, а не зовнішньому рахунку, підтримуваному фінансовою установою. Тому термінали збору платежів через такі картки не потребують доступу до мережі, оскільки кошти можна знімати прямо з картки і вносити безпосередньо на картку. Подібно до готівки, ця платіжна картка може використовуватися анонімно особою, яка має цю картку й управляє коштами на цій картці. Ці картки є електронним розвитком символічних (умовних) монет (token coins) або токенів, що зазвичай використовуються у платіжних системах невеликої вартості чи там, де доступ до мережі важко або дорого реалізувати (наприклад, у паркувальних автоматах, системах громадського транспорту, закритих платіжних системах на ізольованих територіях тощо).

Дисертація Чаума містить код для реалізації протоколу блокчейну, а у 2008 р. її ідеї розвинула особа з іменем Сатоші Накамото, запропонувавши біткойн. У 1989 р. Чаум заснував компанію DigiCash під торговою маркою «ecash» − анонімні криптографічні електронні гроші [11]. Ці гроші у 1995−1998 рр. застосовував Банк Марка Твена у м. Сент-Луїс (штат Міссурі) як систему

мікроплатежів. Проте DigiCash не вдалося розширити свою базу користувачів й успішно розвиватися, оскільки компанія увійшла в ринок раніше, ніж електронна комерція повністю інтегрувалася з Інтернетом [12]. У 1998 р. DigiCash оголосила про своє технічне банкрутство, а потім продала свої активи eCash Technologies, іншій компанії з цифрових валют.

Ефективне застосування новітніх децентралізованих джерел енергії передбачає цифровізацію інтегрованої енергосистеми з усіми наслідками, які випливають з цього, зокрема для проекту Закону України «Про Єдину державну систему моніторингу виробництва, постачання, транспортування, споживання та оплати за паливно-енергетичні ресурси і комунальні послуги».

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Горбачук В.М., Ляшко В.І., Сирку А.А. Питання децентралізованого консенсусу блокчейнів. *Інфраструктура ринку*. 2019. 34. С. 325–332.
2. Горбачук В.М., Сирку А.А., Сулейманов С.-Б. Блокчейнові застосування у фінансах. *Інфраструктура ринку*. 2019. 35. С. 493–499.
3. Morris D.Z. Leaderless, blockchain-based venture capital fund raises $ 100 million, and counting. *Fortune*. 2016, May 16. https://fortune.com/2016/05/15/leaderless-blockchain-vc-fund/
4. Aggarwal K., Verma H.K. Hash_RC6 − Variable length Hash algorithm using RC6. 2015 *International Conference on Advances in Computer Engineering and Applications* (ICACEA) (March 19−20, 2015, Ghaziabad, India). doi:10.1109/ICACEA.2015.7164747
5. Hash digest. *NIST Glossary*. https://csrc.nist.gov/glossary/term/hash_digest
6. Baynham-Herd X. Blockchain: decentralized Google Docs on a grand scale. *Medium*. 2018, August 30. https://medium.com/blockchain/blockchain-decentralized-google-docs-on-a-grand-scale-55a2e15c07d1
7. Горбачук В.М., Денис О.І. Застосування блокчейнових технологій для оподаткування. *Тенденції розвитку публічних та корпоративних секторів економіки України в умовах макроекономічної нестабільності* (29 січня 2020 р., Київ, Україна). Київ: НаУКМА, 2020. С. 24−26.
8. Narayanan A., Bonneau J., Felten E., Miller A., Goldfeder S. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton, NJ: Princeton University Press; 2016. 336 p.
9. Sherman A.T., Javani F., Zhang H., Golaszewski E. On the origins and variations of blockchain technologies. *IEEE Security Privacy*. 2019. 17 (1). P. 72−77.
10. Rivest R., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*. 1978. 21 (2). P. 120−126.
11. Chaum D. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*. 1981. 24 (2). P. 84−90.
12. Горбачук В.М. Постіндустріальна організація державних замовлень у розвитку AUTODIN, ARPANET, PRNET, NSFNET та Інтернету. *Вісник Одеського національного університету. Економіка*. 2016. Т. 21. Вип. 8. С. 116–122.

А.Д. Данилов, Б.В. Бельмаз

# МЕТОДИ ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЕНЕРГЕТИКИ ВІД КІБЕРЗАГРОЗ

Забезпечення безперебійного функціонування об'єктів критичної інфраструктури енергетичного сектору є пріоритетним завданням національної безпеки. Проте кіберзагрози для таких об'єктів невпинно зростають через активізацію кіберзлочинності, розвиток можливостей зловмисників та недостатню захищеність застарілих промислових систем і мереж керування. Успішні кібератаки на енергетичну інфраструктуру можуть призвести до масштабних збоїв в енергопостачанні, значних економічних втрат та навіть техногенних катастроф. Особливу актуальність захист безперебійного функціонування енергетичних об’єктів набуває на тлі безперервних атак на енергетичну галузь України.

**Метою доповіді** є комплексний аналіз сучасних методів протидії кіберзагрозам для об'єктів критичної енергоінфраструктури, розгляд їх переваг, недоліків та обмежень, а також обґрунтування необхідності впровадження багаторівневої стратегії кібербезпеки.

Розглянемо основні методи захисту об’єктів енергетичної інфраструктури.

**Сегментація мереж, ізоляція та контроль доступу**. Цей метод передбачає логічне розділення інфраструктури на окремі сегменти із застосуванням брандмауерів, систем запобігання вторгненням (IPS), міжмережевих екранів, віртуальних локальних мереж (VLAN) тощо. Таке розмежування критичних систем і мереж керування від решти інфраструктури мінімізує ризики проникнення зловмисників та поширення кібератак. Контроль доступу забезпечується засобами автентифікації, авторизації і крипто-захисту [1].

**Впровадження засобів виявлення та протидії кіберінцидентам і кібератакам**. До них відносяться системи виявлення вторгнень (IDS), системи управління інформаційною безпекою та подіями (SIEM), системи запобігання витокам конфіденційних даних (DLP), антивірусні системи тощо. Такі рішення здатні виявляти аномалії в поведінці систем, мережевому трафіку, діяльності користувачів та сигналізувати про потенційні кібератаки і загрози. Вони також можуть автоматично блокувати шкідливу активність та ініціювати відповідні процедури реагування [2].

**Аналіз та усунення вразливостей**. Регулярний аналіз вразливостей обладнання, операційних систем, прикладного програмного забезпечення та своєчасне оновлення компонентів систем керування і мереж для ліквідації виявлених вразливостей є критично важливим. Наявність застарілих чи неоновлених систем створює додаткові можливості для зловмисників. Процедури сканування та тестування на проникнення дозволяють виявити проблеми безпеки та слабкі місця до того, як ними скористаються кіберзлочинці [3].

**Забезпечення надійності та відмовостійкості**. Критичні компоненти систем енергетичної інфраструктури мають бути захищені від відмов та збоїв шляхом резервування, використання відмовостійких топологій, протоколів та архітектур. Також необхідно мати плани відновлення та продовження функціонування після інцидентів безпеки. План безперервності бізнесу та аварійне відновлення даних є важливими складовими цього підходу.

**Постійний моніторинг кіберзагроз та тестування безпеки**. Регулярне сканування та моніторинг загроз, тестування на проникнення, аудити безпеки дозволяють виявити слабкі місця до того, як ними скористаються зловмисники. Це дає можливість вчасно спланувати та реалізувати заходи з підвищення стійкості систем.

**Підвищення кваліфікації персоналу та формування культури кібергігієни**. Людський фактор відіграє визначальну роль у забезпеченні кібербезпеки. Регулярні тренінги, навчання з підвищення обізнаності персоналу щодо кіберзагроз, формування культури кібергігієни, своєчасне реагування на інциденти та постійний моніторинг стану безпеки дозволять значно знизити ризики успішних кібератак [4; 5].

За результатами проведеного порівняльного аналізу було визначено, що найбільш ефективним є комплексний багаторівневий підхід на основі оцінки ризиків, який охоплює етапи проектування, впровадження, безперервного моніторингу та вдосконалення систем захисту критичної енергетичної інфраструктури. Лише поєднання організаційних, технічних та інженерних заходів здатне забезпечити стійкість і безперервність функціонування цих життєво важливих об'єктів перед обличчям зростаючих кіберзагроз.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. USAID Program "Cybersecurity for Critical Infrastructure in Ukraine". https://www.kafcbit.hneu.edu.ua/usaid-program/
2. Protection of Energy Infrastructure from Cyber Attacks - SSSCIP Exercise. https://cip.gov.ua/en/news/protection-of-energy-infrastructure-from-cyberattacks-has-been-trained-at-the-recent-ssscip-s-tabletop-exercise
3. Кіберзагрози для об'єктів енергетики. https://interfax.com.ua/news/blog/775090.html
4. Проект Концепції кібербезпеки в банківському секторі України. https://bank.gov.ua/admin_uploads/article/proekt_2021-11-04.pdf?v=4
5. Training on increasing the cybersecurity level of energy facilities personnel. https://uazmi.org/news/post/c9cd26e6ead1ef4a843b22d8124e29bc

N. Zaika, M. Komarov, A. Zadniprianets, O. Verkhovets

# INTEGRATION OF UAVS AND NAVIGATION TECHNOLOGIES AT CRITICAL INFORMATION INFRASTRUCTURE

## Components of an unmanned aerial vehicle

1. Receiver and Transmitter for Radio Control Signals: These components enable communication between the ground control station and the UAV, allowing operators to send commands and receive telemetry data.

2. UAV Autopilot: The autopilot system controls the UAV's flight, navigation, and mission execution based on pre-programmed instructions or real-time commands from the ground control station.

3. Throttle Controllers: These regulate the speed and power output of the electric motors or engines, adjusting the UAV's altitude and speed during flight.

4. Electric Motors: These provide the mechanical power needed to drive the UAV's propellers or rotors, enabling lift and propulsion.

5. Propellers, Aerodynamic Surfaces: Propellers or rotors and aerodynamic surfaces such as wings or fins contribute to the UAV's flight dynamics and stability.

6. Actuators and Mechanical Mechanisms: These components translate electronic signals into physical movements, controlling the UAV's orientation, flaps, landing gear, or payload deployment mechanisms.

7. Payload: Refers to additional equipment or sensors carried by the UAV for specific mission objectives, such as cameras, sensors, or communication devices.

8. Navigation Equipment: Includes GPS receivers, altimeters, magnetometers, and other sensors used for precise navigation, position tracking, and waypoint following.

9. Single-Board Computer: Provides computing power for onboard data processing, navigation algorithms, and mission planning.

10. Power Supply Systems: These systems manage the distribution of electrical power to various onboard components, ensuring consistent voltage levels and protection against power surges.

11. Battery Pack (LiPo or Li-ion): Serves as the primary power source for the UAV, providing energy for propulsion, avionics, and payload systems.

Onboard the UAV, there is a significant number of devices requiring electrical power. Here are some key power components and supply systems that can be used on board:

1. Voltage Regulators: These devices ensure stable power supply for various electronic devices on board. They may provide protection against overvoltage and regulate voltage from the batteries.

2. Battery Packs: These are the main power source providing energy for all systems on board the UAV. Lithium polymer or lithium-ion batteries are commonly used due to their high energy density and low weight.

3. Power Distribution Boards: These boards are responsible for distributing and controlling electrical power to different subsystems on board, ensuring each device receives the proper power supply.

4. Telemetry Communication Systems: These systems include radio communication, satellite communication, and may use Wi-Fi, Bluetooth, or other wireless technologies to transmit data between the UAV and the ground station or operator.

The autopilot is a device that allows for the control of UAVs, abstracting the operator from direct control of the powerplant. It can receive commands from the operator or execute pre-programmed missions. By setting trajectory parameters, the autopilot autonomously sends control commands to the propulsion actuators.

The autopilot is utilized for controlling the position, altitude, speed, and other flight parameters, enabling UAVs to perform various tasks without direct intervention from the operator. Autopilot algorithms can be tuned according to specific needs and flight conditions.

To navigate the UAV along its flight trajectory, the autopilot solves navigation tasks, continuously receiving inputs from various sensors and navigation instruments. The autopilot solves navigation tasks by processing information from various sensors and navigation systems. Here are some of them:

1. Global Navigation Satellite System (GNSS): The most common is the GPS (Global Positioning System), along with GLONASS, Galileo, and others. These systems use satellites to provide precise coordinates of the UAV's location.

2. Inertial Navigation System (INS): This system measures changes in the UAV's velocity and orientation using gyroscopes and accelerometers. It is capable of providing navigation data independently of satellite communication.

3. Local Navigation System: These can be systems that utilize local resources such as beacons, radio stations, or ground markers to determine the UAV's location.

4. Other Systems: This may include computer vision systems that use cameras to determine the UAV's position and orientation, as well as systems using radio or acoustic signals for navigation.

To establish a two-way communication channel for transmitting information, there are two popular methods for controlling the UAV:

1. Operator Control using Radio Transmitter (Remote Control): In this method, the operator uses a specialized radio device called a remote control transmitter. The transmitter, often referred to as the remote controller or simply the remote, contains various control elements such as joysticks, toggles, or buttons. These control elements allow the operator to send commands to the UAV. The commands are transmitted via radio frequency from the remote controller to the UAV's onboard receiver. The receiver onboard the UAV receives these commands and relays them to the autopilot or other control systems responsible for executing the UAV's movements.

2. Onboard UAV Control: In this method, the control of the UAV is managed directly onboard the aircraft itself, typically by its autopilot system. The autopilot system autonomously controls the UAV's movements based on its programmed algorithms and the data received from onboard sensors. The autopilot processes sensor readings and executes control commands to adjust the UAV's position, altitude, speed, and other flight parameters without direct input from an external operator.

The autopilot is a device equipped with various inputs and outputs. Its circuit board can accommodate a range of sensors and devices to ensure precise navigation and control. For instance, it can be connected to GNSS receivers (Global Navigation Satellite System), radios, rangefinders, ultrasonic systems, as well as transmitters and receivers. GNSS is a system designed to determine the location of terrestrial, aquatic, and aerial objects, as well as spacecraft in low Earth orbit. Additionally, it allows for the calculation of speed and direction of the signal receiver, as well as accurate timekeeping. These systems consist of both space and ground segments, including control systems.

Single-board computers handle tasks that typically require real-time processing, unlike microcontrollers used in autopilots. The tasks for these computers often extend beyond simple flight control and have a more global scope. Standard operating systems such as Ubuntu, Free BSD, or even Windows can be installed and run on single-board computers.

Single-board computers typically offer significantly more computational resources compared to microcontrollers used in autopilots and are equipped with specialized computing devices such as video accelerators, tensor cores, and others. Their primary tasks include map construction, processing large volumes of data from various sensors, such as stereo cameras and other devices. Many modern single-board computers also support running neural networks using specialized video accelerators.

Thus, a single-board computer performs trajectory control functions and simulates operator actions inside an autonomous unmanned aerial vehicle. These computers are primarily provided by companies such as NVIDIA, Raspberry Pi, and Intel, although there are other solutions from various manufacturers, each with its own advantages.

It's worth mentioning that all components of our UAV are mounted on a specialized rigid structure. These structures, known as frames, serve as a skeleton for mounting all components and devices on the UAV. Frames come in various sizes and configurations, made from different materials. The most popular materials for multicopter frames include fiberglass and carbon fiber. Plastic parts, which can be manufactured using a 3D printer, are also commonly used.

**The main sensors used in unmanned aerial vehicles**

A sensor is a device capable of measuring various parameters and converting them into signals suitable for further analysis. Their use is necessary for determining the state of a system. For example, to determine the position and orientation of an unmanned aerial vehicle (UAV) in space, measure distances to surrounding objects, and other parameters. In autonomous UAVs, the most common sensors measure acceleration, angular velocity, magnetic field vectors, and other parameters to determine position and orientation.

The main sensors and devices used in the navigation systems of unmanned aerial vehicles include:

1. Cameras: Used to gather visual information about the surrounding environment and determine the position of the aircraft.

2. Photodetectors: Measure light parameters such as illuminance to correct the orientation of the aircraft.

3. Barometers, gyroscopes, magnetometers: Used to measure atmospheric pressure, angular velocity, and magnetic field to determine the position and orientation of the aircraft.

4. Ultrasonic rangefinders: Measure the distance to surrounding objects using high-frequency sound waves.

5. Laser rangefinders and LiDARs: Used for precise distance measurements and creating three-dimensional models of the surrounding space.

6. GNSS receivers and differential correction systems: Used to obtain global positioning information of the aircraft using satellite signals, with differential correction systems improving the accuracy of these measurements.

There is also a classification of sensors based on their action. In addition to those mentioned earlier, there are optical, capacitive, and potentiometric sensors. Special metric systems are used to measure height above the surface or distance to surrounding objects. These include laser, ultrasonic, and radio rangefinders, as well as systems based on Stereo Cameras. Stereo Cameras provide volumetric data about surrounding objects, allowing for depth information retrieval. Lidars, which are rotating-head laser rangefinders, are widely used for obtaining distance measurements to objects. Although they are quite expensive, they are often replaced by stereo camera systems, which can reduce system costs and, in some cases, achieve even greater accuracy. Meanwhile, monocular cameras and photodetectors are essential components of any machine vision system.

**Navigation tasks**

Navigation is used to determine the position, orientation, and velocity of the aircraft. It is an essential component in the management and control of aircraft movement. Global satellite navigation systems provide accurate real-time geographic positioning. Navigation also involves forming vectors of velocity, position, and orientation of the aircraft in coordinate systems, as well as onboard time scale.

Inertial navigation is another method for determining the aircraft's position. This method relies on internal sensors such as gyroscopes and accelerometers, which measure angular velocities and linear accelerations. Using mathematical algorithms, the inertial navigation system processes these data to determine the orientation, position, and velocity of the aircraft. It operates independently of satellite signals, making it useful for autonomous calculations and navigation process automation. Inertial navigation systems consist of three elements:

1. Gyroscopes (for determining angular velocities),

2. Accelerometers (for determining linear acceleration, acting as correctors for gyroscopes),

3. High-performance computer with mathematical algorithms (for computing navigation tasks, processing, and filtering data).

**The principle of operation of radio navigation systems**

Radio navigation systems operate by measuring the distance between the unmanned aerial vehicle (UAV) and a ground-based station that emits a special radio signal into space. Onboard the UAV is a radio signal receiver, known as a navigation

receiver, which receives these signals. The main goal is to determine the time it takes for the signal to travel from the station to the receiver. Knowing the distance from the base station to the navigation receiver allows determining the UAV's position in space. If the base station is stationary and its coordinates are known, a system of equations can be solved to determine the UAV's coordinates in space. This method involves using three equations to determine coordinates. After clock synchronization, the system of equations is solved to determine the precise location of the aircraft.

**Satellite navigation**

Satellite navigation utilizes the Global Navigation Satellite System (GNSS), which consists of various constellations of satellites such as GPS, GLONASS, Beidou, Galileo, as well as the Indian and Japanese systems. Each satellite sends a special data packet to the receiver onboard the aircraft, including information about its identifier, current time, and status. The accuracy of satellite navigation systems typically ranges from 1 to 10 meters, depending on the satellite constellation conditions. However, one drawback of this system is the low data update frequency: the receiver can only receive information at frequencies ranging from 10 to 100 Hz, while satellite vehicles transmit data at a much lower frequency, approximately 10 Hz. To improve the accuracy of the navigation system, reference stations can be used to correct the satellite signal. These stations determine the error in determining the aircraft's position and transmit special differential corrections to its onboard system, allowing for greater navigation accuracy.

**Factors affecting the accuracy of coordinate determination**

In urban environments, satellite navigation systems face significant challenges due to signal reflection, known as multipath effect. This occurs when signals from satellites reflect off urban infrastructure objects, creating multiple signal paths that differ from the direct path. Consequently, the receiver struggles to discern the correct signal. To mitigate multipath effects, specialized systems incorporating inertial navigation systems calculate the probability of the UAV's position [1].

GNSS systems are practically ineffective indoors because signals struggle to penetrate structures like iron and concrete. Therefore, indoor environments typically deploy local radio navigation systems. The most precise positioning systems indoors utilize optics, with laser-based systems being the preferred choice. Such systems are widely used in the film industry and game production. An example is a special base station housing an array of infrared LEDs, which emit light at a specific frequency. Inside the base station, special motors rotate at a set angular velocity, emitting light akin to a beacon in the infrared spectrum.

When the light reaches the photodiode receiver surface, the UAV's position relative to the base station is determined. Subsequently, the signal is processed by a microcontroller, which constructs a signal intensity graph over time to determine the navigation system's angles. Using trigonometric expressions and calculations, spatial coordinates are obtained. Another navigation option involves ultrasonic beacons. Here, the principle is similar: the beacon emits a signal received by the receiver, which measures its passage time and calculates coordinates. This system's main advantage is high precision and robustness against obstacles. However, it may be

susceptible to noise and external distortions, potentially affecting accuracy.
Onboard the UAV, within the autopilot module, a graphical microprocessor can be installed to process analog images and overlay special telemetry onto them. This allows the pilot to visualize the aircraft's status on the image, such as angular velocity, position, satellite count, and other useful information. For the microcontroller to function correctly, precise time measurement is necessary, achieved using a special quartz resonator placed on the board. Navigation using computer vision employs cameras connected to a single-board computer via a special interface ribbon cable. The computer vision system transmits data about the UAV's position and orientation in space onboard, enabling the autopilot to receive this information for precise control, coordinate determination, and spatial positioning using a universal asynchronous serial port.

**The tasks are related to the coordination of a large number of devices**

To control a group of UAVs performing various aerobatic maneuvers, such as LED flashing to create spectacular aerial displays, a control program needs to be developed for each aircraft, followed by pre-flight testing. During flight, the aircraft can form both simple geometric shapes and complex animations. Simulation modeling systems allow for the calculation of all flight trajectories, from takeoff to landing, and assess the feasibility of executing the flight program considering the characteristics of the aircraft and their flight time. During flight, the distance between aircraft when forming figures can be just a few dozen centimeters, so it's essential to have a navigation system with centimeter-level accuracy. For takeoff and landing, when the accuracy of the navigation system may be insufficient, the aircraft take off in small groups. In indoor environments for group flights, special local positioning radio navigation systems can be used, along with other systems with a similar operating principle. A crucial aspect is synchronizing the group of aircraft, for which a temporary scale of the navigation spacecraft with a highly accurate atomic clock is utilized.

**Recommendations**

To enhance resilience against cyber attacks on state information resources and critical infrastructure objects [2], the following recommendations are proposed:

1. Utilize advanced technologies to automate monitoring processes and recognize threats for critical infrastructure objects [3].

3. Modernize the external security system and conduct periodic analyses of the state of large commercial, industrial, and residential facilities [4].

4. Conduct site surveys of enterprise premises using aerial reconnaissance to perform terrain photography, measure radiation levels of communication channels, and measure environmental indicators. For monitoring stationary objects, it is convenient to utilize base stations capable of recharging drone batteries or replacing them after landing and positioning the UAV inside the station. When flying indoors and conducting group flights, it is necessary to build a map of the area and calculate the route using simulation modeling.

5. Employ stationary bases for servicing and storing UAVs. Utilize additional signal repeaters for more accurate navigation.

