НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

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

МАТЕРІАЛИ VI НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ «БЕЗПЕКА ЕНЕРГЕТИКИ В ЕПОХУ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ»

13 грудня 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 № 12 від 28 листопада 2024 р.)

Б-39 **Безпека енергетики** в епоху цифрової трансформації, VI науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України : матеріали (Київ, 13 грудня 2024 р.). Київ : ІПМЕ ім. Г.Є.Пухова НАН України, 2024. 191 с.

В-39 **Energy security** in the digital transformation era, VI scientific-practical conference of the G.E. Pukhov Institute for Modeling in Energy Engineering National Academy of Sciences of Ukraine : materials (Kyiv, December 13, 2024). Kyiv: PIMEE NAS of Ukraine, 2024. 191 p.

НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ
ім. Г.Є. ПУХОВА НАН УКРАЇНИ

МАТЕРІАЛИ
VI НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

БЕЗПЕКА ЕНЕРГЕТИКИ В ЕПОХУ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

13 грудня 2024 року

м. Київ

2024

Вельмишановний учасник _____

_____

Запрошуємо Вас прийняти участь в роботі VI науково-практичної конференції «Безпека енергетики в епоху цифрової трансформації», яка буде проходити 13 грудня 2024 року в Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України (м. Київ).

ОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ

Інститут 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, професор,
заступник директора з наукової роботи

Артемчук Володимир Олександрвич
доктор технічних наук,
заступник директора з науково-організаційної роботи

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

ОРГАНІЗАЦІЙНИЙКОМІТЕТ

Артемчук Володимир Олександрвич
доктор технічних наук,
заступник директора з науково-організаційної роботи

Клименко Тетяна Михайлівна
завідувачка науково-організаційного відділу

Цуркан Оксана Володимирівна
молодший наковий співробітник

Ю.П. Величко

ТРАНСФОРМАЦІЯ ЕНЕРГОГЕНЕРАЦІЇ В УКРАЇНІ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ НА СУЧАСНОМУ ЕТАПІ

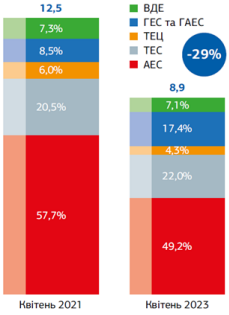
Енергетичний сектор України знаходиться в стані глибокої трансформації та адаптації до нових викликів. В умовах війни, що триває, енергосистема зазнає надзвичайних навантажень через постійні атаки на інфраструктурні об'єкти. Основні проблеми включають нестабільність електропостачання, залежність від викопного палива та необхідність зниження техногенного впливу на довкілля. Ці виклики є особливо актуальними для української енергосистеми, оскільки воєнний конфлікт не тільки загострює старі проблеми, але й дає нові, пов'язані з безпекою енергопостачання та стійкістю інфраструктури. У цих умовах пошук нових підходів до забезпечення енергетичної безпеки та ефективності набуває більшої актуальності.

До війни Україна мала добре розвинену систему енергогенерації, до якої входили атомні, теплові, гідро- та відновлювані потужності. Однак з початком повномасштабних бойових дій значна частина цих потужностей була пошкоджена або окупована.

З жовтня 2022 року по вересень 2024 року об'єкти української енергетичної інфраструктури зазнали 1024 російських атаки [1].

Крім того, було пошкоджено/втрачено 24 об'єкти генерації (ТЕС – 3,8 ГВт, ТЕЦ – 1 ГВт, ГЕС – 540 МВт, ГАЕС – 650 МВт), що становить близько 6 ГВт загальної потужності. Без цього, через окупацію значних територій, Україна втратила доступ до понад 50% потужностей ТЕЦ – 1,5 ГВт, 74% ТЕС – 7 ГВт та 25% АЕС – 6 ГВт, що загалом становить більше ніж 14,5 ГВт. Такий масштаб втрат суттєво вплинув на загальний енергобаланс і підвищив ризики енергетичної нестабільності [2].

Приклад динаміки і структури генерації представлено на Діаграмі 1 [3]:



Діаграма 1 – Динаміка і структура генерації в квітні 2023, ТВт год

Як видно з Діаграми 1, атомна енергетика завжди була основним джерелом генерації в Україні.