**Conclusions**

The utilization of modern technologies for protecting critical information infrastructure objects significantly expands capabilities in the domains of tracking, monitoring, automation, and enhancement of comprehensive data security systems. Analyzing information during environmental monitoring involves identifying potential threats, determining their parameters and level of risk, as well as implementing risk reduction methods and preventing potential issues, along with continuously monitoring the situation. This is a crucial stage in ensuring the security of information resources.

## REFERENCES


1. Security and critical infrastructure. https://dronehub.ai/defence-security.
2. Gryshchuk R., Okhrimchuk V. Setting a scientific task for developing templates of potentially dangerous cyber attacks. Information Security. 2015, Vol. 21. No. 3. P. 301-308.
3. Protection of critical infrastructure in emergency situations / ed. by P. B. Volianskyi. Kyiv: NISD, 2021. 375 p.
4. Autonomous security drone. https://sunflower-labs.com.

Є.О. Застьола, О.А. Сергієнко

# ВИКОРИСТАННЯ ФІНАНСОВИХ ІНСТРУМЕНТІВ НА ОСНОВІ КРИПТОВАЛЮТНОГО РИНКУ ДЛЯ РОЗВИТКУ СТАРТАПІВ КІБЕРБЕЗПЕКИ ЕНЕРГЕТИЧНОЇ ГАЛУЗІ

В останні десятиліття сталася динамічна еволюція кіберзагроз, що відбивається на всіх сферах життя, включаючи енергетичний сектор. За останні кілька років енергетична промисловість стала предметом постійних кібератак, що наголошує на необхідності постійного вдосконалення кібербезпеки в цій галузі. У цьому контексті стартапи з кібербезпеки мають великий потенціал у запобіганні та реагуванні на кіберзагрози в енергетичному секторі. Використання фінансових інструментів на основі криптовалютного ринку може забезпечити необхідний капітал для розвитку таких стартапів, що стане ключовим фактором їх успішного зростання та впливу на кібербезпеку в енергетичній галузі.[1]

Технологічні інновації у кібербезпеці.

Передові технології, такі як штучний інтелект, машинне навчання та блокчейн, відіграють важливу роль у вирішенні кіберзагроз. Стартапи, які спеціалізуються на розробці та впровадженні цих технологій, мають потенціал стати ключовими гравцями у сфері кібербезпеки. Наприклад, блокчейн може забезпечити безпеку даних та транзакцій, штучний інтелект може виявляти аномальну поведінку, а машинне навчання може постійно вдосконалювати системи оборони.[2]

Фінансові інструменти на основі криптовалютного ринку.

Криптовалютний ринок відкриває нові можливості для залучення інвестицій та фінансування стартапів. Ініціативи, такі як Initial Coin Offerings (ICO) та Security Token Offerings (STO), дозволяють стартапам залучати капітал без необхідності проходження складних процедур традиційного банківського сектору. Крім того, використання криптовалют дозволяє створювати децентралізовані системи, що забезпечують більшу прозорість та безпеку операцій.

Приклади успішних стартапів.

Деякі стартапи вже успішно використовують фінансові інструменти на основі криптовалютного ринку для розвитку своїх проектів у сфері кібербезпеки в енергетичній галузі. Наприклад, Grid+ - це стартап, який використовує блокчейн і криптовалютні технології для розробки інноваційних рішень у сфері енергетики. Вони створюють децентралізовану платіжну систему, яка дозволяє споживачам купувати та продавати енергію безпосередньо між собою, обходячи традиційні енергетичні компанії. Grid+ здійснив успішну кампанію з краудфандингу, використовуючи технологію блокчейну та криптовалюту, що дозволило їм залучити необхідний капітал для розвитку своєї платформи та поширення на нові ринки. Цей приклад демонструє, як використання фінансових інструментів на основі криптовалютного ринку може сприяти розвитку стартапів у сфері енергетики та

підвищенню кібербезпеки.[3]

Hacken - це стартап, спеціалізований на кібербезпеці, який вдало використовував фінансові інструменти на основі криптовалютного ринку. Вони здійснювали успішні Security Token Offerings (STO), щоб залучити інвестиції на розвиток своїх проектів з кібербезпеки. Це дозволило їм розширити свої послуги та забезпечити більш широкий охоплення ринку.[4]

Децентралізовані мережі - Багато стартапів у цьому секторі використовують блокчейн-технології для створення децентралізованих мереж, які забезпечують більш високий рівень безпеки. Наприклад, створення децентралізованих систем моніторингу та управління енергетичними мережами може зменшити ризики кібератак та забезпечити більш ефективне функціонування інфраструктури.[4]

Відкритий доступ до фінансування - Криптовалютний ринок відкриває можливості для стартапів у кібербезпеці залучати фінансування від широкого кола інвесторів з усього світу. Це дозволяє навіть невеликим компаніям отримати доступ до капіталу для розробки своїх продуктів та послуг.

Регуляторний прогрес - Зростаюча увага до криптовалютного ринку з боку регуляторних органів може сприяти більшій стабільності та довірі до цих фінансових інструментів. Наприклад, введення регулювань щодо Security Token Offerings може забезпечити більшу захищеність інвесторів та зробити ці інвестиції більш привабливими для широкої аудиторії.

Глобальний ринок - Криптовалютний ринок є глобальним, що означає, що стартапи з кібербезпеки в енергетичній галузі можуть отримати доступ до інвесторів та клієнтів з усього світу, збільшуючи свої шанси на успіх та розширення бізнесу.[5]

Ці приклади та факти ілюструють потенціал фінансових інструментів на основі криптовалютного ринку для розвитку стартапів кібербезпеки в енергетичній галузі та їхнього впливу на безпеку в цій сфері.

Як висновок, можна сказати, що використання фінансових інструментів на основі криптовалютного ринку виявляється потужним каталізатором для розвитку стартапів кібербезпеки в енергетичній галузі. Це дозволяє створювати інноваційні рішення та забезпечувати необхідний капітал для їх реалізації, що в свою чергу підвищує рівень кібербезпеки в енергетичному секторі.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Демедюк С. Кібербезпека сьогодні – життєво важливий фактор існування енергетичної галузі. URL: https://www.rnbo.gov.ua/ua/Diialnist/5024.html.
2. Ткачук Н. Стан та проблемні питання реалізації Стратегії кібербезпеки України. Інформація і право. № 1(28)/2019. С. 129-134.
3. https://twitter.com/gridplus
4. https://hacken.io/
5. Технологія blockchain як складова інформаційної безпеки / https://csecurity.kubg.edu.ua/index.php/journal/article/view/84.

О.І. Зінченко

# КІБЕРТЕРОРИЗМ В ЕНЕРГЕТИЧНОМУ СЕКТОРІ УКРАЇНИ ТА ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Енергетичний сектор України стикається з численними викликами у сфері кібербезпеки, особливо в умовах тривалого конфлікту з Росією. Однією з основних проблем є застаріла інфраструктура. Багато енергетичних компаній в Україні все ще використовують обладнання та програмне забезпечення, що вже не відповідають сучасним стандартам безпеки. Це робить їх уразливими до кібератак, оскільки сучасні загрози швидко еволюціонують, а старі системи не можуть ефективно протистояти новітнім методам злому. Зростаюча кількість і складність кібератак на енергетичний сектор вимагає комплексного підходу до вирішення проблем кібербезпеки. Це включає не лише технічні заходи, але й організаційні зміни, спрямовані на підвищення обізнаності та готовності до реагування на інцидент.

Україна вже неодноразово ставала жертвою масштабних кібератак на свою енергетичну систему. На жаль, є лише декілька відомих прикладів кібератак на українську енергетичну систему. Так,у грудні 2015 року хакери атакували системи керування електромережею Прикарпаття, використовуючи шкідливий програмний код. Ця атака спричинила відключення електропостачання в деяких районах області. У 2016 році хакери вторглися в систему керування електромережею Чернівецької області та відключили електропостачання на деякий час. Це призвело до незручностей для місцевих мешканців та підкреслило потенційну загрозу кібербезпеці в енергетичному секторі. У 2017 році відбулася спроба кібератаки на систему керування Хмельницької атомної електростанції. Хоча ця атака не призвела до порушення роботи станції, вона викликала серйозні обурення і стимулювала подальші заходи з підвищення кібербезпеки. З початку 2020-х років українська енергетична система продовжує стикатися з постійними кіберзагрозами та спробами вторгнень. Хоча багато з цих інцидентів можуть бути непомітними для широкої громадськості через ефективні заходи кіберзахисту, вони підкреслюють постійну необхідність підтримки та покращення кібербезпеки у сфері енергетики. Ці атаки показали вразливість енергетичних систем перед кіберзагрозами та вимагають посилення заходів з кібербезпеки для захисту критично важливої інфраструктури.

Такі атаки не тільки створюють фізичну шкоду, але й сіють хаос і недовіру до здатності держави захищати своїх громадян та інфраструктуру. Після початку повномасштабного вторгнення Росії в 2022 році кількість кібератак на енергосистему України значно зросла, що створило нові виклики в умовах воєнного стану. Воєнний стан суттєво ускладнив ситуацію з кібербезпекою.

Постійні фізичні атаки на інфраструктуру разом із кібератаками створюють умови для систематичного руйнування енергетичної мережі.

З початку війни на об'єкти енергетичної інфраструктури України було здійснено понад 1 200 000 кібератак, тоді як за весь 2021 рік їх було зафіксовано 900 000. У відповідь на це міжнародні партнери, такі як США та Європейський Союз, почали надавати Україні допомогу у відновленні та захисті критичної інфраструктури, включаючи постачання генераторів та підтримку кібербезпеки. Зусилля зосереджені на підвищенні стійкості енергосистеми та її інтеграції з європейськими мережами. Попри всі труднощі, війна також стимулювала розвиток внутрішніх ресурсів і технологій кібербезпеки в Україні. Підприємства та уряд активно працюють над удосконаленням своїх систем захисту, впроваджуючи нові технології та розробляючи стратегії для ефективного протистояння кіберзагрозам. Військовий конфлікт підштовхнув Україну до більш рішучих дій у сфері кібербезпеки, що в майбутньому може стати ключовим фактором у зміцненні національної безпеки

Недостатня кількість кваліфікованих фахівців з кібербезпеки є значною проблемою. Підготовка таких спеціалістів вимагає значних ресурсів і часу, і Україна, як і багато інших країн, стикається з дефіцитом професіоналів у цій сфері. Відсутність належного рівня підготовки та знань у працівників енергетичних компаній часто призводить до того, що вони не можуть ефективно реагувати на кібератаки, що ще більше ускладнює ситуацію. Крім того, слабка інтеграція з європейськими системами безпеки означає, що Україна не має повного доступу до передових технологій та методик захисту. Хоча деякі заходи були прийняті для покращення співпраці з ЄС, цього недостатньо для забезпечення належного рівня захисту. Брак фінансових ресурсів обмежує можливості модернізації інфраструктури та впровадження сучасних систем захисту, що робить українські енергетичні компанії легкою мішенню для кіберзлочинців.

Вважаємо, що задля зміцнення кібербезпеки в енергетичному секторі України, необхідним є застосування наступних заходів:

1. модернізація інфраструктури (інвестиції в оновлення застарілого обладнання та впровадження сучасних технологій, таких як розподілена генерація та мікромережі, які забезпечать більшу стійкість до атак);

2. навчання фахівців (підвищення кваліфікації кадрів через освітні програми та тренінги для кіберспеціалістів, що дозволить ефективно протидіяти кіберзагрозам);

3. міжнародне співробітництво (розширення співпраці з міжнародними партнерами та організаціями для обміну досвідом та передовими практиками у сфері кібербезпеки);

4. вдосконалення законодавства (оновлення нормативно-правової бази, яка регулює питання забезпечення кібербезпеки, для її відповідності сучасним викликам і загрозам);

5. постійний моніторинг та аудит (впровадження систем постійного моніторингу та аудиту безпеки критичної інфраструктури для своєчасного виявлення та нейтралізації загроз).

Отже, стан кібербезпеки енергетичного сектору України залишається предметом підвищеної уваги, і необхідні подальші заходи для посилення захисту критично важливої інфраструктури країни. Умови воєнного конфлікту створюють серйозні виклики для кібербезпеки енергетичного сектору України. В умовах війни кібератаки можуть бути використані як один із інструментів гібридної війни для завдання шкоди енергетичній системі. Напади можуть спрямовуватися на відключення електропостачання, перешкоди у виробництві енергії або навіть спроби знищення критичних об'єктів. В умовах воєнного конфлікту уряд і енергетичні компанії повинні максимально посилити заходи з кібербезпеки, включаючи моніторинг та виявлення загроз, підвищення готовності до реагування та відновлення після атак. Відключення електропостачання або інші руйнівні наслідки кібератак на енергетичну систему можуть мати серйозні наслідки для населення та економіки країни, особливо в умовах війни.

Отже, в умовах воєнного конфлікту важливою є підтримка високого рівня кібербезпеки енергетичного сектору, щоб забезпечити безпеку та стабільність енергопостачання країни. Впровадження цих заходів допоможе Україні не лише впоратися з поточними викликами, але й створити більш стійку та захищену енергетичну систему в майбутньому.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. З початку війни зафіксовано понад 1,2 млн кібератак на енергосектор, – Фарід Сафаров. *Урядовий Портал*. URL: https://www.kmu.gov.ua/news/z-pochatku-vijni-zafiksovano-ponad-12-mln-kiberatak-na-energosektor-farid-safarov (дата звернення: 18.05.2024)
2. Ukraine–Cybersecurity for Critical Infrastructure Activity · DAI: International Development. *DAI · Shaping a more livable world*. URL: https://www.dai.com/our-work/projects/ukraine-cybersecurity-for-critical-infrastructure-activity (date of access: 18.05.2024)

3. Ukraine–Cybersecurity for Critical Infrastructure Activity DAI: International Development. *DAI · Shaping a more livable world*. URL: https://www.dai.com/our-work/projects/ukraine-cybersecurity-for-critical-infrastructure-activity (date of access: 18.05.2024).

О.А. Хоменко, М.М. Худинцев,

# ТРЕНДИ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ КІБЕРСТРАХУВАННЯ

Збільшення залежності сучасного суспільства від цифрових послуг спонукало організації до значних інвестицій в адміністративні та технічні контрзаходи для запобігання випадковим або зловмисним інцидентам кібербезпеки. Реалізація сучасних кіберінцидентів та кібератак та, які призводять до серйозних наслідків, показала, що управління кібербезпекою організації не може покладатися лише на заходи пом'якшення ризиків [1]; натомість кіберстрахування постає як необхідне доповнення до організаційних заходів безпеки. Типові атаки на кібербезпеку, які призвели до критичних втручань, вплинули на тисячі компаній у багатьох регіонах і галузях [2,3]. Розширені кіберзагрози, які переважають сьогодні, включають криптоджекінг, зловмисне програмне забезпечення, атаки на ланцюги поставок, програми-вимагачі, компрометацію бізнес-електронної пошти та інші [4,5].

Основна стратегія страхування полягає в тому, що організація ділить ризик із зовнішньою стороною, яка може найбільш ефективно керувати конкретним ризиком залежно від оцінки ризику. Застосування технологій автоматичної оцінки кіберризиків, індексації стану захищеності, зрілості та розвитку інформаційних, комунікаційних, безпекових ресурсів, смарт-технологій пришвидшують та покращують процес об'єктивної оцінку та розподілу ризиків. Ринок і практики кіберстрахування у світі швидко зростають і очікується подальший розвиток [2,5]. Пандемія COVID-19, а в Україні ще і відкрита фаза російської збройної агресії змусили перейти до віддаленого режиму роботи велику кількість робітників, що призвело до зміни ландшафту загроз, ризиків та тенденцій кіберстрахування. Огляди літератури [6-8] свідчать про фундаментальний розвиток та трансформацію сфери кіберстрахування, нові тренди в усіх ланках відповідних технологічних та бізнес- процесів.

Метою дослідження є підготовка інформаційної бази та виявлення особливостей технологічних, бізнес-процесів та тенденцій кіберстрахування, дослідження можливостей та передумов застосування інформаційних технологій для автоматизації та цифровізації повного циклу процесів кіберстрахування.

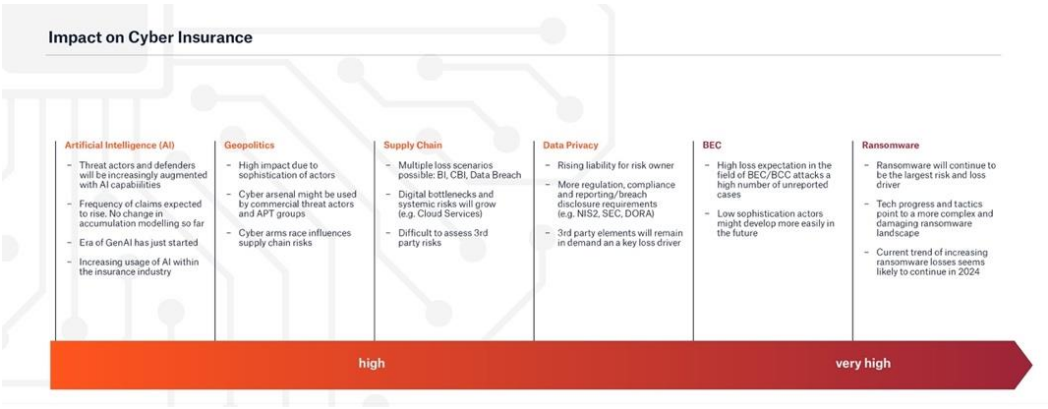



Рисунок 1 – Впливові показники кіберстрахування
(взято з https://www.munichre.com/)

Основну увагу приділено дослідженню андерайтингу, управління претензіями, аналізу доступних типів страхових полісів і ризиків кібербезпеки, які зазвичай підлягають страхуванню.

Також розглянуто стан нормативного забезпечення та практики кіберстрахування в Україні, зокрема у зв'язку з впровадженням аудиту інформаційної безпеки об'єктів критичної інфраструктури [9].

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Franke U.:ThecyberinsurancemarketinSweden.Comput.Secur.68, 130–144 (2017).
2. Survey, H. Cyber Insurance: A Hard Reset, Howden Broking, https://www.howdengroup.com (2022).
3. Gallagher Cyber Insurance Market Conditions Report: Guidanceas the cyber insurance market continues to harden. https://www.ajg.com/us/news-and-insights/ (2023).
4. ENISA Threat Landscape 2023. https://www.enisa.europa.eu/publications/ (2023).
5. Report, H.: Don't let cyber be a game of chance. https:// www.hiscoxgroup.com/sites/group/files/documents/2021-04/.
6. Marotta, A., Martinelli, F., Nanni, S., Orlando, A., Yautsiukhin, A.: Cyber-insurance survey. Comput. Sci. Rev. 24, 35–61 (2017).
7. Aziz, B.: Others A systematic literature review of cyber insurance challenges. In: 2020 International Conference on Information Technology Systems and Innovation (ICITSI), pp. 357–363 (2020).
8. Dambra, S., Bilge, L., Balzarotti, D.: SoK: Cyber insurance? technical challenges and a system security roadmap. In: 2020 IEEE Symposium On Security And Privacy (SP), pp. 1367–1383 (2020).
9. Постанова Кабінету Міністрів України від 24 березня 2023 року № 257 «Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури».

М.М. Худинцев, І.Л. Палажченко

# МОДЕЛЬ ІНДЕКСУ МЕРЕЖЕВОЇ АКТИВНОСТІ

Дослідженням глобальних та мережевих індексів кібербезпеки, стійкості (резильєнтності, кіберризильєнтності), цифровізації присвячені чисельні публікації, кількість яких значно збільшується [1,2].

Окремі глобальні мережеві індекси кібербезпеки зведені у Таблиці. Методика формування наведених індексів передбачає кінцеву оцінку для індексу суб'єкта індексування у вигляді безрозмірного показника (коефіцієнта), який не є конфіденційною інформацією про кібербезпеку або стан зрілості кібербезпеки суб'єкта індексування.

Таблиця 1 – Глобальні мережеві індекси кібербезпеки

| Назва | Скорочення | Тип | Категорія | Видавник |
|---|---|---|---|---|
| Automate Third-Party Security Rating Platform | A3SRP | Global | Network | Panorays |
| Black Kite Cyber Risk Ratings Platform | BKCRRP | Global | Network | Black Kite Inc. |
| BitSight Security Ratings Platform | BSSR | Global | Network | BitSight Technology LTD |
| Cyber Exposure Index | CEI | International | Network | Cyber Intelligence House |
| Cyber Green Index | CGI | Global | Network | CyberGreen Institute |
| Prevalent Vendor Threat Monitor | PVTM | Global | Network | Prevalent, Inc. |
| RiskRecon Cybersecurity Ratings | RRCR | Global | Network | RiskRecon Co., |
| SecurityScorecard Ratings Platform | SSR | Global | Network | Security Scorecard Co. |
| UpGuard Ratings Platform | UGR | Global | Network | UpGuard Inc. |

Основні індикатори (показники) мережевих індексів кібербезпеки:

- Незахищені сертифікати SSL/TLS;
- Ризики підробки електронної пошти та фішингу;
- Вразливості;
- Сприйнятливість до шкідливих програм;
- Мережева безпека;
- Непотрібні відкриті порти;
- Вразливе програмне забезпечення;
- Схильність до атак зсередини;
- Доступність HTTP;
- Конфігурація безпечних файлів cookie.

Прикладом неглобального мережевого індексу є локальний індекс кібербезпеки Local CyberSecurity Index (скор. – LCSI) (Network Monitoring Index, 2023). Тип – корпоративний (corporative). Категорія – комбінований (combined). Інші параметри індексу визначаються його версією. Формат версії індексу – LCSI.XX.YY, де XX – останні дві цифри року, YY – номер версії. Нижче міститься опис версії LCSI.22.01. Розробник індексу – Міжнародний університет кібербезпеки (International Cybersecurity University, скор. – ICU), Київ (Україна).

Об'єкт індексування (суб'єктний рівень) – об'єкт критичної інформаційної інфраструктури об'єкта критичної інфраструктури, органу державної влади, підприємства, установи, організації.

Об'єкт індексування (секторальний рівень) – критична інформаційна інфраструктура, інформаційні, комунікаційні, мережеві ресурси або сукупність об'єктів індексування (суб'єктний рівень) критичної інфраструктури, галузі, сектору економіки.

Об'єкт індексування (національний рівень) – критична інформаційна інфраструктура або сукупність об'єктів індексування (галузевий рівень) країни, інформаційні, комунікаційні, мережеві ресурси критичної інфраструктури органів управління державою та економікою, органів безпеки та оборони, державних реєстрів, державні електронні сервіси або інші електронні сервіси, якими користуються більше 10% населення країни.

Методологія формування LCSI.22.01 базується на моделі оцінки і індексації стану кібербезпеки в критичній інфраструктури з використанням методу експертних оцінок, індексного методу математичної статистики, математичної теорії рейтингів, теоретико-ігрової кооперативної ресурсної моделі [1].

Показники (субіндекси) LCSI:

- Індекс мережевої активності Network Monitoring Index (скор. – NMI);
- Показник опитування (Indicator of the Survey, скор.– IS);
- Показник аудиту (Audit Indicator, скор. – AI).