У 2024 році на енергоблоці №4 розпочали експлуатацію ядерного палива виробництва американської компанії Westinghouse. Нині чотири ядерні установки РАЕС частково завантажені американським ядерним паливом. Поступово залишки російських ТВЕЛів будуть замінені на паливо Westinghouse [4].

У строковий перспективі це забезпечить енергетичну незалежність в атомній енергетиці від РФ та підвищить безпеку енергопостачання.

Другим за встановленою потужністю і обсягами виробництва електроенергії в Україні залишається теплова генерація.

Вагомою зміною в тепловій енергетиці у 2023 році можна вважати частковий перехід ТЕС з використання вугілля на природний газ та мазут, що пов'язано із ускладненням видобутку вугілля та труднощами із його імпортом [3].

Близько 2 ГВт пошкодженої потужності ТЕС потенційно можуть бути відновлені протягом 1-2 років [5].

Гідроенергетика є важливою складовою енергетики України, зокрема через збалансовану здатність забезпечити швидкий доступ до маневрових потужностей у пікових моментах. Втім, військові дії завдали значної шкоди і цьому сектору.

Відновлювальна енергетика (ВДЕ) набула особливої актуальності в умовах воєнного часу. Через значні пошкодження і окупацію теплових та атомних потужностей роль вітрових, сонячних та біоенергетичних станцій стає дедалі важливою. За даними Національного плану дій з відновлюваної енергетики Україна планує довести збір ВДЕ до 27% у загальному кінцевому споживанні енергії до 2030 року. Для цього планується побудувати 6,1 ГВт наземних вітрових станцій, 12,2 ГВт сонячних станцій, 876 МВт біоенергетичних та 40 МВт геотермальних потужностей [6].

Україна значно збільшила обсяг імпорту електроенергії з ЄС. Збільшення з 1 грудня 2023р. пропускних спроможностей для імпорту електроенергії з європейських країн з 1,2 ГВт до 1,7 ГВт [7] дозволило посилити енергетичну безпеку України і частково покривати дефіцит потужностей під час пікових навантажень.

Гармонізація з європейським енергетичним ринком не лише покращує стабілізацію української енергосистеми, але й відкриває можливості для майбутньої інтеграції України в європейську енергосистему ENTSO-E, що дозволить забезпечити більш стійке енергопостачання.

За останні кілька років прийнято 3 стратегічних документа, які визначають перспективи розвитку вітчизняної електроенергетики, а саме: Оновлений національний визначений внесок України до Паризької Угоди (НВВ2), Національний план з енергетики та клімату до 2030 року та Енергетична стратегія України до 2050 року.

Важливу роль у відновленні енергетичного сектору України відіграють цифрові технології. Зокрема, впровадження систем Smart Grid, які сприяють оптимізації управління енергетичними потоками, а також цифрового моніторингу стану енергетичної інфраструктури, що дозволяє виявляти та прогнозувати аварії. Застосування цих інновацій підвищить стійкість та ефективність енергетичної системи країни.

У планах українського уряду є як ремонт пошкоджених об’єктів, так і будівництво нових маневрових потужностей, які швидко реагуватимуть на коливання попиту.

З огляду на величезні втрати енергетичної інфраструктури, основні напрямки розвитку мають стати відновлення пошкоджених об'єктів, розбудова та модернізація існуючих потужностей, розширення відновлюваних джерел енергії, подальша інтеграція з європейськими енергетичними системами, а також впровадження розподіленої генерації.