Показники LCSI формуються у відповідності до вимог нормативних документів, а саме Загальних вимог до кіберзахисту об'єктів критичної інфраструктури (Постанова КМУ від 19.06.2019 №518), а також Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури (Наказ Адміністрації Держспецзв'язку від 06.10.2021 №601), які узгоджуються з основними вимогами ISO 27000 та NIST Cybersecurity Framework.

Індекс мережевого моніторингу NMI формується шляхом аналізу:

- мережевого трафіку на виявлення кібератак та зловмисної активності від зовнішніх постачальників;
- внутрішнього мережевого трафіку та зловмисної активності всередині периметру;
- захищеності веб-ресурсів;
- результатів віддаленого сканування на вразливість.

Апаратною базою моніторингу є сенсори моніторингу мережевого трафіка системи виявлення вразливостей і реагування на кіберінциденти та кібератаки (порядок функціонування системи визначено Постановою КМУ від 23.12.2020 р. №1295), а також комплекс організаційно-технічних заходів з виявлення вразливостей і недоліків у налаштуванні інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси (порядок проведення експериментального проекту щодо запровадження відповідного комплексу визначено Постановою КМУ від 23.12.2020 р. №1363).

Показник аудиту AI формується шляхом проведення незалежного аудиту інформаційної безпеки у відповідності до Порядку проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури (Постанова КМУ від 24.03.2023 р. №257).

Показник опитування (самооцінювання) IS формується шляхом надання відповідей (у офлайн або онлайн формах) власником (розпорядником, довіреною особою) об'єкту індексування.

У 2023-2024 році здійснювався збір та аналіз даних мережевого моніторингу.

Для різних версій LCSI можуть змінюватися:

- кількість та перелік показників індексу;
- кількість та перелік складових показників індексу;
- методика розрахунку (формування) вагових та інших коефіцієнтів індексу;
- перелік та зміст методів формування.

Вимоги до об'єкту індексування:

- готовність до обговорення умов обміну відомостями (чутливою інформацією) та участі у індексуванні;
- готовність на отримання та використання відомостей мережевого моніторингу від зовнішніх постачальників та внутрішніх джерел;
- наявність сенсорів на вході до корпоративної мережі або даних про мережеву активність від партнерів (зовнішніх постачальників);
- готовність проходити передбачені методикою внутрішні (зовнішні) аудити інформаційної безпеки;
- готовність надавати відповіді на питання опитувальників;
- готовність на оприлюднення загального індексу.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Худинцев М.М. (заг. ред.), Жилін А.В., Давидюк А.В. Світові індекси кібербезпеки: огляд та методики формування (Глобальний звіт / Каталог), Монографія, Міжнародний університет кібербезпеки, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. – К.: 2021. – 240 с. ISBN 978-966-136-887-2.
2. Khudyntsev, M., Lebid, O., Bychenok, M., Zhylin, A., Davydiuk, A. (2023). Network Monitoring Index in the Information Security Management System of

Critical Information Infrastructure Objects. In: Dovgyi, S., Trofymchuk, O., Ustimenko, V., Globa, L. (eds) Information and Communication Technologies and Sustainable Development. ICT&SD 2022. Lecture Notes in Networks and Systems, vol. 809. Springer, Cham. https://doi.org/10.1007/978-3-031-46880-3_17, ISBN 978-3-031-46879-7.

O.M. Dzhyhun

# UKRAINIAN ENERGY: CHALLENGES AND TASKS DURING A FULL-SCALE WAR

The energy industry of Ukraine has been in a state of war since 2014, therefore, from February 24, 2022, with a full-scale invasion of the territory of Ukraine, certain solutions have already been worked out in the territories of Ukraine, where active hostilities were previously conducted, and temporarily occupied territories. At the same time, the Ukrainian energy industry faced a list of new, even more threatening challenges, such as nuclear terrorism with the seizure of nuclear power plants, numerous damages to critical infrastructure — electric and gas networks, a critical decrease in demand for energy products due to the departure of the population and the termination of business, an even more critical reduction in the level of payments in the energy system, and the decision to continue synchronizing the energy system of Ukraine with the energy system of Continental Europe, despite the hostilities throughout the country, the fuel crisis, etc. [1].

The energy industry has a significant number of critical assets that need to be managed effectively, including scheduling and timely maintenance and repairs to reduce unplanned downtime and increase equipment availability. The upheaval caused by the war in Ukraine showed how automation of asset management processes helps to quickly respond to accidents and ensure the stability of the energy system.

From the first hours after the invasion, Russian troops have been massively shelling not only Ukrainian cities and towns, but also trying to destroy critical energy infrastructure facilities: high-voltage networks, transformer substations, control centers, as well as directly power plants, including renewable energy facilities.

A year ago, the Russians tried to destroy the Ukrainian energy system and leave the country without electricity. The titanic efforts of the military, air defense teams and power engineers managed to save the power system. However, the enemy inflicted significant damage on the entire sector.

Compared to the pre-war years, nuclear generation capacity decreased by 44%, hydrogen generating capacity by 29%, and renewable energy sources (RES) capacity by 24%. Now the main component is nuclear generation. All nine power units of the South Ukrainian, Rivne and Khmelnytsky NPPs with a total capacity of 7,880 MW were loaded at full capacity in the winter period from November 2023 to February 2024. The Zaporizhzhia NPP with a capacity of 6 GW was seized by the Russian Federation on March 4, 2022, and has not been producing electricity for almost a year [2].

Since the beginning of the full-scale invasion and massive shelling of infrastructure facilities, the main emphasis has been directed towards solving urgent issues to avoid the threat of stopping the equipment, which could result in a blackout. Therefore, the implementation of asset management systems (EAM) becomes an integral part of the successful operation of enterprises in modern realities. The automated process of maintaining a database of equipment with detailed

characteristics helps in the search for analogs for energy equipment of substations, lines, etc., damaged as a result of military actions. In particular, the 220 kW autotransformer has more than 50 important characteristics. EAM helps to quickly find analogues of such equipment. The use of EAM in the energy industry is becoming a key element of the strategy that helps to optimize processes, increase reliability and ensure compliance with regulations that are important for successful operation in this industry [3].

The EAM system allows you to make quick and correct decisions even during military operations and large-scale destruction, thanks to an up-to-date and complete database of equipment and regulations and automated business processes. For example, if an infrastructure object is destroyed or equipment is damaged, the EAM system will provide reliable information about the equipment and its maintenance history, will allow effective planning and management of restoration work, or will provide analytics on the need for restoration. EAM systems help solve a number of challenges faced by managers of energy and civil infrastructure enterprises, both in peacetime and during war or other emergency events:

• create an inventory database of all assets such as buildings, equipment, vehicles, communication networks, roads, etc., damaged or destroyed during the war;

• create maintenance and repair plans for assets so that their functionality and reliability are restored as soon as possible;

• monitor the state of assets in real time and predict and detect possible problems in a timely manner;

• organize stocks and materials for asset recovery and repairs;

• effectively use resources, determine priorities and plan actions to restore assets;

• the ability to analyze data to make informed decisions and generate reports for control and reporting;

• monitor the costs of restoration and maintenance of assets, which is important for the efficient use of limited resources;

• store critical asset data and make it available for future recovery.

The field of energy during the war suffered unrealistic losses and in the future needs changes and reforms. For this, significant changes in the country's energy sector will be considered, it will have to modernize and become more mobile and stronger. This will have to be done not gradually, as in EU countries and the world, but at a fairly high pace.

## REFERENCES


1. https://jurliga.ligazakon.net/aktualno/12602_energetika-pd-chas-vyni-v-ukran-yak-zmni-v-regulyuvann.
2. Омельченко В. Сектор відновлюваної енергетики України до, під час та після війни. https://razumkov.org.ua/statti/sektor-vidnovlyuvanoyi-energetyky-ukrayiny-do-pid-chas-ta-pislya-viyny.
3. Енергетика під час війни: як системи управління активами надають ефективні рішення для енергетики. https://www.epravda.com.ua/publications/2024/01/29/709143/.

А.В. Ковилін

# ПОРІВНЯЛЬНИЙ АНАЛІЗ ЗАСТОСУВАННЯ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ В ЕНЕРГЕТИЧНИХ СИСТЕМАХ

Виявлення кіберзагроз та вчасне реагування – важлива функція кібербезпеки, метою якої є своєчасна ідентифікація потенційних загроз, що надає можливість реагувати на них до завдання шкоди інформаційним системам [1].

Кібератаки на енергетичні системи є серйозним викликом сучасного світу. Зловмисники активно використовують новітні технології і методи для проникнення в інформаційні системи, що мають пряме чи опосередковане відношення до керування виробництвом та розподілом енергії. Це може призвести до надзвичайних ситуацій, відключень електроенергії, матеріальних та репутаційних збитків. Зростання рівня цифровізації технологічних процесів ще більше загострює ситуацію [2].

З метою підвищення адаптивності та пришвидшення процесу виявлення потенційних загроз спеціалісти з безпеки комп'ютерних систем, кіберрозвідки, дата-аналітики або дослідники звертаються до методів штучного інтелекту й машинного навчання (ML), які на сьогодні вважаються найбільш перспективними для вирішення даних задач.

Одним з найпопулярніших застосувань ML у виявленні кіберзагроз є сфера threat hunting (полювання на загрози) [3]. Threat hunting передбачає проактивний підхід до ідентифікації ознак підозрілої активності в інформаційній інфраструктурі чи мережі організації (в тому числі на об’єктах критичної інфраструктури), а алгоритми машинного навчання, значно посилюють ці зусилля [4].

Традиційно системи кібербезпеки, засновані на сигнатурному методі, забезпечують більш чітке виявлення вторгнень та менший відсоток хибних тривог (false positive) порівняно з конкуруючими рішеннями. Але у випадку захисту об'єктів критичної інфраструктури підвищений рівень відповідальності таких систем вимагає здатності виявляти нові загрози, швидко адаптуватися до змін в оперативному оточенні та до появи нових підходів щодо здійснення кібератак [5].

Виявлення аномалій є поширеним підходом ідентифікації потенційних кібератак, що базуються на використанні ML. Він розглядає відхилення поведінки системи від стандартної як потенційну загрозу безпеці [4]. Аналізуючи логи системних журналів операційних систем, мережевий трафік або дії користувачів, підхід на основі аномалій знаходить певні закономірності, що можуть сигналізувати про кіберзагрозу [1].

Дана робота присвячена дослідженню потенційного використання алгоритмів виявлення аномалій таких як Isolation Forest, DBSCAN, Autoencoder для створення моделей що можуть допомогти спеціалістам з кібербезпеки швидко виявляти потенційні загрози. Описане рішення передбачає аналіз статистичних даних з використанням таких технологій як, Python, NodeJS, TypeScript.

Опис досліджуваних алгоритмів:

– **Isolation Forest** – алгоритм, заснований на формуванні кластерів («дерев») з точок даних. Заснований на припущенні, що аномальні точки даних завжди рідкісні і знаходяться далеко від центру нормальних кластерів. Завдяки чому має здатність розділяти точки даних на "нормальні" та "аномальні" [6].

– **DBSCAN** – алгоритм кластеризації, який групує дані на основі щільності, але може бути неефективним при різній щільності кластерів або при великій кількості шуму [7].

– **Autoencoders** – алгоритми, що використовуються для ідентифікації патернів або поведінок, які відрізняються від нормальної або очікуваної поведінки системи. Вони досягають цього, вивчаючи низьковимірне представлення даних [8].

Основні параметри методів наведені в таблиці 1.

Таблиця 1 – Переваги та недоліки технік виявлення аномалій на базі алгоритмів машинного навчання

| Алгоритм | Переваги | Недоліки |
|---|---|---|
| Isolation Forest | - Ефективність у виявленні аномалій;<br>- Незалежність від розподілу даних;<br>- Відносно швидкий у порівнянні з іншими методами виявлення аномалій | - Чутливість до параметрів;<br>- Можлива нестабільність при роботі з малими вибірками або складними даними; |
| DBSCAN | - Виявлення кластерів довільної форми;<br>- Здатність ідентифікувати шум;<br>- Не вимагає заздалегідь визначеного числа кластерів | - Чутливість до параметрів (epsilon, мінімальна кількість точок);<br>- Неефективність при різній щільності кластерів або великій кількості шуму;<br>- Висока обчислювальна складність при роботі з великими наборами даних; |
| Autoencoder | - Адаптивність до складних внутрішніх представлень даних;<br>- Гнучкість у налаштуванні для різних типів даних та задач;<br>- Виявляє аномалії як дані з високою помилкою реконструкції | - Потребує великої кількості даних для ефективного навчання;<br>- Чутливість до вибору параметрів навчання; |

В якості джерела даних було використано датасет приблизно на 40 тис строк від компанії Incribo, який містить оброблені дані про підозрілу активність в комп’ютерній мережі. За допомогою розробленого нами ПЗ що включало реалізацію вищезгаданих алгоритмів ML отриманий датасет подавався в якості вхідних даних для аналізу. В табл. 2 наведено результати порівняльного аналізу.

Таблиця 2 – Порівняльна таблиця результатів виявлення аномалій на базі алгоритмів машинного навчання

| Model | Precision | Recall | F1-Score | Anomalies Detected | AUC |
|---|---|---|---|---|---|
| Isolation Forest | 0,998204 | 0,998205 | 0,998204 | 3997 | 0,999936 |
| DBSCAN | 0,917355 | 0,090909 | 0,015152 | 44000 | NaN |
| Autoencoder | 0,960853 | 0,959091 | 0,953603 | 2200 | NaN |

Як можна побачити, Isolation Forest виявився найбільш ефективним алгоритмом для виявлення аномалій у представленому наборі даних.

**Висновок.** Високі значення precision, recall та F1-score, а також AUC, близький до 1, при використанні алгоритму Isolation Forest вказують на високу здатність алгоритму розрізняти нормальні та аномальні дані. Цей алгоритм показує найкращі результати для аналізу даних про кіберзагрози. DBSCAN виявився неефективним для даного набору даних. Високий рівень хибних спрацювань та низькі значення recall і F1-score свідчать про не високу здатність цього алгоритму до виявлення аномалій або високий рівень шуму. DBSCAN не підходить для використання у поточному контексті через його низьку ефективність. Autoencoder добре справляється з виявленням аномалій, але знаходить менше аномалій порівняно з Isolation Forest. Проте має високі значення precision і recall, що вказує на хорошу продуктивність моделі. Існує потенціал для подальшого вдосконалення цього алгоритму, щоб збільшити кількість виявлених аномалій без значного зниження точності.

Як бачимо у файлі даних з вже відомими атаками ми додатково знайшли декілька тисяч прикладів аномальної поведінки що показує застосування алгоритмів, таких як Isolation Forest та вдосконалені Autoencoder, може значно покращити ефективність виявлення та запобігання кіберзагрозам. А також що моделі машинного навчання розширюють можливості дата-аналітиків, спеціалістів з безпеки комп'ютерних систем та кіберрозвідки щодо виявлення підозрілої активності і вживання заходів з підвищення рівня захисту. Використання підходів машинного навчання для протидії кібератакам є перспективним напрямком у розвитку систем захисту інформації (в т.ч. на об'єктах критичної інфраструктури).

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Thakkar, A., & Lohiya, R. (2022). A survey on intrusion detection system: Feature selection, model, performance measures, application perspective, challenges, and future research directions. Artificial Intelligence Review, 55(1), 453–563. https://doi.org/10.1007/s10462-021-10037-9
2. С.Я. Гільгурт, А.В. Ковилін. Застосування алгоритмів машинного навчання для виявлення кіберзагроз в енергетичних системах. Збірник матеріалів XLII Науково-технічної конференції молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, м. Київ, 15 травня 2024 р. / ІПМЕ ім. Г.Є. Пухова НАН України. – 2024. – 171 с. https://ipme.kiev.ua/wp-content/uploads/2024/05/Матеріали-конференції-2024-v-2.pdf
3. Simion, C. P., Verdeș, C. A., Mironescu, A. A., & Anghel, F. G. (2023). Digitalization in energy production, distribu-tion, and consumption: A systematic literature review. Energies, 16(4), 1960. https://doi.org/10.3390/en16041960
4. Afrifa, S., Varadarajan, V., Appiahene, P., Zhang, T., & Domfeh, E. A. (2023). Ensemble machine learning techniques for accurate and efficient detection of botnet attacks in connected computers. Eng, 4(1), 650-664; https://doi.org/10.3390/ eng4010039
5. Гільгурт С.Я. НРС та реконфігуровні засоби підвищення резильєнтності кіберфізичних систем // Живучість та резильєнтність критичної інфраструктури – 2023: Матеріали міжнародної науково-практичної конференції, м. Київ, 19 жовтня 2023. – К. : ІПМЕ ім. Г.Є. Пухова НАН України, 2023. – С. 11-14. https://ipme.kiev.ua/wp-content/uploads/2023/11/Матеріали_конференції_ Survivability_and_Resilience-2023-4.pdf
6. Zhiguo Ding, Minrui Fei. (2013), An Anomaly Detection Approach Based on Isolation Forest Algorithm for Streaming Data using Sliding Window, 3rd IFAC International Conference on Intelligent Control and Automation Science. September 2-4, 2013. Chengdu, China. https://doi.org/10.3182/20130902-3-CN-3020.00044
7. Irving Cordova, Teng-Sheng Moh, DBSCAN on Resilient Distributed Datasets, High Performance Computing and Simulation. International Conference. 2015. (HPCS 2015) (CD-ROM). https://doi.org/10.3182/20130902-3-CN-3020.00044
8. Mironeanu, C., Archip, A., Amarandei, C. M., & Craus, M. (2021). Experimental cyber attack detection framework. Electronics, 10(14), 1682. https://doi.org/10.3390/ electronics10141682.

O. Ogir

# FROM RISK TO REWARD: IMPORTANCE OF COMPREHENSIVE COST-BENEFIT ANALYSIS OF ENERGY CYBERSECURITY

In today's interconnected world, where digital infrastructure forms the backbone of critical services like energy systems, ensuring robust cybersecurity measures is paramount. The cyber platform research projects emerges as a beacon of innovation, poised to revolutionize the landscape of energy system security. In this thesis, we explain stages and strategies the cost-benefit analysis, delving into the intricate financial considerations and potential value propositions while meticulously dissecting the associated investment costs.

Cost Analysis – Investment in Cybersecurity.

At the core of the cybersecurity platforms lies a strategic commitment to fortifying cybersecurity measures within energy systems. This multifaceted investment strategy encompasses:

- Deployment of cutting-edge encryption protocols to safeguard critical data and communications channels against unauthorized access and tampering. Implementation and continuous maintenance of sophisticated intrusion detection and prevention systems, capable of identifying and neutralizing evolving cyber threats in real-time.
- Ongoing investment in comprehensive employee training programs to cultivate a culture of cyber awareness and resilience, empowering personnel to detect and respond effectively to potential security breaches.

Failure to fortify energy systems against cyber threats exposes organizations to a myriad of dire financial repercussions, including direct financial losses arising from data breaches, ransomware attacks, and prolonged system downtime, which can disrupt essential services and incur substantial remediation costs and indirect costs such as reputational damage, regulatory fines, and legal expenses incurred in the aftermath of security incidents, which can tarnish brand credibility and erode stakeholder trust.

The dynamic and evolving nature of cyber threats necessitates a proactive approach towards risk mitigation. Quantifying the efficacy of cybersecurity investments entails grappling with inherent uncertainties and complexities. Central to this analysis is the concept of "expected cost savings," which hinges on estimating potential losses from cyber breaches and discerning the differential breach probabilities pre and post-investment. Despite the inherent challenges in quantifying these metrics, organizations stand to benefit immensely from proactive cybersecurity investments, mitigating the probability and severity of cyber incidents and their associated financial impact.

Measurement of Effectiveness of Cyber Security Controls is assessing the efficacy of cybersecurity controls requires a nuanced understanding of their impact on mitigating loss probability and enhancing overall security posture. Mere augmentation of control measures may not necessarily translate into improved

security outcomes if underlying strategies are flawed or misaligned with organizational risk mitigation objectives.

Organizations must adopt a holistic approach to cybersecurity, ensuring that controls are not only robust but also adaptive, responsive, and aligned with emerging threat landscapes and regulatory requirements.

Benefit Analysis. Derived Benefits from Cyber Security Investment:

The primary impetus behind cybersecurity investment lies in realizing future cost savings derived from the prevention of potential losses stemming from cyber breaches. Estimating these prospective losses necessitates a rigorous analytical framework, drawing upon methodologies such as Gordon and Loeb's model and Huang et al.'s expected utility theory to delineate the optimal level of investment.

By quantifying threat probabilities, potential losses, and risk aversion parameters, organizations can navigate the complex landscape of cybersecurity investment, optimizing resource allocation to maximize risk mitigation benefits and return on investment.

Measurement the Effectiveness of Cyber Security Controls is to recognize how a set of applied controls translates to a loss probability. The marginal development of adding one to a set of controls is already in operation. However, the proposal focuses on what a designated policy recommends, such as how many computers have an antivirus installed. What if the strategy is flawed, but the characteristics otherwise score thoroughly? That may lead an organization to be tricked into a false sense of security.

Derived Benefits from Cyber Security Investment. The first difficulty related to cybersecurity investments is recognizing and assessing the benefits derived from such investments.

The main benefits pertaining to cybersecurity investments are the future "cost savings" derived from the prevention of losses due to cybersecurity breaches [1]. However, if breaches were prevented, the actual losses would not occur and would not be observable. The better the security, the less an organization, will observe the losses resulting from cybersecurity breaches. Thus, organizations need to estimate the potential losses from cybersecurity breaches in order to evaluate the benefits derived from cybersecurity investments. Faced with an opportunity to invest in more protection, it is beneficial to understand how to calculate the benefits from security investments and get guidance on finding the optimal level to invest. Gordon and Loeb (2006) postulate that cost-savings result from the potential losses from incidents, the loss probability, and its reduction from an investment [2]. The authors propose an approach to determine the optimal level of investment by a loss probability function with an investment level and a vulnerability level. Expected losses are generated by threat probability and monetary losses to an asset. The calculation may be conducted without historical attack data; the investment level is the only decision variable. However, the vulnerability level and expected losses still need to be derived somehow. To compute the optimal security investment, the security team must determine the probability of a security incident occurring in each time frame, an investment level, a potential loss and a risk- aversion coefficient. The applied classical economic theories to compute an optimal security investment to

protect an asset. As an input, historical data to determine the loss probability are needed and a risk- aversion coefficient [2].

And in Conclusion we can say that the cybersecurity platforms research projects represents a paradigm shift in fortifying energy systems against the omnipresent threat of cyber-attacks. While the initial investment costs may appear daunting, the long-term benefits in terms of mitigated losses, enhanced security posture, and organizational resilience justify these expenditures manifold. Moreover, the imperative to continuously evaluate and optimize cybersecurity controls underscores the dynamic nature of this domain. By embracing a proactive stance towards cybersecurity and leveraging innovative technologies and strategies, organizations can not only safeguard critical infrastructure but also foster a culture of resilience and innovation in the face of evolving cyber threats.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Zhou, L. (2015) Externalities and the Magnitude of Cybersecurity Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. Journal of Information Security, 6, 24–30. https://www.scirp.org/pdf/JIS_2015010710521369.pdf.
2. L. Gordon, M, Loeb, and Zhou, L. "Investing in Cybersecurity: Insights from the Gordon-Loeb Model." Journal of Information Security, 2016. 7, 49-59. doi: 10.4236/jis.2016.72004
   https://www.scirp.org/journal/paperinformation?paperid=64892.