1. Галущенко Г.В. (2024). *За два роки росія атакувала українську енергетику понад 1000 разів України Герман Галущенко*. Міністр енергетики. https://mev.gov.ua/novyna/za-dva-roky-rosiya-atakuvala-ukrayinsku-enerhetyku-ponad-1000-raziv-herman-halushchenko.
2. Сігал О.І. (2024). *Розподілена когенерація-технічний, екологічний та економічний виклик централізованому теплопостачанню*. IX Міжнародний конгрес інженерів-енергетиків. Інститут технічної теплофізики НАН України. https://www.iec-expo.com.ua/5e-2024/konhres-2024.html; https://cigre.org.ua/wp-content/uploads/2024/10/sigal.pdf.
3. Українська вітроенергетична асоціація. (2024). *ВІТРОЕНЕРГЕТИЧНИЙ СЕКТОР УКРАЇНИ 2023. Огляд Ринку*. (с. 17-18).
4. Рівненська АЕС. (2024). «*Енергія»-Інформаційний вісник Рівненської АЕС 26 вересня 2024р.* (с. 3). https://www.facebook.com/share/p/1EaTb22dFi/.
5. Ю. Кубрушко, Г. Цахманн, О. Гружинська, В. Коваль. (2024). *Залучення приватних інвестицій у розвиток маневреної генерації*. (с. 4). GreenDealUkraina.org. https://greendealukraina.org/uk/products/analytical-reports/encouraging-private-investments-into-flexibility.
6. Журнал Forbes Ukraine. (2024). *Курс за вітром – чому вітрова генерація має стати пріоритетним напрямком розвитку енергетики України*. https://forbes.ua/money/kurs-za-vitrom-chomu-vitrova-generatsiya-mae-stati-prioritetnim-napryamkom-rozvitku-energetiki-ukraini-30082024-23148.
7. Галущенко Г.В. (2023). *До 1,7 ГВт: збільшено пропускні спроможності для імпорту електроенергії з ЄС*. Міністр енергетики. https://www.kmu.gov.ua/news/do-17-hvt-zbilsheno-propuskni-spromozhnosti-dlia-importu-elektroenerhii-z-ies.

Ye. Kotukh

THE APPLICATION OF QUANTUM MACHINE LEARNING IN CRYPTOGRAPHY

The convergence of Quantum Machine Learning (QML) with cryptographic systems represents a significant paradigm shift in information security methodology and implementation. This analysis examines the theoretical foundations, practical applications, and implications of this integration, with particular emphasis on cryptanalytic capabilities and defensive measures.

The theoretical framework underlying QML applications in cryptography rests fundamentally on quantum mechanical principles, specifically superposition and entanglement. The quantum bit (qubit) state representation, described by $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $|\alpha|^2 + |\beta|^2 = 1$, enables computational capabilities that transcend classical limitations. This quantum framework, when integrated with machine learning methodologies, creates a synergistic system capable of enhanced pattern recognition in high-dimensional Hilbert spaces and optimization through quantum tunneling effects.

The mathematical formulation for QML-based cryptanalysis considers a cryptographic system C with key space K, where the quantum state $|\psi\rangle$ represents a superposition of all possible keys: $|\psi\rangle = \Sigma_k c_k|k\rangle, k \in K$. The quantum machine learning algorithm A operates on this state to optimize the probability amplitude c_k of the correct key, fundamentally altering the approach to cryptanalytic attacks.

Contemporary implementations demonstrate significant advancements in several critical areas. Shor's algorithm, a cornerstone of quantum cryptanalysis, has been enhanced through QML optimization, particularly in period-finding efficiency and error correction through learned noise models. The development of post-quantum cryptography benefits from automated security parameter optimization and quantum-resistant algorithm validation. These implementations have demonstrated measurable improvements in computational efficiency and security robustness.

The security implications of QML integration are profound and multifaceted. The threat landscape is characterized by the exponential acceleration of certain cryptanalytic attacks and enhanced capabilities for side-channel analysis. Particularly vulnerable are systems in transition periods between classical and quantum implementations. Defensive strategies necessarily include the implementation of quantum-resistant algorithms, dynamic security parameter adaptation, and machine learning-enhanced intrusion detection systems. These countermeasures must evolve continuously to address emerging quantum computational capabilities.

Technical challenges persist in several critical areas. Quantum decoherence management remains a significant obstacle to practical implementation, as does the scalability of quantum systems and their integration with existing cryptographic infrastructure. The development of error correction mechanisms and noise-resistant protocols continues to be an active area of research, particularly in the context of cryptographic applications where error tolerance is minimal.

The economic implications of QML integration in cryptographic systems are substantial. Infrastructure transition costs, market competition dynamics, and security investment requirements will significantly impact organizational and national security strategies. Policy frameworks must address international standardization, regulatory compliance, and security certification protocols. The development of comprehensive

standards for quantum-enhanced cryptographic systems remains a critical challenge for the international security community.

Research trajectories in this field are diverse and rapidly evolving. The development of hybrid classical-quantum cryptographic systems represents a promising intermediate approach, allowing for gradual transition while maintaining security assurance. Implementation of adaptive security protocols and investigation of quantum-native encryption methodologies continue to advance our understanding of secure communication in a quantum-enabled environment.

Methodological approaches in QML-based cryptanalysis primarily manifest through Quantum Neural Networks (QNNs) for pattern analysis in cipher texts, Quantum Support Vector Machines (QSVMs) for classification of cryptographic weaknesses, and quantum annealing processes for optimization in key search spaces. These approaches demonstrate superior performance in specific cryptanalytic tasks compared to classical methods, particularly in pattern recognition and feature extraction from encrypted data.

The societal implications of these developments extend beyond technical considerations. The potential for quantum computers to compromise current encryption methods raises significant concerns regarding data privacy and national security. Economic considerations, including transition costs and market dynamics, will significantly impact adoption rates and security practices. International cooperation in developing regulatory frameworks and standards for quantum cryptography becomes increasingly critical as these technologies mature.

The successful integration of QML in cryptographic systems requires careful consideration of practical implementation challenges. These include hardware requirements, energy consumption, and system complexity. The development of efficient quantum algorithms that can operate within these constraints while maintaining security assurance remains an active area of research.

Future developments in this field will likely focus on improving the efficiency of quantum algorithms, developing more robust error correction methods, and creating practical implementations of quantum-resistant cryptographic systems. The continued evolution of QML capabilities suggests that cryptographic systems must maintain adaptability while ensuring security against both classical and quantum attacks.

This comprehensive analysis demonstrates that the integration of Quantum Machine Learning with cryptographic systems represents not merely a technological advancement but a fundamental transformation in information security methodology. The continued development of these technologies, coupled with appropriate security measures and regulatory frameworks, will define the future of secure communication in the quantum era.

1. Kotukh Y., Khalimov G., Hard problems for non-abelian cryptography, 2021: Fifth International Scientific and Technical Conference Computer And Information Systems And Technologies, 2021, pp. 39-40, https://doi.org/10.30837 /csitic52021232176.
2. Kotukh, Y., Khalimov, G., Korobchynskyi, M., Rudenko, M., Liubchak, V., Matsyuk, S., & Chashchyn, M. (2024). Research horizons in group cryptography in the context of post-quantum cryptosystems development. *Radiotekhnika*, *1*(216), 62–72. https://doi.org/10.30837/rt.2024.1.216.05.
3. Kotukh E., Severinov O., Vlasov A., Tenytska A., & Zarudna E. (2021). Some results of development of cryptographic transformations schemes using non-abelian groups. Radiotekhnika, 1(204), 66–72. https://doi.org/10.30837/rt.2021.1.204.07.

Д.В. Бондаренко

ЕЛЕКТРИЧНЕ МОДЕЛЮВАННЯ ФОТОЕЛЕКТРИЧНИХ ДЖЕРЕЛ ЕНЕРГІЇ ДЛЯ РОЗПОДІЛЕНИХ МЕРЕЖ

Одним із кроків забезпечення безпеки енергетики є впровадження розподілених енергетичних мереж з застосуванням розподіленої генерації. Розподілені енергетичні мережі, особливо які базуються на великій кількості невеликих мереж (мікромереж) потребують організації узгодженої роботи та інтелектуального керування [1]. Сучасні пристрої, які основані на мікропроцесорній та мікроконтролерній техніці можуть здійснювати керування з урахуванням результатів імітаційного моделювання, навіть в реальному часі. Крім того, моделювання є потужним інструментом дослідження, проектування та впровадження різноманітних технологічних рішень в енергетичних системах.

Сонячна енергетика, а саме фотоелектричні джерела електричної енергії є перспективним напрямком побудови розподілених енергетичних мереж. Зазначимо, що для впровадження мікромереж з фотоелектричними джерелами енергії необхідно проводити моделювання з урахуванням усіх можливих параметрів.