О.М. Безуглий

# МЕТОДОЛОГІЯ ВИЯВЛЕННЯ ПОЗАШТАТНИХ СИТУАЦІЙ У КРИТИЧНІЙ ІНФРАСТРУКТУРІ

У сучасних умовах підвищеного ризику для критичної інфраструктури необхідно розробляти нові підходи до забезпечення її резильєнтності та живучості. Одним із перспективних методів є використання сучасних технологій та засобів масової інформації для збору даних і моніторингу подій на певних територіях. У даній статті пропонується аналіз ефективності використання телеграм-каналів та місцевих друкованих ЗМІ для моніторингу стану критичної інфраструктури та оперативного реагування на виниклі загрози.

## Вступ

Критична інфраструктура відіграє ключову роль у забезпеченні життєдіяльності суспільства. Її резильєнтність та живучість визначаються здатністю системи витримувати та швидко відновлюватися після зовнішніх ударів. В умовах зростаючих загроз, таких як природні катастрофи, техногенні аварії та терористичні акти, необхідно використовувати нові підходи для моніторингу стану інфраструктури. Телеграм-канали та місцеві друковані ЗМІ можуть стати ефективними інструментами для збору оперативної інформації та аналізу ризиків.

## Актуальність

Сучасні інформаційні технології відкривають нові можливості для моніторингу та управління критичною інфраструктурою. Телеграм-канали дозволяють швидко отримувати інформацію від великої кількості користувачів, що сприяє оперативному виявленню проблем та реагуванню на них. Місцеві друковані ЗМІ, у свою чергу, є джерелом достовірної інформації, що може бути використана для довгострокового аналізу та планування. Таким чином, інтеграція цих двох джерел інформації може значно підвищити ефективність управління критичною інфраструктурою.

## Методика збору даних

Для збору даних про стан критичної інфраструктури в прикордонній смузі України з Білоруссю та РФ було обрано кілька ключових джерел інформації зокрема телеграм-канали, що спеціалізуються на новинах з цих регіонів.

До моніторингу було включено телеграм-канали, що наведені у таблиці 1.

Таблиця 1 – Телеграм Канали для моніторингу

| | Місцеві | Схід | Північ |
|---|---|---|---|
| ТГ канали | "Харків 1654","Чернігів Оперативний", "Суми Інформ", "Північний Офіс" | "Военный Осведомитель", "Белгородские новости", "Брянск Today", "Курск Инфо", | "Білоруський Гаюн", "Минск Новости", "Гомельская правда", "БелТА", |

Для моніторингу стану критичної інфраструктури в прикордонній смузі України було обрано низку телеграм-каналів. Практична користь цих каналів полягає в їх здатності надавати оперативну інформацію в режимі реального часу від широкого кола користувачів та місцевих журналістів, що дозволяє швидко виявляти та реагувати на події, які можуть впливати на безпеку та функціонування критичної інфраструктури. Зокрема, телеграм-канали можуть миттєво повідомляти про інциденти, такі як аварії, обстріли чи військові переміщення, забезпечуючи своєчасний збір даних для подальшого аналізу та вжиття заходів з мінімізації ризиків.

**Процедура збору та обробки даних**

Для ефективного збору даних з телеграм-каналів застосовується спеціалізоване програмне забезпечення — телеграм парсер. Цей інструмент автоматично збирає та аналізує повідомлення з обраних каналів, використовуючи налаштовані ключові слова. Процес роботи телеграм парсеру включає кілька основних етапів: спочатку парсер підключається до визначених телеграм-каналів, потім у реальному часі відслідковує та фільтрує всі повідомлення за заданими ключовими словами. Відповідні повідомлення зберігаються у базі даних для подальшого аналізу.

Ключові слова підбираються таким чином, щоб максимально охопити тематику критичної інфраструктури та пов’язаних з нею інцидентів. Наприклад, для моніторингу стану критичної інфраструктури в прикордонній смузі України з Білоруссю та РФ використовуються такі ключові слова:

"аварія" - для виявлення повідомлень про техногенні інциденти.

"обстріл" - для фіксації інформації про обстріли та інші воєнні дії.

"пошкодження" - для збору даних про будь-які пошкодження інфраструктурних об'єктів.

"перебої з електропостачанням" - для моніторингу проблем з електроенергією.

"відключення водопостачання" - для виявлення проблем з водопостачанням.

"залізниця" - для відслідковування інцидентів на залізничних коліях.

"газопостачання" - для фіксації повідомлень про проблеми з газопостачанням.

"мост" - для виявлення інформації про стан мостів та їх пошкодження.

"перекриття дороги" - для відслідковування перекриття автомобільних доріг.

Наприклад, парсер налаштований на ключове слово "обстріл" здатен в реальному часі виявити повідомлення типу: "Сьогодні вранці відбувся обстріл об'єктів інфраструктури в Сумській області", що дозволить оперативно реагувати на подію та вживати необхідні заходи для мінімізації її наслідків. Такий підхід забезпечує високу ефективність моніторингу та управління критичною інфраструктурою в умовах підвищеної небезпеки.

Для підтвердження достовірності даних з телеграм-каналів інформація перевірялася через місцеві друковані ЗМІ та офіційні джерела, такі як прес-служби обласних адміністрацій та державних установ. Це дозволило забезпечити високу надійність отриманих даних та уникнути поширення непідтвердженої інформації.

**Висновки**

Результати показали, що використання телеграм-каналів дозволяє значно підвищити оперативність отримання інформації про стан критичної інфраструктури, тому застосування телеграм-каналів для моніторингу критичної інфраструктури є ефективним підходом, що дозволяє підвищити резильєнтність та живучість систем. Інтеграція оперативних та надійних джерел інформації створює умови для швидкого виявлення проблем та прийняття адекватних заходів реагування. Подальші дослідження в цьому напрямку можуть включати розробку алгоритмів автоматичного аналізу даних та створення систем підтримки прийняття рішень на основі отриманих результатів.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Каплун, В. А., та ін. (2018). "Резильєнтність критичної інфраструктури: основні аспекти та підходи." Інфраструктурний розвиток, 3(1), 45-56.
2. Тарасов, І. В., та Бєляєв, П. Ю. (2020). "Використання інформаційних технологій для моніторингу критичних об'єктів." Журнал безпеки та ризик-менеджменту, 6(2), 90-104.
3. Smith, J., & Jones, A. (2021). "Telegram Channels as a Tool for Real-Time Data Collection in Critical Infrastructure Monitoring." International Journal of Information Systems, 15(4), 210-225.

С.М. Дяченко

# МОДЕЛЮВАННЯ ЗБІРНОГО УЛЬТРАЗВУКОВОГО СОНОТРОДУ З ТОЧКИ ЗОРУ ПЕРЕДАЧІ ПРУЖНОЇ МЕХАНІЧНОЇ ЕНЕРГІЇ

При роботі ультразвукового технологічного обладнання велика роль відводиться сонотроду, як елементу який узгоджує передачу пружної механічної енергії між джерелом цієї енергії та об'єктом технології [1]. В даній роботі розглядається узгодження сонотроду в вигляді «чаші» який має власний резонанс з яскраво вираженими згинальними рухами бічної поверхні рис.1.

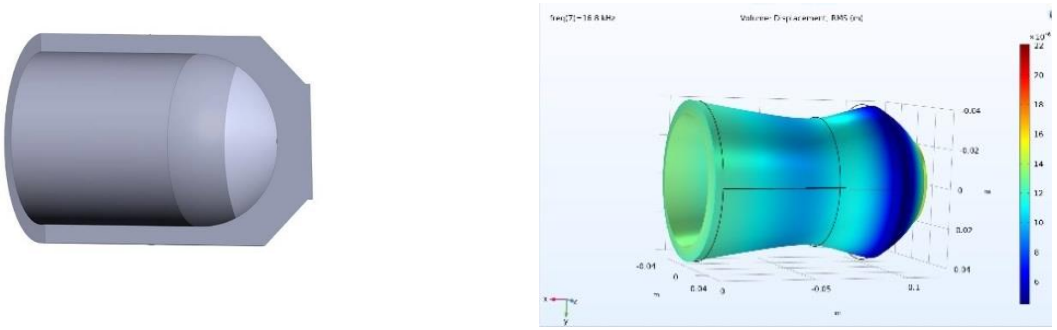


Рисунок 1 – Зовнішній вигляд «сонотроду-чаші».
Розріз та мода коливання на резонансі

Задача даного сонотроду є передача пружної енергії до технологічного середовища, яке розташовується всередині «чаші» [2]. Моделюванню підлягають три варіанти збірного сонотроду: який виконується з'єднанням «чаші» з стержневим ступінчастим сонотродом. Якщо він приєднується до «чаші» торцем з малим діаметром, будемо називати такий збірний сонотрод – пряме з'єднання, а торцем з великим діаметром, будемо називати – зворотне з'єднання та третій варіант, сонотрод стержневий постійного діаметру, що дорівнює вхідному діаметру «чаші». Збірний сонотрод збуджується гармонійною силою постійної амплітуди, яка рівномірно розподілена на поверхні вхідного торця, тобто вільного торця збірного сонотроду. Методика побудови збірного сонотроду будується на принципі однакових порційних власних частот окремих сонотродів [3].

Модель збірного сонотроду має властивості матеріалу титанового сплаву, де використовуються такі параметри як: модуль Юнга, коефіцієнт Пуассона, щільність матеріалу. В моделі враховується дисипативні властивості матеріалу через модель демпфірування Релеєвського типу – на двох частотах коливання збірного сонотроду задано коефіцієнти демпфірування - 0,03.

На рис.2. показано частотна характеристика щільності пружної енергії деформації для прямого збірного сонотроду.

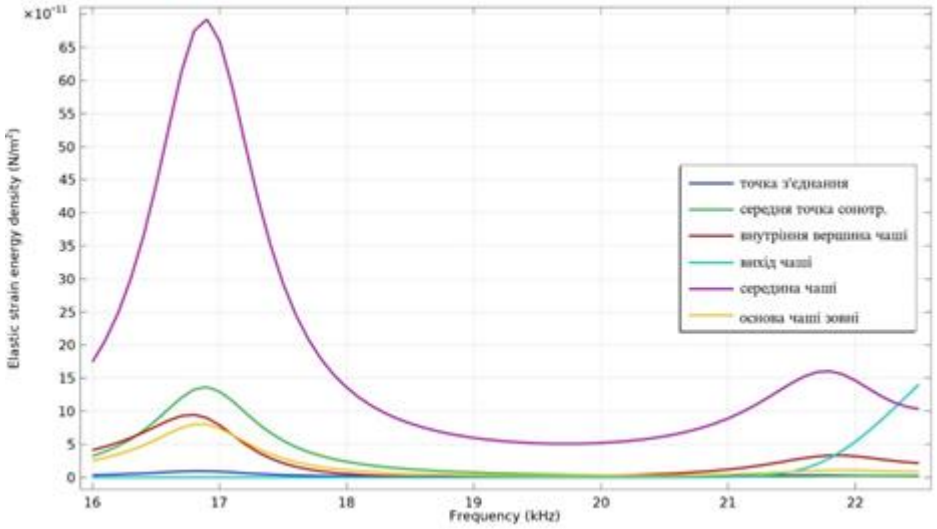



Рисунок 2 – Частотна характеристика щільності пружної енергії деформації для прямого збірного сонотроду

Ці частотні характеристики якісно відповідають всім трьом збірним сонотродам. Ці криві показують, що сонотроди мають резонансний тип коливання та що щільність пружної енергії деформації концентруються в зоні ємності «чаші».

На рис. 3, 4, 5 показано розподілення щільності пружної енергії деформації по координаті збірних сонотродів в зоні резонанса.

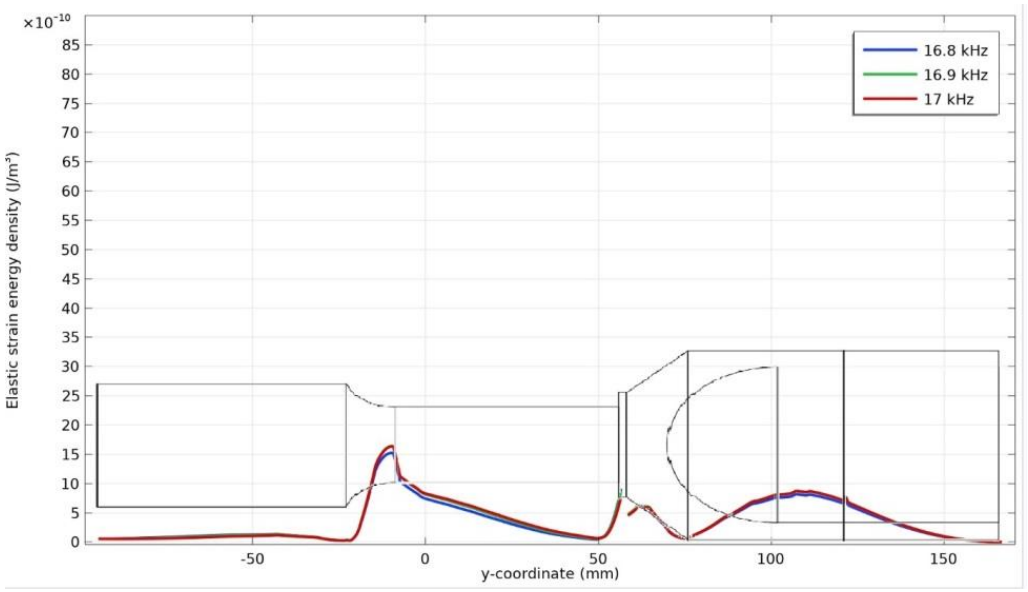



Рисунок 3 – Розподілення щільності пружної енергії деформації по координаті збірного сонотроду прямого з’єднання

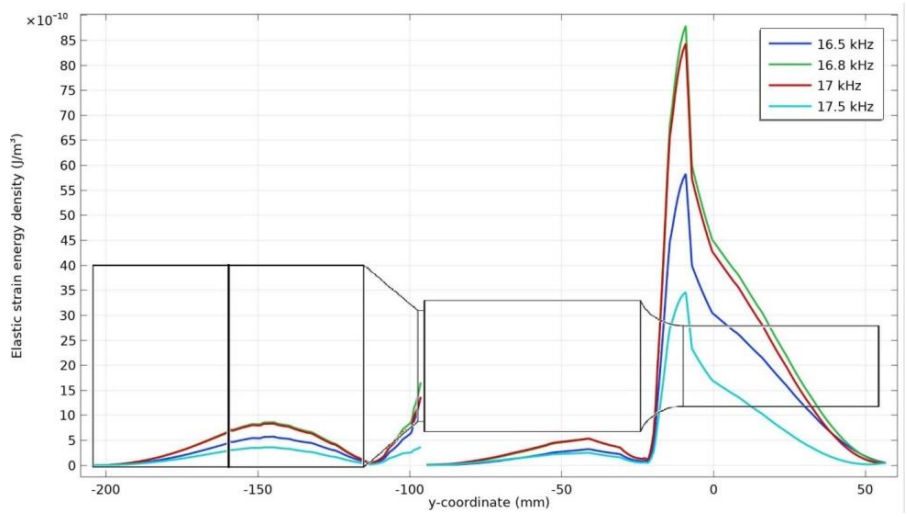



Рисунок 4 – Розподілення щільності пружної енергії деформації по координаті збірного сонотроду зворотного з’єднання

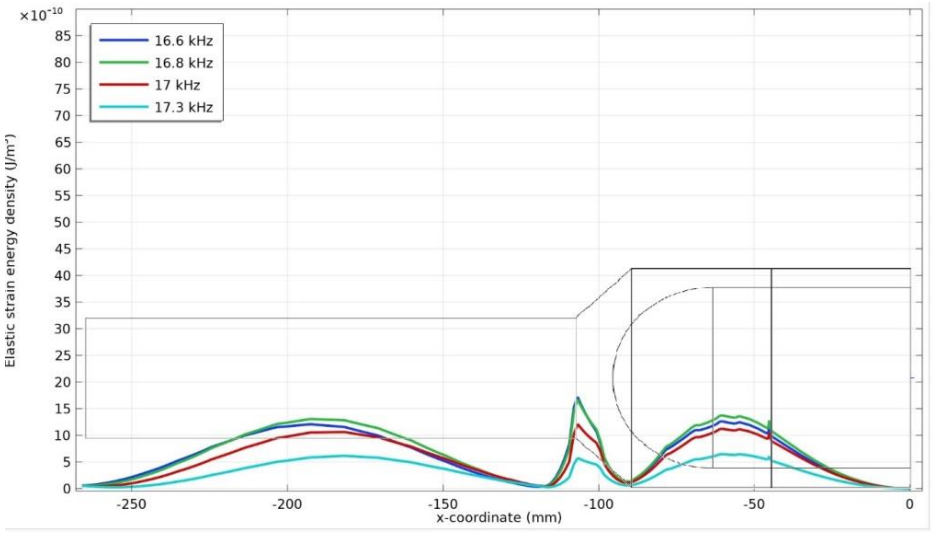



Рисунок 5 – Розподілення щільності пружної енергії деформації по координаті збірного сонотроду з сонотродом постійного діаметру

**Висновки.**

Розподілення пружної енергії по координаті показують, що варіант збірного сонотроду з циліндром постійного діаметру має неперервне розподілення по координаті. Максимальні значення трьох екстремумів: в зоні «чаші», зоні з’єднання простих сонотродів та в сонотроді постійного діаметру. Розподілення енергії в сонотроді з зворотним з’єднанням має великий стрибок значення в зоні переходу діаметрів в стрижневому сонотроді. Варіант с постійним діаметром стрижневого сонотрода має більше значення енергії пружної деформації в зоні «чаші» приблизно в 1,5 рази. З точки зору досягнення концентрації пружної енергії в зоні «чаші», переважним є варіант з сонотродом з постійним діаметром.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. И.К. Сенченков. Модальная классификация и проектирование сонотродов для ультразвуковой обработки материалов.//Акустичний вісник. 1998.Т.1 №4 С.55-64/
2. Ультразвуковий сонотрод-концентратор – для поверхневого зміцнення деталей : пат. 155254 Україна : B24B 1/04, B24B 31/06 / С.М. Дяченко, Т.А. Красовський.— № u 2023 04802 ; заявл. 12.10.2023 ; опубл. 31.01.2024, Бюл. № 5.
3. Дяченко С.М. Задача моделювання характеристик складного збірного сонотроду для ультразвукового зварювання полімерів. Матеріали науково-практичної конференції «Кібербезпека енергетики» .Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України : матеріали, 27 травня 2022 р. Київ : ІПМЕ ім. Г.Є.ПуховаНАН України, 2022. 129 с.

М.Р. Неізвєсна, А.Д. Данилов

# АНАЛІЗ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Об'єкти критичної інфраструктури, такі як електростанції, транспортні мережі, телекомунікаційні системи, є серцем нашого суспільства та економіки. Їх неперервна робота є життєво важливою для забезпечення безпеки та комфорту громадян.

З урахуванням зростаючої кількості атак та загроз суверенітету держави, захист цих об'єктів та їх інформації стає надзвичайно важливим завданням. Незабезпечення адекватного захисту може призвести до серйозних наслідків, таких як руйнування критичних об'єктів інфраструктури, припинення надання життєво важливих послуг для населення і держави, та безпосередню небезпеку для життя людей. Наприклад, інфраструктура енергетичних систем охоплює різноманітні об'єкти, мережі та активи, необхідні для виробництва, передачі, розподілу та управління енергетичними ресурсами, як відновлюваними, так і невідновлюваними. Функціонування сучасного суспільства значною мірою залежить від цієї інфраструктури, що робить її надійність, стійкість і безпеку вирішальними.

Загрози безпеки для таких об'єктів переважно виникають через існуючі вразливі місця у апаратних або програмних ресурсах, які можуть бути використані для впровадження непередбачених змін у надані послуги та відхилення від їх звичайної поведінки. Ці недоліки можна розділити на дві категорії: внутрішні та зовнішні. Внутрішня помилка відповідає за аномальні зміни, які відбуваються всередині системи. Зовнішня помилка пов'язана з впливами зовні, такими як природні явища, зловмисні дії або аварії. Зловмисні дії також можуть призвести до порушення конфіденційності та цілісності інформації, яка циркулює на даних об'єктах, що зможе сприяти подальшим загрозам припинення діяльності об'єкту критичної інфраструктури або його втрати у цілому.

Основні заходи кіберзахисту інформації критичних інфраструктур, що повсюдно використовуються в Україні, можна поділити на п'ять класів: ідентифікація ризиків, кіберзахист, виявлення кіберінцидентів, реагування на кіберінциденти.

До класу заходів кіберзахисту "Ідентифікація ризиків" належать такі дії, як управління активами, формування обов'язків персоналу щодо забезпечення кібербезпеки, формування правил, процедур і процесів для управління й моніторингу, оцінка ризиків, визначення пріоритетів, обмежень, допустимого рівня ризику для підтримки рішень щодо зниження ризиків кібербезпеки, управління ризиками системи постачання.

До класу заходів кіберзахисту "Кіберзахист" належать такі дії, як управління ідентифікацією, автентифікацією та контроль доступу, забезпечення інформування та обізнаності організації та партнерів організації щодо питань кібербезпеки, забезпечення управління та захисту інформації та документації,

забезпечення підтримання та управління політикою безпеки, технічне обслуговування та регулярний ремонт компонентів системи управління виробничими процесами, управління технологіями кіберзахисту метою забезпечення безпеки та стійкості систем і активів організації з дотриманням правил, процедур з безпеки.

До класу заходів кіберзахисту “Виявлення кіберінцидентів” належать такі дії, як своєчасне виявлення аномальної активності та передбачення потенційного впливу кіберінцидентів, безперервний моніторинг кібербезпеки, підтримання і тестування процесів й процедур виявлення кіберінцидентів.

До класу заходів кіберзахисту “Реагування на кіберінциденти” належать планування реагування на кіберінциденти, координація заходів з реагування між внутрішніми та зовнішніми партнерами об’єкту критичної інфраструктури, проведення аналізу кіберінцидентів, мінімізація наслідків, удосконалення заходів з реагування.

До класу заходів кіберзахисту “Відновлення стану кібербезпеки” належать планування відновлення, удосконалення процесів відновлення, комунікації про відновлення з внутрішніми та зовнішніми партнерами організації.

Для впровадження цих заходів використовуються різні методи захисту інформації. Для забезпечення контролю доступу зазвичай встановлюють огорожу по периметру, шлагбауми, камери для запобігання несанкціонованому доступу та використовують датчики та сигналізації для виявлення несанкціонованого проникнення. Рекомендуються засоби ідентифікації та автентифікації у вигляді використання біометричних сканерів та карт-рідерів для обмеження доступу лише для авторизованого персоналу.