Основою моделювання фотоелектричних систем є побудова електричних моделей генеруючих пристроїв. Для побудови електричної моделі сонячного фотоелектричного елемента зручно використовувати принцип аналогій. Згідно такому принципу потоку фотонів, які падають на фотоелектричний перетворювач, відповідає електричний струм електричної моделі (I), а енергії фотона, який поглинається напівпровідниковою структурою – напруга електричної моделі (U):

$$\frac{ne}{t} \to I\,, \tag{1}$$

$$\frac{h\nu}{e} \to U\,, \tag{2}$$

де n – кількість фотонів, яка поглинута напівпровідником; e – елементарний заряд; h – постійна планка; ν – частота фотона; t - час.

Треба відмітити, що ключовим елементом такого представлення на основі аналогій є потужність. Як потужність електромагнітного випромінювання сонця, так і електрична потужність, яка отримується з фотоелектричного модуля. Акцентуємо, що використання потужності є одним з основних видів представлення енергетичних процесів. Бачимо що:

$$P = UI = \frac{h\nu}{e}\frac{ne}{t}. \tag{3}$$

Зазначимо, що вираз (3) описує не потужність сонячного випромінювання, яке падає на панель, а вихідну потужність пов'язану з поглинанням фотонів, та не враховує втрати на поглинання без створення електронно-діркових пар, втрати на відбиття фотонів, втрати на рекомбінацію носіїв заряду та інші дисипативні процеси.

Таким чином, будуємо електричну модель (Рисунок 1), яка об'єднує джерело струму і джерело напруги.

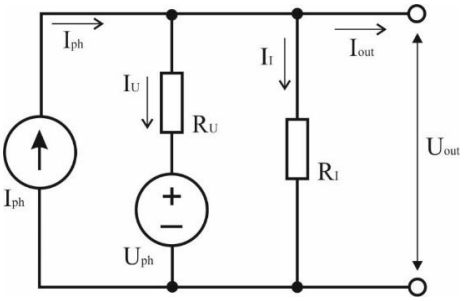


Рисунок 1 – Електрична модель фотоелектричного перетворювача

Вирази для струмів і напруг електричної моделі фотоелектричного джерела (Рисунок 1) мають вигляд:

$$I_{out} = I_{ph} + I_U + I_I \,, \tag{3}$$

$$U_{out} = U_{ph} + U_{Ru} \,, \tag{4}$$

$$U_{Ru} = I_U R_U \,, \tag{5}$$

де I_{ph} – струм процесу перетворення фотонів в носії заряду; I_I – струм внутрішнього опору джерела струму; I_U – струм джерела напруги; I_{out} – вихідний струм фотоелектричного джерела; R_U – внутрішній опір джерела струму; U_{ph} – напруга процесу перетворення фотонів в носії заряду; U_{Ru} – напруга на внутрішньому опорі джерела напруги; U_{out} – вихідна напруга фотоелектричного джерела.

Для подальшої побудови енергетичної системи також використовують електричну модель накопичувача, яким може бути або конденсатор, або іоністор [2], або електрохімічний акумулятор [3]. Крім того моделюється підключення навантаження.

Розподілена електрична мережа передбачає з'єднання генеруючих та зберігаючих пристроїв в мережу [4]. Електричні моделі дозволяють це робити, залучаючи в електричні кола моделей реальні електронні схеми готових пристроїв перетворення електричної енергії, таких як понижувальні чи підвищувальні перетворювачі, інвертори та конвертори.

В загальному розумінні, для утворення розподіленої мережі змінного струму з відокремлених фотоелектричних генераторів потрібно мати окрім фотоелектричних модулів (PV-module), ще й контролер заряду (MPPT-control), вузол підвищення напруги (flyback converter), перетворювач з постійного струму в змінний (full bridge inverter) та модуль узгодження з мережею (grid control), так як такі параметри мережі, як амплітуда, частота та фаза, повинні бути узгоджені [5]. Таким чином система виглядає наступним чином (Рисунку 2):

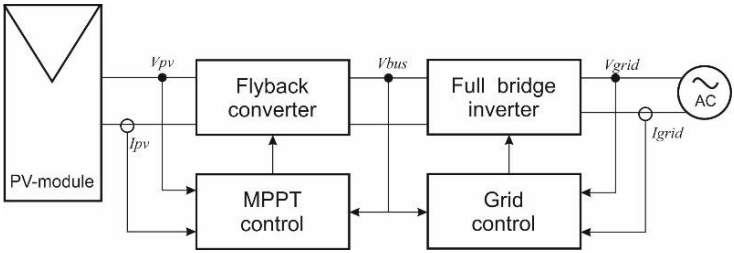


Рисунок 2 – Схема підключення фотоелектричного модуля до мережі

Отже резюмуємо, що цифрова трансформація нашої держави спонукає до використання передових технологій моделювання та сучасних керувальних систем, для реалізації потужної мережі розподіленої генерації на основі програмно керованих комплексів з застосуванням відновлюваних джерел енергії. А інструменти пов'язані з моделюванням можуть пришвидшити цей процес та застосувати ефективні рішення.