Віддалений доступ слід дозволяти лише через VPN. Також для забезпечення захисту обов’язково впровадження брандмауерів, автоматичних систем виявлення вторгнень і систем запобігання вторгненням для захисту мережевої інфраструктури, ведення журналу подій за допомогою інструментів SIEM, які відповідають передовим міжнародним стандартам. Компанії реалізують криптостійке шифрування конфіденційної інформації для захисту від несанкціонованого доступу під час передачі та зберігання, виконують криптографічну перевірку збережених даних та блокують неавторизованих осіб від доступу до них. Можливі атаки, такі як Man-in-the-middle, дамп пам’яті, виконання помилкових команд для активації/деактивації критичних активів, модифікація значень стану або критичних процесів повинні бути передбачені та визначені політикою безпеки.

Для підвищення та посилення рівня безпеки у сучасному світі та реаліях, доцільно використовувати більш технологічні та інноваційні методи захисту. Наприклад, має сенс впровадження сучасних технологій спостереження: використання безпілотних літальних апаратів та дронів, і аналіз та/або апскейлінг відеоданих за допомогою штучного інтелекту для покращеного моніторингу. Здатність отримувати семантичні концепції з безперервної обробки відеопотоку в режимі реального часу призвела до дослідження таких рішень для підвищення безпеки роботи критичної інфраструктури від зловмисників.

За результатами проведеного аналізу проблемної галузі були сформовані наступні висновки – захист енергетичних об’єктів є постійним процесом, що вимагає постійної оцінки та адаптації до нових загроз і вразливостей. Будь-яка атака або компрометація системи може спричинити внутрішній ефект, який може призвести до згортання важливих служб і дій для контролю. Співпраця між різними секторами та міжнародними партнерами є вирішальною для ефективного захисту критичної інфраструктури.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Наказ адміністрації державної служби спеціального зв’язку та захисту інформації України «Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури» №601 (2021, 6 жовтня). *Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури,* 11-14.
2. Sylvia Bach. (2020). Ethical, legal, and social implications of projects. У Habtamu Abie, Davide Ferrario, Ernesto Troiano, John Soldatos, Fabrizio Di Peppo, Aleksandar Jovanović, Ilias Gkotsis, Evangelos Markakis (Ред.), *Consolidated Proceedings of the first ECSCI Workshop on Critical Infrastructure Protection*. (с. 33-34). https://ec.europa.eu/newsroom/cipr/items/752425/en.

К.Ю. Писаренко, А.Д. Данилов

# ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ВІД КІБЕРЗАГРОЗ

Захист критичної інфраструктури від кіберзагроз – ключове питання сучасного світу, що стосується безпеки критично важливих систем та об'єктів, які є життєво необхідними для нормального функціонування суспільства та економіки. До критичної інфраструктури належать такі сектори: енергетика, транспорт, телекомунікації, фінанси та охорона здоров'я, де захист від кіберзагроз стає все більш нагальним і складним завданням.

Проблема захисту критичної інфраструктури включає в себе ряд важливих аспектів:

− складність технічних систем, які можуть бути застарілими або побудованими на різних стандартах, що робить їх вразливими до кібератак;

− великий обсяг даних, які потрібно обробляти і захищати в реальному часі, що може бути складною задачею;

− глобальність і мобільність, певні частини критичної інфраструктури можуть бути розташовані у різних місцях або використовувати мобільні технології, що робить їх більш вразливими;

− необхідність постійного доступу, та брак координації і співпраці або брак фінансування також становлять великий ризик до вразливості.

Швидке зростання кількості та складності кіберзагроз потребує швидкого реагування для підтримки функціонування критичної інфраструктури. Ці проблеми вимагають комплексного підходу до захисту, який включає: технічні, організаційні, правові та соціальні заходи. Для покращення захисту критичної інфраструктури варто звернути увагу на кілька важливих аспектів:

1 оцінка ризиків та вразливостей: визначення ключових загроз та факторів ризику шляхом комплексного аналізу потенційних кіберзагроз та вразливостей систем критичної інфраструктури;

2 формулювання стратегії безпеки: розробка можливих сценаріїв кібератак та формулювання стратегії безпеки, що включає технічні, організаційні та правові заходи;

3 впровадження стратегії безпеки: впровадження сучасних засобів виявлення та запобігання кібератакам, шифрування даних, контролю доступу, тощо;

4 організаційні заходи: підвищення кваліфікації персоналу, розробка та впровадження політики безпеки, регулярні тренінги та аудити;

5 законодавчі та регуляторні заходи: розробляти, та впроваджувати відповідне законодавство, та нормативно-правові акти для забезпечення відповідальності за захист критичної інфраструктури;

6 моніторинг та аналіз: постійний моніторинг ситуації з кібербезпекою, та аналіз інцидентів і вразливостей для забезпечення своєчасного реагування, та вдосконалення заходів захисту;

7 міжнародна співпраця: співпрацювати з іншими країнами та міжнародними організаціями для обміну інформацією про кіберзагрози, та спільного реагування;

8 інновації: використання новітніх, таких як штучний інтелект, блокчейн, квантові обчислення, та інші інновації у сфері кібербезпеки.

Ці аспекти взаємодіють між собою і в сукупності дозволяють створити ефективну систему захисту критичної інфраструктури від кіберзагроз. Порушення критичних систем і основних послуг може призвести до значних економічних втрат. Аварії, терористичні атаки та кібератаки можуть мати каскадний негативний вплив на всі галузі нашого життя.

Підвищення стійкості критичної інфраструктури є необхідною задачею функціонування держави. Основним призначенням об’єктів критичної інфраструктури країни є створення необхідних умов для реалізації основних потреб людини та виконання основних функцій держави в умовах мирного, надзвичайного, воєнного стану та війни.

Пропонується визначати важливість того чи іншого об’єкта на основі ступеня його впливу на виробництво супутніх товарів і послуг, на виконання функцій, що забезпечують життєдіяльність індивідів та країн.

Відсутність критичних об’єктів інфраструктури всередині країни або нестабільність діяльності, може становити загрозу національній безпеці.

У цьому контексті розробка національних систем безпеки для об’єктів критичної інфраструктури є перш за все відповідальністю влади.

Розглянуте питання є особливо актуальним у ситуаціях гібридної війни, коли будь-яка сторона може бути схильна до терористичних загроз. Його вирішення має бути одним із перших у порядку денному.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Five Key Guidelines To Protect Critical Infrastructure From Cyber Threats. URL: https://www.linkedin.com/pulse/five-key-guidelines-protect-critical-infrastructure-from-cyber (дата звернення: 05.03.2024).
2. Critical Infrastructure Protection. URL: https://www.gao.gov/products/gao-23-105468 (дата звернення: 05.03.2024).
3. Cyber Security Critical Infrastructure Protecrion. URL: https://link.springer.com/book/10.1007/978-3-030-91293-2 (дата звернення: 05.03.2024).

А.О. Аксюк

# ОРГАНІЗАЦІЯ ДІЯЛЬНОСТІ МИТНИХ СКЛАДІВ В УКРАЇНІ

Компанії, що імпортують або експортують товари, часто орендують склади для тимчасового зберігання товарів. Однак у більшості випадків це не є розумним. Це пов'язано з тим, що вони повинні платити певну плату. Відповідно до норм Митного кодексу України (далі – МКУ), підприємство має право на створення та використання складу для тимчасового зберігання товарів або митного складу. Часто майбутнім операторам складів ставлять питання про їх схожість у суті та наявність принципових відмінностей, оскільки ці поняття часто сплутуються. Для виявлення відмінностей між ними проводиться аналіз (табл.1).

Таблиця 1 – Відмінності між митним складом та складом тимчасового зберігання

| Критерії відмінності | Склад тимчасового зберігання | Митний склад |
|---|---|---|
| Товари, що розміщуються | Не поміщені у жоден з Митних режимів | Поміщені у митні режими митного складу, транзиту, тимчасового ввезення або вивезення, переробки на митній території або за її межами, експорту |
| Хто може розміщати | Будь-які особи | Особи, що уклали договір з учасником або утримувачем складу |
| Строки зберігання | Не більше 90 календарних днів (з врахуванням терміну зберігання товарів) | Не більше 1095 календарних днів (з врахуванням терміну зберігання товарів |
| Операції з товарами | Створення оптимальних умов зберігання | Створення оптимальних умов зберігання, передача майнових прав, продаж, вивезення за межі складу за необхідності |
| Митні процедури | Не можуть проводитися | Можуть проводитися |

Обидва види складів призначені для тимчасового зберігання товарів під митним контролем. Однак, згідно зі статтею 437 МКУ, склад тимчасового зберігання – це належно облаштоване приміщення або територія, що використовуються для зберігання товарів під митним контролем до їх поміщення у митний режим. У свою чергу, відповідно до статті 424 МКУ, митний склад використовується для тих самих товарів, якщо вони вже перебувають у митному режимі митного складу. Однаковим для обох типів складів є можливість їхня класифікація як закритого або відкритого. Згідно зі статтею 437 МКУ, закритий склад тимчасового зберігання призначений лише для зберігання товарів, що належать утримувачу складу, тоді як на відкритому складі можуть зберігатися товари будь-яких осіб. Згідно з тією ж статтею, на закритому митному складі можуть бути збережені товари осіб, які уклали угоду з утримувачем цього складу, або об’єднанням підприємств, учасником якого є

утримувач складу. У відкритому складі, згідно з такою ж статтею, товари дозволено розміщувати особам, які уклали договір з утримувачем визначеного складу або іншими особами.

Оскільки товари на складі тимчасового зберігання не перебувають у жодному конкретному митному режимі, термін їх зберігання визначається згідно зі статтею 204 МКУ і становить 90 календарних днів. У випадку, коли товари зберігаються на митному складі, це свідчить про їх вже введення у відповідний митний режим. Відповідно до статті 125 МКУ, строк зберігання таких товарів не повинен перевищувати 1095 днів з моменту їхнього поміщення у митний режим митного складу. У обох випадках товари, які мають обмежений термін зберігання чи швидко втрачають свої корисні якості, можуть перебувати на складах протягом встановленого законодавством терміну, за умови, що він не перевищує встановлені строки. Однак, виняток становлять товари, термін придатності яких закінчується менше ніж за один місяць – їхнє розміщення на складах тимчасового зберігання заборонено. Згідно зі статтею 203 МКУ, на складі тимчасового зберігання можуть проводитися лише маніпуляції, пов’язані з створенням оптимальних умов для зберігання розміщених товарів: огляд, вимірювання, усунення пошкоджень упаковки, взяття проб, сортування, пакування, маркування, навантаження та вивантаження, захист від корозії, боротьба зі шкідниками, провітрювання, чистка, інвентаризація тощо.

Також на митному складі дозволяється проводити усі перелічені процедури, проте існує відмінність. Згідно зі статтею 127 МКУ, з дозволу органу доходів і зборів та за умови надання фінансової гарантії, товари, які перебувають у митному режимі митного складу, можуть тимчасово вивозитися з митного складу на строк, обумовлений метою такого вивезення, але не більше ніж на 45 днів. Розміщення у митному режимі “митний склад” товарів, які поміщені в інші митні режими для їх зберігання, перевантаження або дозавантаження, здійснюється на основі митних декларацій, відповідних митних режимів (транзиту, тимчасового ввезення, переробки на митній території, експорту, тимчасового вивезення, переробки за межами митної території). На митному складі можуть поміщатися товари, термін зберігання яких перевищує 90 днів, за винятком [2]:

1. товарів, які заборонені для експорту, імпорту та транзиту;
2. товарів, у яких закінчився термін придатності;
3. товарів гуманітарної допомоги;
4. живих тварин;
5. електроенергії, що переміщується лініями електропередачі.

На митному складі можуть виконуватися складські операції, пов’язані із забезпеченням умовзберігання товарів, які у ньому розміщені. Такі операції необхідно здійснювати із дотриманням заходів щодо забезпечення цілісності

характеристик товару відповідно до коду Української класифікації товарів зовнішньоекономічної діяльності. До таких операцій належать [2]:

1. переміщення товарів у межах складу з метою їх раціонального розміщення;
2. чищення;
3. провітрювання;
4. створення оптимального температурного режиму зберігання;
5. сушіння;
6. захист від корозії;
7. боротьба зі шкідниками;
8. інвентаризація.

Для спрощення митних процедур митні органи України активно впроваджують механізм електронного декларування. Цей механізм суттєво зменшує вартість, прискорює процес митного оформлення та підвищує ефективність митного контролю. Митне оформлення є необхідною умовою для застосування заходів тарифного і нетарифного регулювання. Питання ефективності митного оформлення мають велике значення у зовнішньоекономічній діяльності, оскільки вони безпосередньо впливають на обсяги експорту та імпорту.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Кормич Б. А., Біленець Д. А. (2017). Режим зони митного контролю: адміністративно-правові основи: монографія. Чернівці: Технодрук. 180 с.
2. Любін Н. М. (2016). Прагматизм митного оформлення товарів та інших предметів, що переміщуються через митний кордон України. Державне управління: удосконалення та розвиток, № 5. 93 с.
3. Наказ Міністерства фінансів України № 835 від 16.07.2012 р. “Про затвердження Порядку надання складським об’єктам статусу “митний склад” та позбавлення такого статусу” URL: https://zakon.rada.gov.ua/laws/show/z1324-12#Text.
4. Титор В. Й. (2019). Митний контроль та митне оформлення транспортних засобів // Економіка та митно-правові відносини, Вип. 11–12, червень–серпень. 66 с.

З.Х. Борукаєв, В.А. Євдокімов, К.Б. Остапченко, Д.Р. Цвілій

# ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ КОМП'ЮТЕРНОЇ СИСТЕМИ МОДЕЛЮВАННЯ ПРОЦЕСІВ ЦІНОУТВОРЕННЯ НА РИНКУ ЕЛЕКТРОЕНЕРГІЇ

Реалізація положень Закону про ринок електричної енергії України вимагає створення ефективних умов функціонування учасників нової моделі лібералізованого ринку електричної енергії і запровадження доступної для багатьох його учасників спеціалізованої інноваційної комп'ютерної системи моделювання (КСМ) процесів функціонування енергокомпаній і підприємств-споживачів, яка дозволить здійснювати комплексний аналіз їх поведінки на сегментах цього ринку.

Процес створення комп'ютерної системи у галузі енергетики потребує критичного та аргументованого відбору програмних платформ і апаратних засобів з урахуванням перспектив удосконалення технологій проведення розрахунків, зростання обсягів даних, що використовуються, розвитку обчислювальних потужностей і засобів зберігання даних [1].

Основною метою створення КСМ є підвищення ефективності і оперативності функціонування суб'єктів ринку при проведенні торгів за рахунок визначення ризиків та оптимальних стратегій учасників сегментів ринку на підставі агентно-орієнтованого моделювання процесів поведінки учасників в умовах лібералізованого ринку і конкурентного відбору пропозицій виробників, здійснення оцінки мінімально можливих цін і тарифів, виходячи з витрат, які можуть бути понесені учасниками ринку електричної енергії із використанням сучасних інноваційних технологій [2].

КСМ є середовищем проектування та побудови комп'ютерних моделей об'єктів та процесів функціонування ринку, що включає:

- засоби математичного формального опису досліджуваних складних об'єктів та процесів взаємодії складових їх структурних елементів між собою та зовнішнім середовищем;
- єдиний інформаційний простір, що поєднує засоби концептуального та інформаційного моделювання процесів взаємодії складових її структурних елементів між собою та зовнішнім середовищем;
- уніфіковану систему класифікаторів та довідників, структуру зберігання даних, єдину систему протоколів та інтерфейсів;
- сукупність програмно-технічних засобів, що забезпечують функціонування їх як єдиного комплексу.

Програмне забезпечення КСМ поділяється на системне, інструментальне та прикладне. Системне забезпечення призначене для організації роботи апаратно-технічних засобів КСМ і складає:

- операційні системи серверів, сервісів і комунікаційних засобів;
- операційні системи ЕОМ робочих місць користувачів.

До складу інструментальних засобів КСМ має входити засоби обробки запитів і даних, що надходять до системи із зовнішнього по відношенню до

структуроутворюючих систему компонентів Internet-середовища, де знаходяться клієнти-користувачі КСМ. Основними такими засобами є:

- сервер бази даних (БД);
- веб-сервер управління запитами;
- сервер застосувань з обробки даних.

Прикладним забезпеченням КСМ є комплекс програм, який реалізовує функції системи за інформаційною технологією “клієнт-сервер” і спирається при роботі на інструментальні засоби.

В результаті до програмної архітектури КСМ включені наступні компоненти:

- проксі-сервер обробки запитів Nginx;
- веб-сервер відтворення інформації Apache2;
- сервер обробки даних Django;
- сервер бази даних Microsoft SQL Server.

У наведеній на рис.1 основній схемі функціонування компонентів КСМ можлива варіативність застосування серверів, що дозволяє гнучко дублювати кожну ланку та дзеркулювати кожен сервер для створення так званого «гарячого» резерву.

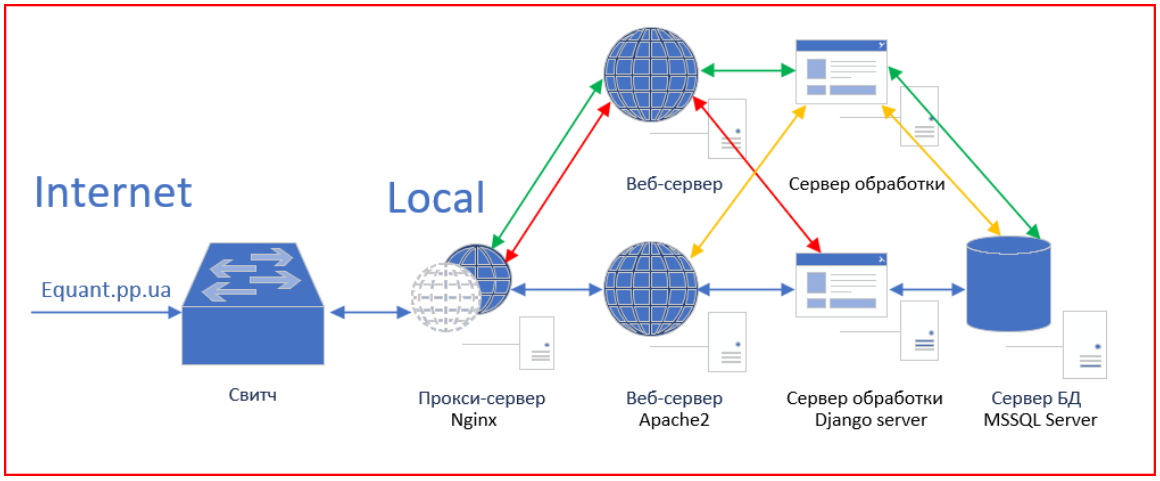



Рисунок 1 – Схема функціонування основних компонентів КСМ

Системне програмне забезпечення серверів КСМ здійснюється за допомогою операційної системи Linux Debian 11, вибір якої обумовлено наступними міркуваннями:

1) жорстка політика стосовно програмних пакетів, репозитарій з величезною їх кількістю, а також висока якість версій;

2) можливість віртуалізації KVM (Kernel-based Virtual Machine) на основі операційної системи;

3) за визначенням Debian є вільним програмним забезпеченням (Open Source). Тому Debian GNU/Linux є однією з найбільш вільних з найпопулярніших операційних систем;

4) враховуючи, що для розробки та роботи БД потрібна ліцензія на Windows Server для Microsoft SQL Server вибір зроблено у бік віртуалізації KVM на основі ОС Linux Debian.

Орієнтований перелік засобів апаратного забезпечення КСМ наведений у таблиці 1.

Таблиця 1 – Орієнтовний перелік засобів апаратного забезпечення КСМ

| № | Тип елемента | Назва |
|---|---|---|
| 1 | Шасі (основа, база) | HP ProLiant DL360e Gen8 Server (4xLFF) |
| 2 | Процесор | 2xIntel Xeon CPU E5-2430 v2 @ 2.50GHz (6 cores; 12 threads) |
| 3 | Оперативна пам’ять | 24 GB (DIMM DDR3 1333 MHz 12x4Gb) |
| 4 | Контролер дискової підсистеми | Smart Array P420 Controller (Cache Module Memory - 1Gb) |
| 5 | Диски (HDD) | 4xHP 533871-001 300Gb 15K 6G SAS 3.5 (EF0300FATFD) |

При виборі елементів апаратного забезпечення враховувалися наступні фактори: ціна; співвідношення продуктивності у виконуваних задачах; набір дисків та обсягу для поточних умов та завдань; споживання потужності у виборі процесорів та блоків живлення для нього.

Отже, основними інструментальними компонентами - фреймворками у складі програмного забезпечення, які забезпечують роботу КСМ є клієнто-орієнтоване середовище AngularJS для відтворення інформації, сервіс-орієнтоване середовище Django Framework для обробки даних та система керування базою даних Microsoft SQL Server.

Перевагою використання вищезазначених компонентів є наступне:

- модульна архітектура, що забезпечує високу швидкість розробки;
- масштабованість та просте розширення функціоналу системи;
- чітка структурованість системи та наявність вбудованих засобів для ефективного тестування та налагодження;
- висока швидкість обробки даних;
- забезпечення цілісності даних;
- мінімізація вихідного коду за рахунок підтримки вбудованих технологій обміну даними із використанням REST API;
- підтримка вбудованого функціоналу для валідації вхідних даних та захисту від типових загроз, зокрема SQL-ін’єкцій (XSS), підміни міжсайтових запитів (CSRF) тощо.

Створення єдиного інформаційного середовища КСМ щодо даних функціонування ринку електричної енергії України та ринків суміжних країн може здійснюватися наступними механізмами обробки даних:

- ручне завантаження даних шляхом автоматизованої обробки вхідних файлів заздалегідь визначеного формату та структури;

- автоматичне завантаження даних шляхом розбору відповідних веб-сторінок енергетичних компаній, учасників оптового ринку електричної енергії, операторів ринку електричної енергії України та ринків суміжних країн, тощо.

- автоматичне завантаження даних із використанням загальнодоступних API сервісів.

Використання вищезазначених механізмів та технологій їх реалізації дозволяє охопити практично будь-які способи отримання даних та забезпечує високу гнучкість під час розробки відповідних сервісів, що у свою чергу забезпечує процес оперативного наповнення інформацією єдину БД КСМ та використання зазначених даних для подальших моделюючих розрахунків.

Слід відзначити наступну особливість у структурі БД для створення єдиного інформаційного середовища КСМ. Структура БД передбачає наявність множини таблиць, які окрім зберігання енергетичних даних та результатів моделювання забезпечують роботу механізмів авторизації та автентифікації користувачів, збереження сесійних даних тощо. Для забезпечення семантичної єдності цих структур варто виділити підхід подання показників суб'єктів функціонування ринку, що безпосередньо пов'язані із обробкою даних, який забезпечить адаптованість структури бази до можливих змін у структурі суб'єктів ринку і особливостей їх функціонування в майбутньому. Цей підхід побудований на механізмі опису метаданих через створення класифікаторів показників, їх зв'язків та сховища даних наведено у роботі [3].

В результаті запропонована структура програмних засобів КСМ забезпечить створення об'єктно-орієнтованого інформаційного середовища з подальшою інтеграцією існуючих та розроблюваних в майбутньому програмних комплексів на єдиній основі. База даних, що інтегрована з комплексом програм адміністрування та обслуговування, надасть інформаційну систему корпоративного призначення для вирішення виробничих, економічних та інших функціональних завдань.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Макоклюев, Б. И., Антонов, А. В., & Набиев, Р. Ф. (2004). Информационная структура и программные средства обработки и хранения данных технологического оборудования и режимных параметров. *Производственно-технический журнал "Электрические станции"*, 6, 48-52
2. Остапченко, К. Б., Лісовиченко, О. І., Євдокимов, В. А., & Борукаев, З. Х. (2021). Створення інформаційно-моделюючої системи аналізу процесів ціноутворення на ринку електричної енергії. *Електронне моделювання*, 43(4), 51-68. https://doi.org/10.15407/emodel.43.04.051
3. Остапченко, К. Б., Євдокимов, В. А., & Борукаев, З. Х. (2022). Сховище оперативних даних системи підтримки прийняття рішень для організаційного управління ринком електроенергії. *Електронне моделювання*, 44(3), 101-112. https://doi.org/10.15407/emodel.44.03.101

Г.П. Костенко

# СТРАТЕГІЇ ЗАСТОСУВАННЯ ВТОРИННИХ БАТАРЕЙ ЕЛЕКТРОТРАНСПОРТУ ДЛЯ ПОКРАЩЕННЯ РЕЗИЛЬЄНТНОСТІ СИСТЕМИ ЕЛЕКТРОПОСТАЧАННЯ

У сучасному світі залежність від стабільного та надійного електропостачання неухильно зростає, особливо в сферах критичної інфраструктури, таких як лікарні, диспетчерські центри та інші життєво важливі служби. З поширенням відновлюваних джерел енергії та поступовим зношуванням традиційних енергетичних систем, потреба в альтернативних джерелах енергії, які можуть гарантувати безперебійність постачання, стає особливо актуальною. Використання вторинних батарей електротранспорту як резервного джерела енергії відкриває нові можливості для покращення резильєнтності енергетичних систем [1].

У контексті глобального переходу на відновлювані джерела енергії, роль електротранспорту та згодом, накопичувачів на базі відпрацьованих батарей електромобілів, в енергосистемі стає критично важливою. Сукупна інтеграція ВДЕ, електромобілів та їх вторинних батарей для зберігання енергії, може значно посилити не тільки ефективність, але й надійність енергетичної інфраструктури (рис. 1), що може мати вирішальне значення у випадках перебоїв у електропостачанні внаслідок природних або техногенних аварій, а також в умовах військової агресії.


Рисунок 1 – Сталий розвиток енергетики – інтеграція ВДЕ, електротранспорту та вторинне застосування літій-іонних батарей

Повторне використання вторинних батарей електротранспорту у системах електропостачання не тільки сприятиме сталому розвитку за рахунок зниження потреби у виробництві нових батарей, але й значно збільшить

енергетичну безпеку. Важливість цього підходу особливо відчутна у ситуаціях, коли перебої в постачанні електроенергії можуть призвести до катастрофічних наслідків, загрожуючи життю та здоров'ю людей, а також стабільності економіки. Таке вторинне використання батарей сприяє ефективному управлінню ресурсами та зниженню витрат, що робить цей підхід потенційно вигідним інвестиційним рішенням для бізнесу та урядів.

Це дослідження спрямоване на аналіз стратегій використання електротранспорту з метою покращення стійкості системи електропостачання в Україні.

Процес перепрофілювання передбачає відновлення акумуляторів, ємність яких знизилися приблизно до 70-80% від початкової (рис. 2). Незважаючи на те, що ці батареї більше неефективні для використання в транспортних засобах, вони все ще мають значну та достатню ємність для вторинних застосувань, пов’язаних зі зберіганням електроенергії [2-3]. Це особливо актуально за умови необхідності сприяннння іінтеграції ВДЕ. Гнучкість, яку пропонують перепрофільовані батареї електромобілів, може мати вирішальне значення для доповнення ВДЕ-генерації (сонячної та вітрової), балансуванні мережі та забезпечення надійного електропостачання.

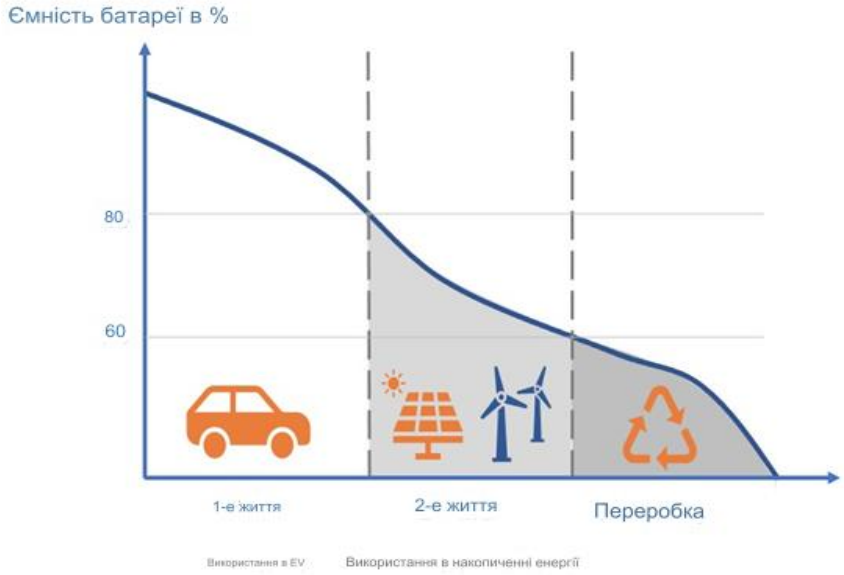



Рисунок 2 – Стадії життєвого циклу батарей електромобілів

Такі системи можуть включатися до енергомереж для підтримки балансування навантаження, забезпечуючи додаткові можливості для згладжування піків попиту на енергію або для збереження енергії від ВДЕ. Вторинне використання батарей також сприяє зменшенню відходів та підвищує екологічну стійкість виробництва батарей.

ЛІБ електротранспорту для повторного використання можуть сприяти підвищенню продуктивності та створювати нові економічні можливості [4]. Дослідження, зокрема, свідчать, що витрати на електромобілі можуть зменшитися завдяки вторинному використанню батарей, що фактично розподіляє початкову вартість між двома застосуваннями

Таблиця 1. Застосування вторинних батарей для покращення резильєнтності енергетичних систем

| Застосування | Ефективність |
|---|---|
| 1. Використання як резервного джерела енергії для критичних навантажень | • Надійність електропостачання |
| 2. Підтримка балансування мережі та управління піковими навантаженнями | • Регулювання піковим навантаженням<br>• Підвищення ефективності<br>• Регулювання частоти |
| 3. Забезпечення енергією у випадках аварійних відключень | • Підтримка резерву<br>• Енергетична самодостатність<br>• Безпека та стійкість |

***1. Використання як резервного джерела енергії для критичних навантажень***

*Надійність постачання:* Вторинні батареї можуть накопичувати відновлювану енергію та забезпечувати її постійне постачання до критично важливих об'єктів, знижуючи залежність від основних джерел енергії.

*Застосування:* Приклади включають лікарні, диспетчерські центри та інші об'єкти, де перерви в електропостачанні можуть призвести до серйозних наслідків.

*Ефективність:* Оптимізація споживання накопиченої енергії забезпечує тривалу підтримку важливих функцій під час енергетичних перебоїв.

***2. Підтримка балансування мережі та управління піковими навантаженнями***

*Регулювання пікових навантажень:* Вторинні батареї допомагають згладжувати піки споживання, шляхом віддачі збереженої енергії у мережу під час високого попиту.

*Підвищення ефективності мережі:* Застосування цих батарей дозволяє знизити навантаження на основні електростанції та зменшити витрати на енергію під час пікових годин.

*Регулювання частоти:* Вторинні батареї можуть швидко реагувати на зміни в навантаженні, допомагаючи підтримувати стабільність і якість електроенергії у мережі.

***3. Забезпечення енергією у випадках аварійних відключень***

*Резервна підтримка:* Вторинні батареї можуть автоматично включатися при відключенні основного джерела, забезпечуючи неперервність електропостачання.

*Енергетична незалежність:* Інтеграція вторинних батарей у місцеві мережі забезпечує гнучкість та знижує залежність від централізованої енергетичної системи.

*Безпека та стійкість:* Наявність автономного джерела живлення

зменшує ризики, пов'язані з енергетичними кризами та природними катастрофами.

Прикладом є робота автомобільних компаній, таких як Nissan, Mitsubishi та Toyota в Японії після стихійних лих, де впроваджувались Vehicle- to-Grid та вторинні батареї які можуть діяти як генератори під час надзвичайних ситуацій [5]. Стратегії циркулярної економіки для ЛІБ електротранспорту може у підсумку сприяти зменшенню викидів CO2, зменшити експлуатаційні витрати та забезпечи стабільне функціонування системи електропостачання.

**Висновки**

Застосування вторинних батарей електротранспорту в системах зберігання енергії містить значний потенціал для підвищення стійкості та ефективності систем електропостачання. Використання вторинних батарей як резервного джерела енергії для критичних навантажень виявляється не тільки коштовно-ефективним рішенням, але й важливим елементом у підтримці екологічної стійкості. Їхня інтеграція у системи електропостачання сприяє зниженню залежності від традиційних джерел енергії, що, в свою чергу, полегшує навантаження на інфраструктуру під час пікових періодів споживання. Завдяки оптимізації використання накопиченої енергії за допомогою сучасних систем управління, забезпечується надійне електропостачання в критичні моменти. Важливо також відзначити, що наявність цих резервних джерел сприяє значному підвищенню резильєнтності енергетичних систем, забезпечуючи їх здатність швидко реагувати на непередбачені відключення, тим самим покращуючи загальну надійність і безпеку енергопостачання.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Kostenko, G., & Zaporozhets, A. (2024). World experience of legislative regulation for lithium-ion electric vehicle batteries considering their second-life application in power sector. System Research in Energy, (2 (77), 97-114. https://doi.org/10.15407/srenergy2024.02.097
2. Kostenko G. P. (2022). Overview of European trends in electric vehicle implementation and the influence on the power system. System Research in Energy, (1 (70), 62-71. https://doi.org/10.15407/srenergy2022.01.062
3. G.P. Kostenko. Situation analysis of the prospects for the development of electric transport and its integration into the energy system of Ukraine. "Energy: Economics, Technology, Ecology", No. 1 (2023). https://doi.org/10.20535/1813-5420.1.2023.276185
4. Neubauer, J, 2012. Techno-economic analysis of PEV battery second use: Repurposed battery selling price and commercial and industrial end-user value. NREL.
5. Esteban, M., Portugal-Pereira, J., 2014. Post-disaster resilience of a 100% renewable energy system in Japan. Energy 68, 756–764.

O. Ponomarenko, A. Krymska

# STRATEGIES FOR ENSURING DATA SECURITY IN ENERGY MONITORING SYSTEMS IN UKRAINE

## Introduction

The issue of the dynamic development and use of information and communication technologies in all spheres of human activity is particularly relevant in the current military realities in Ukraine. Today, information, namely data security, is gaining the status of the most important strategic resource for both the state and the individual [1]. The development of information and communication technologies is increasing the technological gap between the state and elements of the state system, including the energy infrastructure. In particular, the technological gap between the requirements of energy infrastructure organisations to the security of information resources and the capabilities of these technologies is growing. Information security in the field of energy storage and distribution. This raises the problem of scientific research of a number of measures, tools and methods. Management capacity in this sector is an important element for the survival and effective functioning of the sector. This is an important element for the survival and effective functioning of the sector.

Ensuring and strengthening information security at critical infrastructure facilities is a serious problem that is being addressed at the highest level of Ukraine [2]. Today, it is necessary to solve the problems of the development of the domestic technology industry and the low quality of education in order to create an effective security system in the global information space.

## Research results

According to M. Baran, there is a constant threat to security in modern society for various types of information processes [1]. Information terrorism (cyberterrorism) is a common problem in today's environment [3].

The use of information weapons and the development of high-tech information tools include the regulation and comprehensive management of cyberspace, as well as the constant updating of the regulatory framework [4]. The National Information Policy of Ukraine is aimed at creating conditions for its effective functioning, free access of the society to information resources, development of information infrastructure, and, on the other hand, removal of legal barriers to access to information resources.

The national information policy of Ukraine is implemented by creating economic, organisational and other conditions by public authorities necessary to strengthen the protection of the information sphere and promote its sustainable functioning in the current changing environment [5].

The neglect of this policy is due to the slow pace of informatisation in our country, outdated domestic software, information technology tools and critical infrastructure protection. Therefore, subjects of information security systems in the field of energy storage and distribution use hardware and software in the development and operation of information security systems.

Hardware and software are mostly foreign-made, and the risk of unauthorised access to stored and processed information increases because these ICT tools and automated workstations are not subject to special audits and certification for this purpose [6].

In particular, the social component ensures the training of specialists in the field of information security and the rational and efficient use of information systems and technical means necessary for the sustainable functioning of system assets in the global information space.

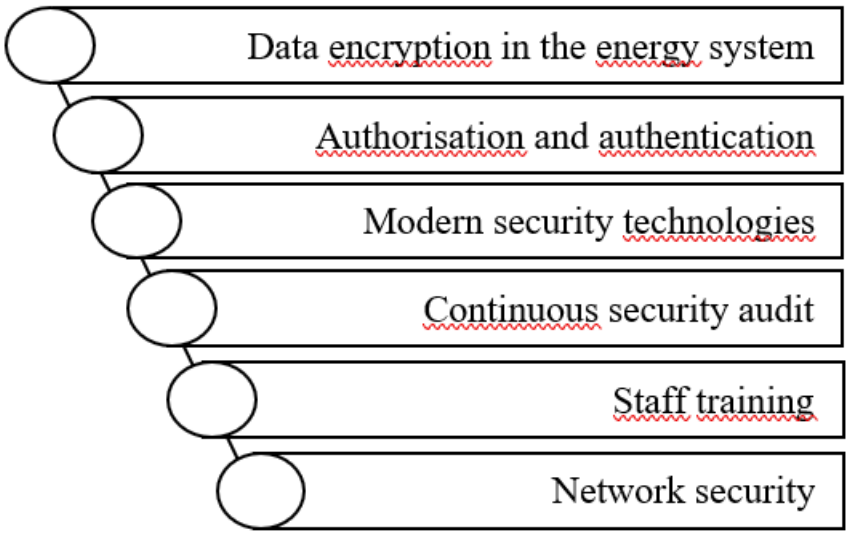
The lack of adequate information protection at critical infrastructure facilities is becoming a more serious problem over time and is one of the main shortcomings of information security by cybercriminals [7]. Ukraine needs to maintain a high level of readiness to prevent and detect computer attacks, as well as to counter computer attacks.

In particular, it should be noted that violations of the rules for the operation of information and communication technologies are caused by weak management control and low levels of responsibility for violations.

The complexity and interconnectedness of the task of improving cybersecurity in the information sector means that the more regulatory, organisational, logistical and other measures are taken, the better it will be implemented [8].

The result of an improved system is, first and foremost, effective security. This result is characterised by the provision of effective information security methods and technologies that will “protect” cyberspace in our food, energy and other sectors [9].

The search for and implementation of optimal solutions to ensure and improve information security in the field of storage and distribution of food and energy resources should be based not only on methods and technologies, but also on the technologies of the industry in which they are used (fig. 1).




*Source: compiled by the author on the basis of his own research*

Figure 1 - Strategies to ensure data security in energy monitoring systems

One of the important elements of the strategy is data encryption, as all data transmitted or stored in energy monitoring systems must be encrypted. The use of modern encryption algorithms can prevent unauthorised access to data. Authorisation and authentication means that all users who have access to the energy monitoring system should be authorised and access to certain data should be restricted by the system. Then there is the use of modern security technologies related to information security management and intrusion detection systems, which can help to increase the level of security of energy monitoring system data [10].

Continuous security auditing reflects the importance of security systems that are required to constantly monitor and check someone or themselves to identify potential threats and vulnerabilities. Raising awareness and training of staff on cybersecurity and data protection issues is considered equally important. Staff should be aware of the risks and know how to act in the event of anomalies or suspicious activity. Protecting the network through which data is transmitted to the energy monitoring system, therefore, must be properly protected. This includes the use of intranets, firewalls and other measures.

**Conclusions**

The main way to solve the current problem is to reduce energy dependence, diversify sources of supply, increase energy efficiency and ensure social stability. The national energy sector should be transformed from a subsidised and problematic one into an economically profitable, competitive and flexible one, creating new opportunities for data protection and the introduction of innovative developments in the field of energy resources. Prospects for further research include vulnerability analysis and penetration testing to identify potential risks and weaknesses in the security system.

## REFERENCES


1. Baran, M. V. (2022). Protection of information in the context of information security. Analytical and comparative jurisprudence, *3*, 150–155. http://journal-app.uzhnu.edu.ua/article/view/264943/260924.
2. Zinovieva, I. S. (2018). Decision-making support in the energy sector based on geographic information systems. Scientific and Technical Conference of Young Scientists and Specialists of the Pukhov Institute for Modelling Problems in Energy of the National Academy of Sciences of Ukraine. https://www.researchgate.net/publication/330358270_PIDTRIMKA_PRIJNATTA_RISEN_V_ENERGETICI_NA_OSNOVI_DANIH_GEOINFORMACIJNIH_SISTEM.
3. Ilienko, A. S. (2019). Energy Security of Ukraine: Essence, Threats and Regulatory Mechanisms. Scientific Notes of Vernadsky Kyiv Polytechnic National University, *30 (69)*, 61–66. https://www.pubadm.vernadskyjournals.in.ua/journals/2019/4_2019/13.pdf.
4. Marutian, R. R. (2020). Mechanisms for Intellectual Support of Ukraine's National Security Policy: Content and Structure. *Web of Scholar: international academy journal, 1(43),* 26-31. https://doi.org/10.31435/rsglobal_wos/ 31012020/ 6883.

5. Mordovtsev, O., Avanesova, N., Liubushyn, R. (2022). Formation of an information security system in the field of storage and distribution of food and energy resources. Aspects of public administration, *10 (3),* 21–30. https://doi.org/10.15421/152216.
6. Svitlychnyi, V. A. (2023). Protection of personal data under martial law in Ukraine. Law and security, *3 (90),* 226–236. https://doi.org/10.32631/pb.2023.3.19 .
7. Sukhodolia, O. M., Kharazishvili, Yu. M., Riabtsev, H. L. (2023). Energy security of Ukraine: a promising model of risk management : monograph. https://doi.org/10.53679/NISS-book.2023.01.
8. Tymchuk, O., Potapova, N. (2022). Principles of information security. Applied aspects of modern interdisciplinary research, 214–215. https://jpasmd.donnu.edu.ua/article/view/12970.
9. Khriakova, N. (2019). Energy Security in Ukraine: Problems of Ensuring and Prospects for Improvement. Young scientist, *10 (74),* 628–633. https://doi.org/10.32839/2304-5809/2019-10-74-132.
10. Shevchenko, O. A. (2021). Energy Security as an Integral Element of Ensuring the Economic Security of the State in the National Security Strategies of Ukraine. Scientific Bulletin of Uzhhorod National University, *67,* 163–168. https://doi.org/10.24144/2307-3322.2021.67.32.

О.І. Грамак, М.М. Ліневич

# ПРОБЛЕМИ ЗБЕРЕЖЕННЯ ЕЛЕКТРОННИХ ДОКАЗІВ КІБЕРЗЛОЧИНІВ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

В Стратегії енергетичної безпеки, яку схвалено розпорядженням Кабінету Міністрів України від 4 серпня 2021 р. № 907-р визначено, що одним пріоритетних завдань досягнення стійкості функціонування енергетичного сектору є забезпечення кібербезпеки критичної інфраструктури енергетичного сектору. Також, Законом України "Про основні засади забезпечення кібербезпеки України" визначено, що суб'єкти забезпечення кібербезпеки : здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення наслідків; здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз. Виконання цих завдань вимагає якісного розслідування кіберзлочинів.

Розслідування кіберзлочинів в енергетиці та на об'єктах критичної інфраструктури відіграє надзвичайно важливу роль у забезпеченні безпеки держави. Кібератаки на енергетичні системи призводять до серйозних перебоїв у постачанні енергії, що має критичний вплив на економіку держави, її безпеку та життя громадян. Втрати, які виникають внаслідок таких атак, можуть бути надзвичайно важкими, як з економічної, так і з соціальної точок зору.

В процесі розслідування кіберзлочинів все більшого значення набуває документування даних щодо кіберінциденту/кібератаки, збору і збереження електронних доказів. Проблема збереження електронних доказів кіберзлочинів на об'єктах критичної інфраструктури виникає з ризиків, які несе кібератака для безперебійної роботи цих об'єктів. Критична інфраструктура, така як енергетичні системи, транспортні мережі, банківські системи тощо, забезпечує нормальне функціонування суспільства і є його життєвоважливими елементами. Будь які перебої або зупинки в роботі цих об'єктів мають серйозні наслідки для громадян, економіки та безпеки країни в цілому.

Успішність співробітництва суб'єктів забезпечення кібербезпеки в розслідуванні кіберзлочинів зумовлена швидкістю збереження електронних доказів кіберзлочинів. Вимога щодо збору та вивчення таких даних (електронних доказів кіберзлочинів) визначена Порядком реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затвердженого Постановою Кабінету Міністрів України від 04.04.2023 № 299 та Методичними рекомендаціями щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затвердженими наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 03.07.2023 № 570.

Збереження електронних доказів кіберзлочинів на об'єктах критичної інфраструктури є складним завданням з кількох причин. По-перше, кіберзлочини, як правило, є дуже витонченими та важкими для виявлення через їхню прихованість і вміння уникнути виявлення. Це стає ще більшою проблемою на об'єктах критичної інфраструктури, де інформаційні системи є

складними та розподіленими. По-друге, багато об'єктів критичної інфраструктури України мають застарілі або неодноразово модифіковані інформаційні системи, які мають вразливості, що робить їх більш вразливими до кібератак. Недостатня координація та співпраця між суб’єктами забезпечення кібербезпеки також ускладнюють збереження електронних доказів кіберзлочинів, оскільки це призводить до недостатнього обміну інформацією та неефективного виявлення загроз.

Збереження електронних доказів кіберзлочинів дозволяє не лише виявити конкретні загрози, але і аналізувати їхні методи та мотивацію, що сприяє вдосконаленню заходів захисту. Запобігання кібератакам на об'єкти критичної інфраструктури стає набагато ефективнішим завдяки системам фіксації, які надають можливість вчасного реагування та мінімізації наслідків.

Збереження електронних доказів кіберзлочинів, також, пов’язано із “людським” фактором. Компетентні та досвідчені працівники можуть швидко та ефективно виявляти та відстежувати кіберзлочини, що, в свою чергу, вимагає кращої підготовки персоналу та досконалості процедур реагування на події в кіберпросторі.

Отже, для забезпечення збереження електронних доказів кіберзлочинів на об'єктах критичної інфраструктури необхідно постійно підвищувати обізнаність персоналу у сфері кібербезпеки, надавати їм відповідну підготовку та навички. В той же час важливо вдосконалювати процедури виявлення та реагування на кіберзлочини, а також впроваджувати технологічні засоби, які допомагатимуть автоматизувати процеси фіксації та аналізу кіберзлочинів.