1. Bondarenko, D., Matiakh, S., Surzhyk, T., Sheiko, I., & Kravchenko M. (2024). Development trends of solar power engineering based on the materials of the scientific and practical conference "Renewable energy and energy efficiency in the 21 centuries". *Vidnovluvana Energetika*, 3(78), 76-83. https://doi.org/10.36296/1819-8058.2024.3(78).76-83.
2. Бондаренко, Д. Моделювання роботи фотоелементів з використанням іоністорів. (2020). *Відновлювана енергетика та енергоефективність у 21 столітті: Матеріали міжнародної науково-практичної конференції* (с. 288-292). Інститут відновлюваної енергетики НАН України.
3. Bondarenko, D. (2019). Equivalent circuits of electric power accumulators connected to solar photocell. *Vidnovluvana Energetika*, 3(58), 30-34. https://doi.org/10.36296/1819-8058.2019.3(58).30-34.
4. Bondarenko, D., Matyakh, S., Surzhyk, T., & Shevchuk, V. (2023). Energy unit kit for photovoltaic cluster. *Vidnovluvana Energetika*, 3(74), 53-58. https://doi.org/10.36296/1819-8058.2023.3(74).53-58.
5. Bondarenko, D., & Matyakh, S. (2024). Using microinverters for photovoltaic cluster. *Vidnovluvana Energetika*, 1(76), 51-56. https://doi.org/10.36296/1819-8058.2024.1(76).51-56.

O. Ogir

ENERGY SECURITY IN THE ERA OF DIGITAL TRANSFORMATION: VIEWS ON THE UKRAINIAN STRUGGLE

The strategic importance of Ukraine's infrastructure. Since Russia invaded Ukraine in 2022, the country's energy and water distribution systems have faced relentless cyber and physical attacks. As a vital part of Europe's energy network, Ukraine's infrastructure plays a key role in maintaining regional stability. But its strategic importance has also made it a prime target for efforts to destabilize not only Ukraine, but Europe as a whole.

One of the most shocking wake-up calls came in 2015, when a cyber-attack knocked out Ukraine's power grid, causing blackouts that affected 225,000 people for hours. It was the first time a national power grid had been successfully attacked in this way, sending a clear message about how vulnerable critical infrastructure can be to cyberattacks. An investigation later revealed that sophisticated malware was being used to breach control systems, ushering in a new era of cyberwarfare that could have devastating effects in the real world.

Since then, Ukraine has been under constant digital siege. In 2017, the NotPetya malware attack caused massive disruption across multiple sectors, and it became clear that cyber threats are increasingly intertwined with geopolitical tensions. More recently, in October 2022, cyber-attacks on Ukraine's power grid were coordinated with missile strikes, showing how the two forms of attack can work together to destabilize a country. This "hybrid war" has shown even more clearly that Ukraine needs stronger defenses to protect its vital infrastructure. An analytical report by the responsible state body[1] reported 55 cyber incidents in the energy sector of Ukraine, including 8 critical incidents with registered consequences, created by Russian hacker groups in the first half of 2023. Russia-backed groups also carried out 62 attacks on telecom sector. In December 2023, a large-scale attack took place on the largest Ukrainian mobile operator, Kyivstar, which serves 25 million subscribers. This attack coincided with the missile strikes in December 2023, which resumed after a long lull.

In addition to cyber-attacks, Ukraine has faced a surge in physical attacks on its infrastructure. Power stations, substations and water treatment facilities were deliberately hit by Russian missiles and artillery. These attacks left millions of people without electricity and clean water. In Kyiv and other regions, repeated strikes at power distribution centers led to emergency shutdowns, resulting in massive power outages and water shortages for hundreds of thousands of people[1,2].