Підсумовуючи вищезгадане, можна запропонувати наступні напрями діяльності, що забезпечать якісне збереження електронних доказів для розслідувань кіберзлочинів на об’єктах критичної інфраструктури, в тому числі на об’єктах енергетики:

впровадження міжнародних стандартів кібербезпеки на об’єктах критичної інфраструктури;

підготовка персоналу у сфері кібербезпеки, в тому числі з забезпечення збереження електронних доказів кіберзлочинів;

посилення співпраці між суб’єктами забезпечення кібербезпеки та приватними компаніями;

вдосконалення процедур виявлення та реагування на кіберзлочини;

впровадження технічних рішень, які автоматизують процеси фіксації та аналізу кіберзлочинів.

Це дасть змогу ефективно розслідувати злочини у глобальних масштабах, отримувати, зберігати, досліджувати та надавати електронні докази з урахуванням трансграничного характеру злочинів.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Розпорядження Кабінету Міністрів України “Про схвалення Стратегії енергетичної безпеки”, 04.08.2021, https://zakon.rada.gov.ua/laws/show/907-2021-%D1%80#Text;

2. Закон України “Про основні засади забезпечення кібербезпеки України”, ВВР, 05.10.2017 №2163-19 (зі змінами) URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text;
3. Постанова Кабінету Міністрів України “ Деякі питання реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі”, 04.04.2023, https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#Text;
4. Наказ Адміністрації Держспецзв'язку “Про затвердження Методичних рекомендацій щодо реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі”, № 570 (03.07.2023), https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-03-07-2023-570-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-reaguvannya-sub-yektami-zabezpechennya-kiberbezpeki-na-rizni-vidi-podii-u-kiberprostori.

M. Antonishyn, Y. Kharlamov, A. Kharlamova

# MOBILE APPLICATIONS SECURITY TESTING METHODOLOGY

Ensuring cybersecurity in the energy sector is a strategic goal №2 of the Energy Security Strategy of Ukraine [1]. The use of mobile applications is increasing, both to control electricity consumption by ordinary users and to pay for energy supply services through these applications, and to control specialized systems through specially developed software or a thin client. That is why the Cybersecurity Strategy states that it is necessary to: "to develop new national standards in the field of cybersecurity, organizational and technical requirements related to the security of applications, mobile devices, workstations, servers and networks, cloud computing models, taking into account European and international standards" [2]. To fulfill the tasks of securing mobile applications, one of the points of ensuring the security of mobile programs is testing for vulnerabilities in the software application. For testing, a methodology is proposed that provides a structured approach to testing. Mobile Security Framework based on the triangle which gives comprehensive information about the security state of the mobile application: Assessment, Penetration testing, and Code review. ByteCode Team provides vulnerability assessment based on the Hybride framework created from the main industry standards, best practices, and discoveries:

- Open Web Application Security Project (OWASP) [3];
- NIST 800-163 Vetting the Security of Mobile Application [4];

And other top-notch industry practices with a comprehensive process that allows us to discover all of the existing security bugs and threats:

- **Level 1 - Automatic scanning**: static analysis by automatic security tools to uncover existing mobile application security bugs, vulnerabilities, and breaches;
- **Level 2 - Vulnerability assessment MASVS**: deep dive into defined security bugs, threats, and vulnerabilities using MASVS methodology to separate false positives and provide risk category and maturity level for the mobile application security;
- **Level 3 - Penetration testing**: penetration testing to simulate a hacker attack on the application as an entry point and on the infrastructure behind it to define all the existing breaches and discover an ability to exploit it to evaluate a business risk;
- **Level 4 - Code review**: review of mobile application code to determine weaknesses in architecture and utilization of the best practices of secure coding;
- **Level 5 - MASVS Adoption, Validation, and Certification (optional)**: when application security is chosen as a primary mindset for application development, MASVS becomes a main guideline for a team and allows organically united user-centric and security-centric approaches.

Table 1 – Core levels of security testing methodology

| | Automatic Scanning Level 1 | Vulnerability Assessment Level 2 | Penetration Testing Level 3 | Code Review Level 4 |
|---|---|---|---|---|
| **Scope** | Defined by scanner | MASVS | Defined by organization | Defined by organization |
| **Objective** | Uncover many vulnerabilities | Uncover many vulnerabilities false-positive free | Penetrate into the system and meet specific goal | Logical errors and ... |
| **Threat Emulation** | Basic | Basic | Advanced | Advanced and persistent |
| **Rules** | Defined by scanner | Well defined and agreed | Well defined and agreed | Anything goes |
| **Employee Awareness** | Typically aware | Typically aware | Discussable | Discussable |
| **Vulnerability Scanning** | Yes | Yes | Yes | Yes |
| **Manual Testing Simulating Attackers** | No | Partially | Yes | Yes |
| **Typical Duration** | 2-3 days | 2-3 weeks | 1,5 - 2 month | 1,5 - 3 month |
| **Report** | Detailed readable report based on automatic findings | Detailed based on MASVS Checklist with findings, steps for reproducing, depth of exploitation | As previous one + Threat Model, exceptional pases requested by client, exploits | Detailed based on VeraCode SecSDLC best practices |
| **Support During Bug fixing process** | No | Yes<br>2 weeks | Yes<br>4 weeks | Yes<br>4 weeks |
| **Re-test for defined and fixed vulnerabilities** | No | 1 release | 1 release | 2 releases |

## REFERENCES


1. Стратегія енергетичної безпеки, схвалена Кабінету Міністрів України від 4 серпня 2021 року №907-р. https://zakon.rada.gov.ua/laws/show/907-2021-%D1%80#Text.
2. Проект Стратегії кібербезпеки України (2021-2025 роки). https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf.
3. OWASP Mobile Application Security Verification Standard https://mas.owasp.org/MASVS/.
4. NIST 800-163 Vetting the Security of Mobile application https://doi.org/10.6028/NIST.SP.800-163r1.

С.Ф. Гончар, О.М. Дибач

# ЗАБЕЗПЕЧЕННЯ КОМП'ЮТЕРНОЇ БЕЗПЕКИ ЯДЕРНИХ УСТАНОВОК

Розвиток цифрових інновацій дає змогу удосконалювати цифрове управління та автоматизацію на ядерних установках, що дозволяє підвищувати ефективність експлуатації, знижувати витрати на робочу силу, зміцнювати безпеку. Як зазначається в [1], удосконалені проекти ядерних реакторів, наприклад модульні реактори малої потужності та мікрореактори, від самого початку передбачають плани щодо використання штучного інтелекту та машинного навчання для реалізації таких інноваційних функцій, як автоматизація, дистанційний диспетчерський контроль та технічне обслуговування, а також використання єдиного пункту управління для кількох установок. Фахівці стверджують [1], що з використанням передових алгоритмів машинного навчання штучний інтелект допоможе підвищити ефективність захисту від кібератак на ядерних установках за рахунок виявлення аномальних даних у комп'ютерних системах, оснащені елементами штучного інтелекту системи безпеки можуть безперервно відстежувати та аналізувати величезну кількість даних, щоб визначити, чи є якась активність аномальної експлуатації установки, системи з елементами штучного інтелекту можуть використовуватися для попередження співробітників, які відповідають за управління атомною електростанцією, про найменші відхилення від нормальної експлуатації, забезпечувати функціонування системи підтримки прийняття рішень.

В той же час цифрові інновації, зокрема штучний інтелект, також можуть являтися джерелом ризиків. Наприклад, переваги, які дає застосування штучного інтелекту на ядерних установках, значною мірою залежать від того, як було виконано навчання таких систем. Штучний інтелект обізнаний тільки в тих межах, в яких представлені навчальні дані для його роботи, і якщо він не має правильних вихідних даних, ним можна маніпулювати, щоб отримувати помилкові показання та результати [1, 2]. Ще однією проблемою, пов'язаною із застосуванням штучного інтелекту у сфері фізичної ядерної безпеки, є розуміння того, як і чому моделлю штучного інтелекту було прийнято те чи інше рішення чи видано певний прогноз, відсутність прозорості та можливості інтерпретації алгоритмів. Багато алгоритмів машинного навчання є «чорними ящиками», тобто важко зрозуміти, як вони приходять до своїх висновків [1, 2].

Таким чином, зловмисники можуть задіяти цифрові інновації, для організації більш витончених і цілеспрямованих кібератак, використовувати їх вразливості для порушення цілісності комп'ютерних мереж або систем та доступу до закритої інформації на ядерних установках. Для захисту чутливої інформації та комп'ютерних систем цих об'єктів необхідно застосовувати комплексний підхід до комп'ютерної безпеки шляхом розроблення та впровадження програми забезпечення комп'ютерної безпеки, ключовими елементи якої є [1]:

– функції та обов'язки;

– управління ризиками, контроль факторів уразливості та забезпечення відповідності нормативним вимогам;

– розроблення заходів безпеки та управління ними;

– управління цифровими активами;

– процедури забезпечення фізичної безпеки;

– управління кадрами.

Деякі з елементів програми забезпечення комп'ютерної безпеки детально досліджувалися науковцями, зокрема питання оцінювання комп’ютерної безпеки інформаційних та керуючих систем АЕС, вивчення нормативної бази у сфері комп’ютерної безпеки інформаційних та керуючих систем АЕС [3, 4].

Разом з тим, слід відмітити, що особливе значення при управлінні кадрами в ядерній промисловості надається благонадійності співробітників, їх кваліфікації та навчанню [1], тобто людським факторам. Вплив таких факторів на забезпечення безпеки ядерних установок має величезне значення, оскільки наслідки порушення безпеки таких об’єктів можуть бути катастрофічними. Більш детально людські фактори, які впливають на забезпечення комп'ютерної безпеки ядерних установок можна розглянути з використанням удосконаленої моделі імовірних деструктивних дій персоналу таких об’єктів (рис.1) [5].

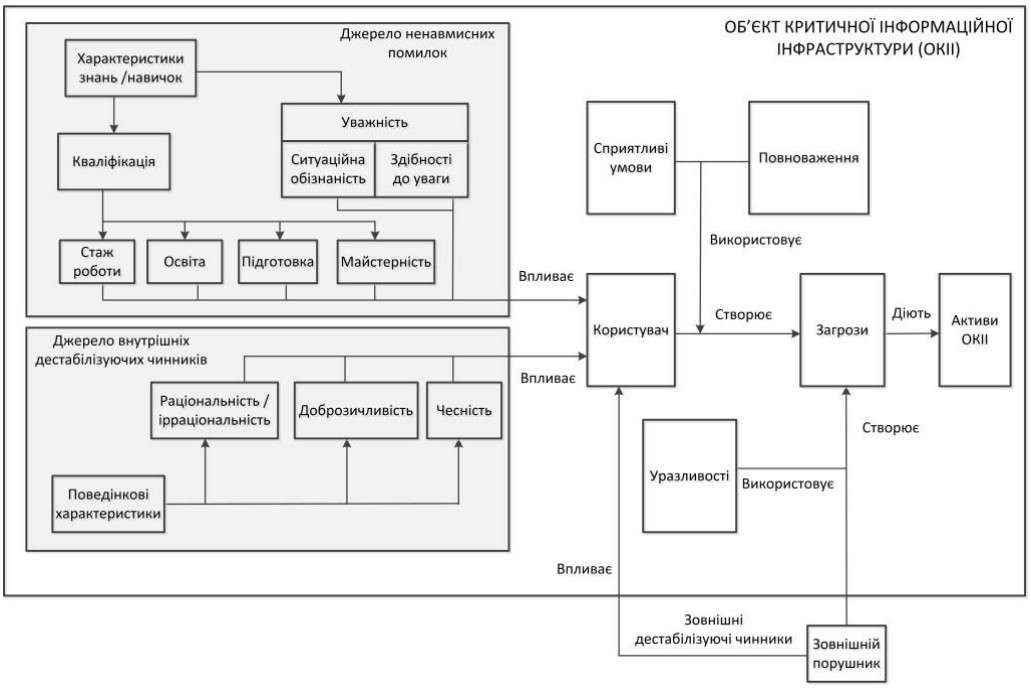



Рисунок 1 – Удосконалена модель імовірних деструктивних дій персоналу ядерних установок

Таким чином, визначено ключові елементи програми забезпечення комп'ютерної безпеки, розроблення та впровадження якої є необхідним для захисту чутливої інформації та комп'ютерних систем ядерних установок. Також приведено удосконалену модель імовірних деструктивних дій персоналу ядерних установок, у якій детально розкрито фактори, що впливають на забезпечення комп'ютерної безпеки таких об’єктів.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Computer Security in the Nuclear World. IAEA BULLETIN. June 2023. Vol. 64-2.
2. ШІ та машинне навчання для управління ризиками [Електронний ресурс] // Режим доступу до ресурсу: https://visuresolutions.com/uk/blog/ai-and-machine-learning-for-risk-management/.
3. Klevtsov, A., Yastrebenetsky, M., & Trubchaninov, S. (2015). Комп'ютерна безпека інформаційних та керуючих систем АЕС. Ядерна та радіаційна безпека, (4(68), 51-57. https://doi.org/10.32918/nrs.2015.4(68).10.
4. Klevtsov, O., Symonov, A., & Trubchaninov, S. (2020). Комп'ютерна безпека інформаційних та керуючих систем АЕС: оцінювання комп'ютерної безпеки. Ядерна та радіаційна безпека, (4(88), 69-76. https://doi.org/10.32918/nrs.2020.4(88).09.
5. Гончар С.Ф., Ткаченко В.В., Удосконалена модель імовірних деструктивних дій користувачів об'єктів критичної інформаційної інфраструктури : Матеріали науково-практичної конференції «Безпека енергетики в епоху цифрової трансформації», Київ, 2023. – С. 43-46.

О.М. Дибач, С.Ф. Гончар

# ІМОВІРНІСНА ОЦІНКА РИЗИКУ КІБЕРАТАК НА АЕС

Впровадження на атомних електричних станціях (АЕС) цифрових інформаційних та керуючих систем на заміну застарілим аналоговим системам, окрім очевидних переваг (швидка обробка та накопичення даних, діагностування відмов та ін.), вимагає вирішення нової актуальної проблеми – забезпечення кіберзахисту цих систем та кібербезпеки АЕС в цілому.

Незважаючи на ізольованість цифрових систем АЕС від зовнішніх мереж, досвід кібератак, зокрема Stuxnet (2010 р.), демонструє, що ізольована мережа може бути неефективним захистом від спрямованих кібератак.

В системі стандартів Міжнародного агентства з атомної енергії (МАГАТЕ) вимоги до кібербезпеки АЕС (в термінології МАГАТЕ «комп'ютерна безпека») встановлені у документах серії «фізична безпека». У технічному керівництві МАГАТЕ NSS No.17 «Computer Security Techniques for Nuclear Facilities», 2021 1 зазначається що комп'ютерна безпека має впроваджуватися із використанням ризик-інформованого підходу. В п.3.11 NSS No.17 надається наступне визначення ризику: «ризик, у контексті комп'ютерної безпеки, – це ризик, пов'язаний із використанням зловмисником вразливості цифрового активу або групи цифрових активів для здійснення або сприяння зловмисній дії. Цей ризик виражається як комбінація імовірності успішної атаки та тяжкості її наслідків, якщо вона відбудеться».

Комісією ядерного регулювання США (U.S. NRC) у лютому 2023 року було опубліковано оновлену редакцію керівництва RG-5.71 (Revision 1) «Cybersecurity programs for nuclear power reactors» 2, що також визначає необхідність використання ризик-інформованого підходу при розробці програм кібербезпеки АЕС.

У березні 2022 року набрав чинності нормативно-правовий акт Державної інспекції ядерного регулювання України «Вимоги до кіберзахисту інформаційних та керуючих систем атомних станцій для забезпечення ядерної та радіаційної безпеки» НП306.2.237-2022 3. Цей НПА було розроблено із урахуванням відповідних міжнародних документів МАГАТЕ, U.S. NRC, ISO, EPRI та ін.

В НП 306.2.237-2022 вперше введено поняття ризик-інформованого підходу до кіберзахисту: «ризик-інформований підхід до кіберзахисту - процес систематичного виявлення потенційних вразливостей інформаційної та/або керуючої системи та кіберзагроз для цієї системи, імовірнісного оцінювання виникнення негативних подій, детерміністичного оцінювання потенційних негативних наслідків цих подій та розроблення рекомендацій щодо реалізації контрзаходів з метою мінімізації вразливостей, імовірностей виникнення негативних подій та негативних наслідків».

Слід зазначити, що в міжнародних та національних нормативних документах та стандартах не представлені методологічні засади щодо оцінки ризику кібератак на АЕС. Це питання є предметом наукових досліджень, зокрема 4-8.

В цій роботі розглянуто перспективи використання імовірнісного методу аналізу безпеки для оцінки ризиків кібератак на АЕС.

Імовірнісний аналіз безпеки (ІАБ) набув значного поширення в Україні для кількісної оцінки безпеки АЕС, визначення домінантних вкладників в загальний ризик, а також для практичного використання при ризик-інформованому прийнятті рішень з безпеки АЕС. За результатами ІАБ визначаються кількісні показники безпеки АЕС в термінах частоти пошкодження активної зони (ЧПАЗ) та частоти граничного аварійного викиду (ЧГАВ) 9. При розрахунку ЧПАЗ/ЧГАВ враховується частота вихідної події та імовірність реалізації сукупності відмов, що призводять до негативного результату (пошкодження активної зони чи аварійного викиду). Наразі розроблені імовірнісні моделі (дерева подій, функціональні та системні дерева відмов) для усіх 15 енергоблоків АЕС України із використанням програмних засобів SAPHIRE та Risk-Spectrum, виконуються роботи із використання ризик-інформованого підходу для оптимізації технічного обслуговування та ремонту обладнання важливого для безпеки АЕС.

З урахуванням досвіду виконання ІАБ для АЕС України, розроблені імовірнісні моделі можуть бути адаптовані та використані для оцінки ризику кібератак.

Вплив кібератак в моделі ІАБ можливо розділити на 4 типи, представлені на рис.1.

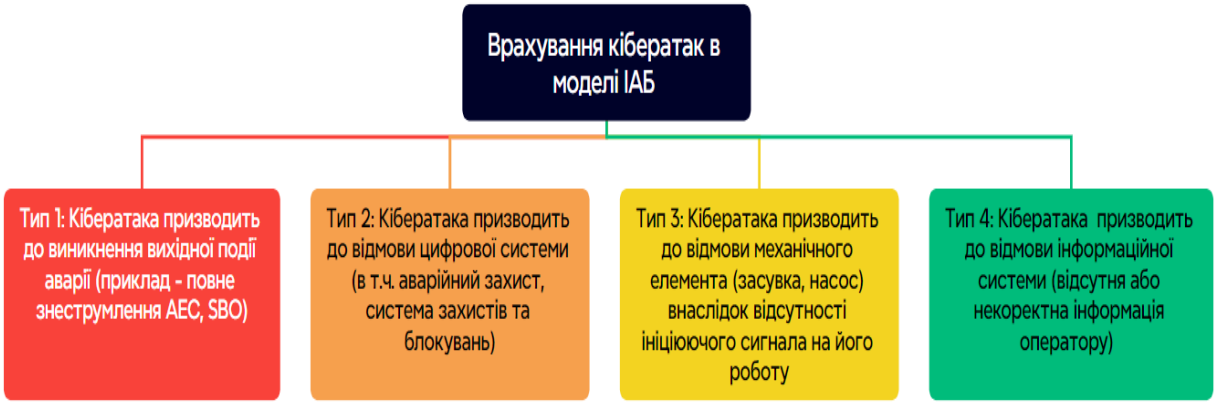



Рисунок 1 – Типи впливу кібератак для врахування в моделі ІАБ

Моделювання додаткових відмов внаслідок кібератак можлива на рівні системних дерев відмов моделі ІАБ шляхом включення у дерева відмов відповідних нових базових подій із імовірнісними параметрами (імовірність відмови, фактор помилки, вид функції розподілу).

Метод врахування кібератак за їх типами у моделі ІАБ представлено у таблиці 1.

Таблиця 1 – Метод врахування впливів кібератак у моделі ІАБ

| **Тип впливу кібератаки** | **Врахування в моделі ІАБ** |
|---|---|
| Тип 1: Кібератака призводить до виникнення вихідної події аварії що розглядається в ІАБ (наприклад, повне знеструмлення майданчику АЕС) | Перегляд частот вихідних подій аварій прийнятих в моделі ІАБ |
| Тип 2: Кібератака призводить до відмови цифрової системи (наприклад, не спрацювання аварійного захисту) | Перегляд частоти перехідних процесів без спрацювання аварійного захисту (ATWS) та імовірності відмови аварійного захисту чи інших цифрових керуючих систем |
| Тип 3: Кібератака призводить до відмови механічного елемента внаслідок не формування сигналу на його роботу | Врахування у деревах відмов додаткових відмов для механічних елементів до звичайних відмов (відмова на запуск, відмова в роботі та ін.) внаслідок кібератаки |
| Тип 4: Кібератака призводить до відмови інформаційної системи (відсутня або некоректна інформація оператору) | Перегляд імовірностей помилок оператора (пропущення дії чи помилка у виконанні). |

За результатами розрахунку моделі ІАБ із додатковими відмовами внаслідок кібератак, отримані значення ЧПАЗ/ЧГАВ доцільно розглядати не як абсолютні величини, а у порівнянні із їх початковими значеннями тобто оцінити відносну вагу кібератаки у загальному ризику.

Розрахунок модифікованої моделі ІАБ дозволить оцінити значимість окремих відмов внаслідок кібератаки і таким чином сфокусувати дії із кіберзахисту на найбільш значущих елементах.

При реалізації зазначеного вище підходу є задачі які потребують подальшого вирішення. Зокрема це оцінка імовірності відмови цифрових систем/елементів внаслідок кібератаки за відсутності достовірних статистичних даних.

Запропонований підхід потребує подальшої практичної реалізації та апробації із використанням імовірнісних моделей для АЕС.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. IAEA Nuclear Security Series No. 17-T (Rev. 1). Computer Security Techniques for Nuclear Facilities, 2021.
2. U.S. Nuclear Regulatory Commission, Regulatory Guide 5.71, Revision 1, Cybersecurity programs for nuclear power reactors, 2023.
3. НП306.2.237-2022 «Вимоги до кіберзахисту інформаційних та керуючих систем атомних станцій для забезпечення ядерної та радіаційної безпеки», затверджений наказом Державної інспекції ядерного регулювання України 22 березня 2022 року № 223.
4. J.W. Park, S. J. Lee, Probabilistic safety assessment-based importance analysis of cyber-attacks on nuclear power plants. Volume 51, Issue 1, February 2019, Pages 138-145.
5. S.Eggers, K.Blanc, Survey of cyber risk analysis techniques for use in the nuclear industry, Progress in Nuclear Energy, Volume 140, October 2021, 103908
6. Do-Yeon Kim, Cyber security issues imposed on nuclear power plants, Annals of Nuclear Energy, Volume 65, March 2014, Pages 141-143.
7. Мохор В. В, Гончар С.Ф., Дибач О.М. Методи оцінки сумарного ризику кібербезпеки об’єктів критичної інфраструктури, Ядерна та радіаційна безпека. 2019. № 2(82), С. 4-8. Doi: https://doi.org/10.32918/nrs.2019.2(82).01.
8. Гончар С.Ф., Бакалинський О.О., Дибач О.М., Дімітрієва Д.О. Метод агрегування ризиків у випадку множини сумісних випадкових подій. Ядерна та радіаційна безпека. 2022. № 1(93), С. 44-50. Doi: https://doi.org/10.32918/nrs.2022.1(93).05.
9. НП 306.2.245-2024. Загальні положення безпеки атомних станцій, Затверджено Наказ Державного комітету ядерного регулювання України від 19 листопада 2007 року № 162 (в редакції наказу Державної інспекції ядерного регулювання України від 04 березня 2024 року № 195).

В.В. Федюк

# ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ОХОРОНИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ: КРИМІНАЛЬНО-ПРАВОВИЙ АСПЕКТ

Всеохоплюючий і надважливий характер інформаційно-комунікаційних технологій в сучасному світі, а також їх потенційна вразливість надзвичайно актуалізує питання безпечності та неперервності їх функціонування. З огляду на зазначене, щодо тих інформаційно-комунікаційних або технологічних систем, які мають винятково важливе значення для держави та суспільства, останніми десятиліттями ведеться активний науковий дискурс стосовно їх розуміння, як об'єктів критичної інформаційної інфраструктури, - невід'ємної складової національної безпеки держави. Наукові напрацювання з даної тематики, здебільшого, представлені в межах техніко-технологічного (роботи спеціалістів технічного спрямування) та організаційно-правового (роботи правників) напрямів [1, с. 289]. В межах другого напряму актуальним питанням дослідники вбачають створення на рівні держави дієвої системи захисту критичної інформаційної інфраструктури від загроз усіх видів, в тому числі й від кримінально-протиправних діянь.

Враховуючи положення ч. 1 ст. 2 Кримінального кодексу України (далі-КК), видається очевидним, що з метою правового забезпечення охорони об'єктів критичної інформаційної інфраструктури від кримінально-протиправних посягань, останні мають бути закріплені у системі ознак того чи іншого визначеного кримінального правопорушення. На жаль, наразі чинний КК не оперує поняттям «об'єкт критичної інформаційної інфраструктури» як ознакою кримінального правопорушення, хоча у ч. 2 ст. 259 та примітці до неї, а також у примітці до ст. 360 КК вживається термін «критично важливі об'єкти інфраструктури» з відсилкою до Закону України «Про основні засади забезпечення кібербезпеки в Україні» від 05.10.2017 р. № 2163-VIII. Слід відмітити, що наразі п. 16 ч. 1 ст. 1 даного Закону, який надавав визначення критично важливого об'єкта інфраструктури (об'єкта критичної інфраструктури) виключено на підставі набрання чинності Законом України «Про критичну інфраструктуру» від 16.11.2021 р. № 1882-IX, у п. 13 ч. 1 ст. 1 якого і міститься нині дане визначення. Як стверджують О. В. Таран та О. Г. Сандул, всі об'єкти критичної інфраструктури поділяють на фізичні, інформаційні та змішані [2, с. 64]. Так, згідно з п. 19 ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки в Україні» об'єктом критичної інформаційної інфраструктури є комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури. Тобто, по суті, об'єкт критичної інформаційної інфраструктури входить до значно більш широкого поняття «об'єкт критичної інфраструктури» (фізичного або змішаного), залишаючись при цьому цілісною, відносно самостійною (автономною) складовою останнього. На підставі вище викладених

законодавчих положень, на перший погляд, маємо констатувати, що за правилами формальної логіки об'єкт критичної інформаційної інфраструктури допустимо розглядати в межах поняття «критично важливі об'єкти інфраструктури», яким оперує КК, проте є низка суджень проти такого підходу.

По-перше, сутнісною характеристикою об'єкта критичної інформаційної інфраструктури, як випливає із законодавчого визначення цього поняття, є реальна або потенційна можливість вчинення кібератаки (дистанційного протиправного впливу із використанням інформаційно-комунікаційних технологій) щодо нього. Проте диспозицією ч. 2 ст. 259 КК передбачено, що критично важливі об'єкти інфраструктури мають бути об'єктами відповідного неправдивого повідомлення про підготовку вибуху, підпалу або інших дій… (очевидно, дій фізичного характеру і аж ніяк не дистанційного протиправного кібернетичного). До того ж родовим об'єктом даного кримінального правопорушення виступає громадська безпека. Тобто обґрунтовано припускаємо, що ч. 2 ст. 259 КК охороняє критично важливі об'єкти інфраструктури від завідомо неправдивого повідомлення про вчинення таких фізичних дій, що потенційно здатні швидко, результативно і однозначно порушити стан громадської безпеки. На відміну від зазначеного, повідомлення відомостей про підготовку якоїсь форми кібервтручання ще потребує ретельного аналізу та перевірки уповноваженими суб'єктами щодо ступеня загрози. Так, наприклад, за повідомленням прес-служби енергопостачальної компанії ПАТ «Прикарпаттяобленерго», датованим початком січня 2016 р., остання зіткнулася з масштабним відключенням електроенергії 23 грудня 2015 р. через стороннє втручання в роботу телемеханіки за допомогою програмного шкідливого забезпечення (як з'ясували фахівці СБУ), тобто мала місце кібератака. Очевидно, що сама компанія є об'єктом критичної інфраструктури, проте атака була спрямована на її інформаційно-комунікаційну складову, а навмисного пошкодження виключно фізичних складових активів компанії (трансформаторів тощо) зафіксовано не було. Таким чином, посягання (навмисні кримінально-протиправні діяння) на об'єкти критичної інформаційної інфраструктури здатні призвести до «каскадних» збоїв, при чому, як показують статистичні дані, енергетичний та інформаційний сектори є найбільш вразливими [1, с. 289].

Що стосується п. 2 примітки до ст. 360 КК, то в ній визначено таке: «Тяжкими наслідками у цій статті вважаються дії, що спричинили припинення надання телекомунікаційних послуг на критично важливі об'єкти інфраструктури». Зазначене положення тлумачить тяжкі наслідки, що настали внаслідок умисного пошкодження або руйнування телекомунікаційної мережі (ч. 3 ст. 360 КК). З аналізу положень ст. 360 КК (частин 1 та 2) не випливає, що пошкодження або руйнування (ч. 1 ст. 360 КК), пошкодження або руйнування, вчинене загальнонебезпечним способом (ч. 2 ст. 360 КК), здійснюється за допомогою кібератаки на об'єкти, які призначені забезпечувати надання телекомунікаційних послуг.

По-друге, відмінності (нетотожність) понять «об'єкт критичної інфраструктури» і «об'єкт критичної інформаційної інфраструктури»

простежується у численних спробах законодавця формалізувати об'єкти критичної інформаційної інфраструктури, як ознаки різних кримінальних правопорушень. Йдеться, зокрема, про Закон України «Про внесення змін до Закону України «Про судоустрій і статус суддів» та процесуальних законів щодо додаткових заходів захисту безпеки громадян» від 16.01.2014 р. № 721-VII (нині втратив чинність), яким КК було доповнено ст. 361-3, чим, серед іншого, було встановлено кримінальну відповідальність за несанкціоноване втручання в роботу критичних об'єктів національної інформаційної інфраструктури та у примітці до даної статті надано визначення зазначених об'єктів. Крім цього, проєктом Закону України № 8304 від 19.04.2018 р. та альтернативним йому проєктом Закону України № 8304-1 від 07.05.2018 р. пропонується окремі норми розділу XVI Особливої частини КК України (ст. ст. 361, 361-2, 362, 363, 363-1) доповнити такими обставинами, що обтяжують відповідальність: «вчинення стосовно об'єкта критичної інформаційної інфраструктури», «щодо інформації, яка оброблюється в об'єктах критичної інформаційної інфраструктури». Тому в умовах відсутності у чинному КК спеціальної норми про відповідальність за посягання на об'єкти критичної інформаційної інфраструктури (хоча Реєстр відповідних об'єктів вже функціонує в державі) все ж таки, як видається, відповідальність за такі кібератаки (які виступають, по суті, актами несанкціонованого втручання в роботу тих систем, що визнані критичними) має наставати за відповідними статями розділу XVI Особливої частини КК. Так, наприклад, чинною ч. 4 ст. 361 КК передбачена відповідальність за несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, якщо вони заподіяли значну шкоду чи створили небезпеку тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків. Наведена норма, зокрема, здатна забезпечити охорону таких загальних характеристик об'єктів критичної інформаційної інфраструктури, їх частин або систем, як важливість для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам. Звісно, що у певних випадках (наприклад, наявності ознак тероризму), необхідна кваліфікація за сукупністю кримінальних правопорушень.

Отже, розвиток правового забезпечення охорони об'єктів критичної інформаційної інфраструктури від кримінально-протиправних діянь слід визнати перспективним напрямом кримінального права. Дані об'єкти критичної інформаційної інфраструктури, як законодавче поняття мають бути формалізовані у нормах Особливої частини КК з притаманними їм характеристиками цілісної інформаційної системи.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Сокіран, М. В. (2023). Стан наукової розробленості проблем адміністративно-правового забезпечення безпеки та стійкості об'єктів критичної інформаційної інфраструктури. *Юридичний науковий*

*електронний журнал, 12, 287-291*. https://doi.org/10.32782/2524-0374/2023-12/70

2. Таран, О. В., Сандул, О. Г. (2019). Проблеми кримінальної відповідальності за посягання на об’єкти критичної інфраструктури в ядерній енергетиці. *Ядерна та радіаційна безпека, 3(83), 58-67*. https://doi.org/10.32918/nrs.2019.3(83).07

В.В. Мохор, О.В. Цуркан, Р.П. Герасимов, Т.М. Клименко, В.П. Яшенков,

# СОЦІОІНЖЕНЕРНИЙ АСПЕКТ ВИКОРИСТАННЯ ГЕНЕРАТИВНОГО ШТУЧНОГО ІНТЕЛЕКТУ

Використання генеративного штучного інтелекту зводиться до прикладного застосування обчислювальних методів для створення певного контенту. На основі навчальних даних можливе генерування відповідей на запитання, тексту, зображень, аудіо, програмного коду [1]. Це досягається застосуванням відповідних моделей генеративного штучного інтелекту, наприклад: ChatGPT, Gemini, Copilot, DALL-E. Їхнє впровадження дозволяє моделювати діяльність різноманітних дійових осіб. Однак, попри такі можливості нині спостерігається негативна тенденція до застосування генеративного штучного інтелекту зі зловмисною метою, зокрема, для отримання несанкціонованого доступу до інформації. Серед його моделей виокремлюються ChatGPT, FraudGPT, WormGPT [2]. Тому аналізування соціоінженерного аспекту використання генеративного штучного інтелекту актуальне.

У межах соціоінженерного аспекту об’єктом атаки є працівники організації. Їхні слабкості, потреби, манії (пристрасті), захоплення експлуатуються зловмисниками як уразливості. Маніпулювання ними дозволяє отримувати «несанкціонований» доступ до інформації. Це пов’язано з формуванням нової моделі поведінки працівника організації шляхом створення сприятливих умов реалізування загроз використання соціальної інженерії. Її типовими формами прояву є, наприклад: шахрайство, обман, афера, інтрига, містифікація, провокація [3]. Використання зазначених форм соціальними інженерами для формування нової моделі поведінки працівника організації може супроводжується за підтримання моделей генеративного штучного інтелекту. Тож існування негативної тенденції зростання його застосовності суттєво впливає на змінення ландшафту загроз використання соціальної інженерії [2, 3].

Застосування моделей генеративного штучного інтелекту орієнтоване як на створення і розповсюдження фішингових листів, так і допомогу соціальному інженеру адаптовувати свою стратегію в режимі реального часу [2, 4]. Так, ChatGPT може дозволяти моделювати вірогідний діалог зловмисника та працівника організації. Його застосування супроводжується підтримкою з боку чат-ботів, віртуальних помічників і водночас обмежується існуванням вбудованих елементів керування. Правдивість листування і створення підроблених вебресурсів досягається застосуванням моделі генеративного штучного інтелекту FraudGPT [2, 5]. Характерною її особливістю є відсутність вбудованих елементів керування і обмежень. Завдяки цьому порівняно з ChatGPT вона може виконувати неприйнятні запити, наприклад, створити шкідливе програмне забезпечення, підібрати пароль. Існування такої можливості пов’язане з призначенністю FraudGPT для полегшення реалізування загроз кібербезпеці, зокрема, й соціальної інженерії [5]. Це

призводить до її використання навіть зловмисниками-початківцями. Наприклад, створення фішингового листа супроводжується вказуванням мінімального обсягу інформації – назви або напрямку діяльності організації. У даному випадку вона виступає як віртуальний помічник, який вказує що та як формулювати [2, 5]. За аналогією з FraudGPT, підвищення успішності реалізування загроз використання соціальної інженерії забезпечується також і моделлю генеративного штучного інтелекту WormGPT. Її упровадження окрім написання шкідливого програмного забезпечення, вільного володіння іноземною мовою дозволяє створювати фішингові листи, радити при плануванні реалізування загроз. Найбільш типовими завданнями, що вирішуються за допомогою WormGPT, є генерування переконливих листів і, як наслідок, компрометування електронної пошти. До того ж виокремлюється функційна можливість створення шкідливого програмного коду мовою Python Таке використання як і FraudGPT позбавлене обмежень [2, 6].

Отже, характерною особливістю зазначеного аспекту використання генеративного штучного інтелекту є забезпеченість реалізування загроз соціальної інженерії від стадії підготовлення до адаптивного реалізування. Це може призводити до його застосування соціальними інженерами початківцями. При цьому ключовими вимогами залишаються доступність моделей ChatGPT, FraudGPT, WormGPT і вміння їх застосовувати на практиці. Поряд з цим варто відмітити й існування позитивної тенденції до застосування генеративного штучного інтелекту для вирішення завдань забезпечення інформаційної і кібер-безпеки, наприклад [7], білими (етичними) хакерами.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

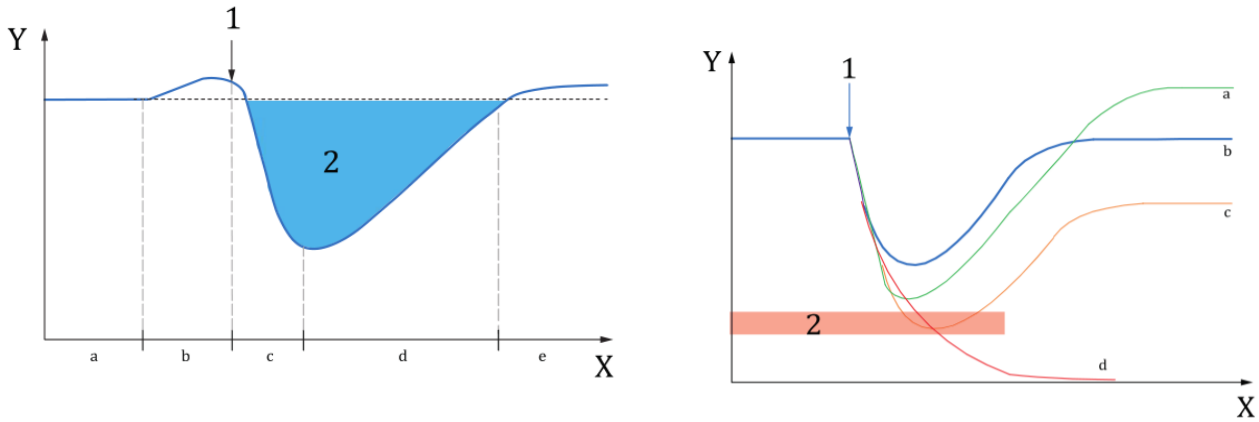

1. Feuerriegel S., Hartmann J., Janiesch C. et al. Generative AI. *Business & Information Systems Engineering*. 2024. Vol. 66, Iss. 1. P. 111–126. DOI: https://doi.org/10.1007/s12599-023-00834-7.
2. Falade P.V. Decoding the Threat Landscape : ChatGPT, FraudGPT, and WormGPT in Social Engineering Attacks, *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*. 2023. Vol. 9, Iss. 5. P. 185–198. DOI: https://doi.org/10.32628/CSEIT2390533.
3. Мохор В. В., Цуркан О. В., Цуркан В. В., Герасимов Р. П. Оцінювання захищеності інформації в комп’ютерних системах за соціоінженерним підходом. *Information Technologies and Security :* selected papers of the XVI International scientific and practical conference (Kyiv, 30 November 2017). Aachen, Germany, 2018. Vol. 2067. P. 92–98. URL: http://ceur-ws.org/Vol-2067/paper13.pdf.
4. Saha Roy S., Thota P., Naragam K., Nilizadeh S. From Chatbots to Phishbots? : Phishing Scam Generation in Commercial Large Language Models. *Security and Privacy* : IEEE Symposium (San Francisco, USA, 19–23 May 2024). 2024. P. 221–221. DOI: https://doi.org/10.1109/SP54263.2024.00182.
5. Amos Z. What Is FraudGPT? URL: https://hackernoon.com/what-is-fraudgpt.
6. Master ChatGPT for Ethical Hackers! URL: https://iclass.eccouncil.org/master-chatgpt-for-ethical-hacking/#chapter-5.

В.В. Мохор, О.О. Бакалинський, Я.Ю. Дорогий, В.В. Цуркан

# ПАРАДИГМА НОВИХ РИЗИКІВ КІБЕРБЕЗПЕКИ

Діяльність будь-якої організації незалежно від типу, розміру та природи направлена на досягнення поставленої мети [1]. Цьому сприяє глобальна мережа Інтернет, яка з одного боку є середовищем для обміну інформацією. Тоді як з іншого – джерелом нових ризиків кібербезпеки [2]. Тож запорукою діяльності організацій є здатність реагувати на змінювання як внутрішніх, так і зовнішніх обставин [3]. У даному випадку ключовою вимогою ефективного управління новими ризиками кібербезпеки є можливість передбачення, підготовлення і реагування організаціями на будь-які змінення обставин їх діяльності [4, 5]. Насамперед це досягається реагуванням на неочікувані або маловірогідні ризики з боку глобальної мережі Інтернет. Крім того відновленням нормального функціонування після виникнення нових ризиків кібербезпеки. І, що не менш важливе, адаптуванням до таких проявів небезпек [1–3]. Тож здатність організацій засвоювати, відновлювати та адаптовувати свою діяльність до мінливих обставин визначає організаційну резильєнтність (рис. 1, а) [3]. Цим обумовлюється актуальність аналізування парадигми нових ризиків кібербезпеки.

Під новим (емерджентним) ризиком кібербезпеки (англ. emerging cybersecurity risk) розуміється ризик зі значною невизначеністю, що призводить до настання серйозних наслідків (рис. 1, б[c, d]). З огляду на типове його тлумачення [4], це вказує, по-перше, на відсутність або незначний обсяг даних про вразливості, загрози, наслідки. По-друге, виникнення нового ризику кібербезпеки може призвести до припинення діяльності організації (рис. 1, б[d]).




а) реалізування сценарію:
1 – настання нового ризику;
2 – припинення діяльності;
[a] ідентифікування нового ризику;
[b] передбачення/підготовлення;
[c] поглинання/витримування;
[d] реагування/відновлення;
[e] адаптування/трансформування

б) наслідки реалізування сценарію:
1 – настання нового ризику;
2 – межі стрес-тестування;
[a] діяльність покращилася;
[b] діяльність не змінилася;
[c] діяльність призупинилася;
[d] діяльність припинилася

Рисунок 1 – Приклад впливання сценарію нового ризику кібербезпеки на діяльність організації: X – тривалість реалізування сценарію, Y – діяльність організації [3]

Залежно від змінення обставин діяльності організації природа нових ризиків кібербезпеки визначається [3]:

- проігнорованими або не відчутними ризиками;
- відомими ризиками в новому або незнайомому інтерпретуванні;
- ризиками зі значним розвитком;
- системними ризиками;
- новим комбінуванням ризиків.

Належність нових ризиків кібербезпеки до однієї з виокремлених груп визначається відповідними факторами, а саме [3]:

- знання (невідомі зміни обставин діяльності організації, недостатньо даних для визначення імовірності (вірогідності) та наслідків);
- волатильність (швидкі, непередбачувані зміни умов або обставин, впливання невідомого фактору, нестабільність інформації);
- невизначеність (перехід від ранніх попереджень до нових ризиків, визначення джерел нових ризиків);
- складність (системний характер або взаємодіяння нових ризиків з іншими ризиками);
- неоднозначність (можливість різноманітних інтерпретувань наявних даних, незрозумілість причин змінення обставин діяльності організації).

Характерною особливістю урахування даних факторів є мінливість з часом. Це стосується доступності інформації для ідентифікування, аналізування, зіставлення і, як наслідок, обробляння нових ризиків кібербезпеки [3, 5]. До того ж накопичення, аналізування, інтерпретування даних для прийняття рішення про необхідність і обирання варіантів їх обробляння. Крім того, в окремих випадках, запорукою ідентифікування нових ризиків є можливість зіставлення з подібними ризиками, зокрема, завдяки наявності інформації про них [5].

Отже, нові ризики кібербезпеки характеризуються значною невизначеністю і настанням серйозних наслідків, наприклад, припиненням діяльності організації. Їх поява здебільшого обумовлена часовою мінливістю внутрішніх і зовнішніх обставин. Тож здатністю організації передбачати, готуватися, реагувати на такі зміни обумовлюється ефективність управління новими ризиками кібербезпеки і в кінцевому випадку забезпечується організаційна резильєнтність.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. ISO/IEC 27000:2018. Information technology. Security techniques. Information security management systems. Overview and vocabulary. [Valid from 2018-02-07]. URL: https://www.iso.org/standard/73906.html.
2. ISO/IEC FDIS 27032:2023. Cybersecurity. Guidelines for Internet security. [From 2023-05-09]. URL: https://www.iso.org/standard/76070.html.
3. ISO/ TS 31050:2023. Risk management. Guidelines for managing an emerging risk to enhance resilience. [Valid from 2023-10-27]. URL: https://www.iso.org/standard/ 54224.html.
4. ISO 31000:2018. Risk management. Guidelines. [Valid from 2018-02-14]. URL: https://www.iso.org/standard/65694.html.
5. IEC 31010:2019. Risk management. Risk assessment techniques. [Valid from 2019-06-17]. URL: https://www.iso.org/standard/72140.html.

**ЗМІСТ**

**МАТЕРІАЛИ**

**НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ**
**«КІБЕРБЕЗПЕКА ЕНЕРГЕТИКИ»**
**29 травня 2024 року**

Відповідальні за випуск:

О.В. Цуркан, Т.М. Клименко

**Місце проведення:** Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України; м. Київ, вул. Генерала Наумова, 15. Їхати від станції метро «Академмістечко» автобусом № 97, № 97к або марш. таксі № 200к, № 408, № 437 до зупинки «Інститут моделювання».

**З питаннями щодо конференції звертатися**:

ІПМЕ ім. Г.Є. Пухова НАН України, вул. Генерала Наумова, 15, кім. 303, Цуркан Оксана володимирівна, тел. 424-91-62, 068-014-57-22, e-mail: otsurkan24@gmail.com

Інститут проблем моделювання в енергетиці
ім. Г. Є. Пухова НАН України,
вул. Генерала Наумова, 15, Київ, 03164, Україна,
тел.: +38 044 424 91 62, факс: +38 044 424 10 63
веб сайт: https://ipme.kiev.ua/