The impact of these attacks goes far beyond the borders of Ukraine. They threaten the uninterrupted supply of energy resources to Europe and pose a risk to European security. The combination of digital and physical attacks underscores how complex and unpredictable today's infrastructure threats have become.

[1] https://cip.gov.ua/services/cm/api/attachment/download?id=64621

Strengthening defenses for the future. Ukraine's experience is a powerful reminder of the urgent need for better protection of critical infrastructure, especially in hybrid warfare. The country's energy and water systems are under constant threat from both cyber and physical attacks. A failure at one facility doesn't just cause a disruption in operations—it can set off a chain reaction that affects many other parts of society. This makes it clear that comprehensive security strategies are essential.

This is where **Horizon Europe projects** [3] can play a crucial role in addressing some of these challenges. Horizon Europe, the EU's main research and innovation program, funds projects aimed at strengthening cyber security, increasing the resilience of infrastructure and developing advanced technologies to combat hybrid threats. By cooperating with European partners, Ukraine can gain access to advanced research and solutions that can improve the security of its energy and water networks. These projects also promote cross-border cooperation, allowing countries to share best practices and build a collective defense against emerging cyber and physical threats.

By constantly testing and improving emergency response systems, Ukraine can identify weaknesses and improve its resilience. Strengthening cyber security, strengthening physical defenses and fostering collaboration between infrastructure operators and government are key steps to building a more secure future.

Additionally, conducting a detailed risk assessment and integrating this information into broader infrastructure management plans will help address potential vulnerabilities before they become critical. If Ukraine can successfully protect its infrastructure, it will not only secure its own future, but also contribute to the stability of Europe as a whole.

Conclusion. Ukraine's ongoing struggle to protect its critical infrastructure provides vital lessons about the importance of energy security in the digital age. The combination of cyber-attacks and physical attacks reveals the need for a more comprehensive approach to protection that combines digital security with physical protection. As Ukraine strengthens the protection of its infrastructure, it is setting an example for other countries facing similar threats. Horizon Europe projects offer a valuable opportunity to address these challenges by supporting innovation and fostering international cooperation. Ensuring the stability of these systems is important not only for the security of Ukraine, but also for the stability of interconnected energy and utility networks in Europe.

1. Tagabe, P. M. (2022, November 8). How to protect critical infrastructure from Cyber Threats. Infrastructure Magazine. Retrieved February 8, 2023, from https: // infrastructuremagazine.com.au / 2022 / 11 /04/ how-toprotect-critical-infrastructure-from-cyber-threats/.
2. Critical Infrastructure Cyber Security Solutions. Huntsman. (2021, May 6). Retrieved February 13, 2023, from https://www.huntsmansecurity.com/ industries/ critical-infrastructure.
3. *Horizon Europe* supports research on building resilience in infrastructure, with a focus on cybersecurity, energy security, and defense against hybrid threats. Information about Horizon Europe and its projects can be found on the European Commission's website: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/home.

О.С. Кобус, С.Ю. Бондаренко

БЕЗПЕКА ФІЗИЧНОГО РІВНЯ В КОМУНІКАЦІЯХ SMART GRID: ДОСЛІДЖЕННЯ КВАНТОВОЇ КРИПТОГРАФІЇ ТА ЦІЛІСНОСТІ СИГНАЛУ В ЕНЕРГЕТИЧНИХ МЕРЕЖАХ

Інтеграція інформаційно-комунікаційних технологій (ІКТ) із сучасною електричною інфраструктурою перетворила традиційні енергетичні системи на високоефективні, взаємопов'язані та «розумні» мережі. Однак ця еволюція принесла безліч вразливостей, особливо на фізичному рівні зв'язку. Оскільки кіберфізичні загрози зростають, особливо в критичній інфраструктурі, існує нагальна потреба досліджувати надійні рішення безпеки фізичного рівня. Нами розглядаються передові механізми безпеки в комунікаціях з інтелектуальною мережею, зосереджуючись на методології квантової криптографії та протоколах цілісності сигналу для підвищення стійкості зв'язку в електромережі.

Розвиваючись, інтелектуальні мережі вимагають двостороннього зв'язку та збору даних у режимі реального часу між різними елементами мережі, що значно збільшує вразливість кіберфізичних загроз. Традиційні криптографічні методи, незважаючи на ефективність на вищих рівнях моделі OSI, стикаються з проблемами на фізичному рівні через посилення атак, спрямованих на перешкоди, маніпуляції сигналами та несанкціонований доступ. Щоб зменшити ці ризики, квантова криптографія постає як потенційне рішення, забезпечуючи теоретично незламне шифрування за рахунок використання квантово-механічних властивостей.

Квантова криптографія в основному працює на квантовому розподілі ключів (QKD), методі, який використовує квантові біти (кубіти) для безпечного обміну ключами по каналу зв'язку. Основний принцип QKD, зокрема таких протоколів, як BB84 і E91, полягає в тому, що будь-яка спроба прослуховування квантового каналу вносить вимірні збурення, попереджаючи як відправника, так і одержувача про потенційне порушення.

У додатках розумної мережі QKD передбачається для захисту зв'язку між центрами управління, підстанціями та розподіленими енергетичними ресурсами (DER). Впровадження протоколів QKD у цих каналах може забезпечити надійне шифрування навіть у разі зловмисних спроб. наприклад: 1) Протокол BB84 – цей базовий протокол QKD використовує стани поляризації фотонів для встановлення спільного ключа між двома сторонами. Завдяки принципу невизначеності Гейзенберга будь-яка спроба прослуховування змінює квантовий стан, таким чином попереджаючи законних користувачів про потенційні порушення безпеки; 2) Протокол E91 – заснований на квантовій заплутаності, протокол E91 передає заплутані частинки між вузлами сітки. Перевага безпеки полягає в миттєвій кореляції заплутаних частинок; будь-яке втручання або спостереження порушує

заплутаність, знову сигналізуючи про порушення. Незважаючи на надійність QKD, практичне розгортання в електромережах стикається з кількома проблемами.

По-перше, QKD вимагає вузькоспеціалізованого обладнання, яке часто працює лише через оптичні волокна. Враховуючи велике фізичне покриття електромереж, розгортання інфраструктури QKD є непомірно дорогим і складним. Крім того, такі чинники навколишнього середовища, як ослаблення сигналу, тепловий шум і масштабованість мережі, створюють значні технічні перешкоди. Дослідження квантової комунікації у вільному просторі та гібридних класично-квантових криптографічних систем можуть містити ключ до вирішення цих проблем у додатках розумної мережі.

Цілісність сигналу є життєво важливою для надійності та точності передачі даних у розумних мережах, оскільки погіршена якість сигналу може призвести до введення помилкових даних, помилок керування та навіть відключень. Два ключових підходи до посилення цілісності сигналу включають адаптивну обробку сигналу та технології розширеного спектру.

Враховуючи природне шумне середовище електромереж через електричні перешкоди, була розроблена адаптивна обробка сигналу для динамічного фільтрування шумів і перешкод. Такі методи, як адаптивна фільтрація за методом найменшого середнього квадрата (LMS), фільтрація Калмана та вейвлет-перетворення, зазвичай використовуються для підтримки точності сигналу в реальному часі.

Наприклад: 1) Фільтр Калмана [LQE] – оптимальний рекурсивний фільтр, який оцінює стан лінійної динамічної системи на основі серії шумових вимірювань. У зв'язку з інтелектуальною мережею фільтр Калмана може бути застосований для прогнозування та пом'якшення шумових перешкод від змінних навантажень мережі; 2) Вейвлет-перетворення – розкладаючи сигнал на різні діапазони частот, вейвлет-перетворення дозволяють покращити виявлення аномалій, особливо корисно в каналах зв'язку по лінії електропередач (PLC), де шум може порушити зв'язок.

Технології розширеного спектра прямої послідовності (DSSS) і розширеного спектра зі стрибками частоти (FHSS) є ефективними методами протидії атакам з перешкодами. Завдяки поширенню сигналу в широкому діапазоні частот або швидкому перемиканню частот під час передачі, методи розширення спектру ускладнюють зловмисникам визначення місцезнаходження та глушіння сигналу.

DSSS збільшує смугу пропускання переданого сигналу, поширюючи його в більшій смузі частот. Якщо супротивник намагається створити перешкоди, йому знадобиться значно більше потужності, що зменшує ймовірність успішної атаки з перешкодами. FHSS постійно змінює частоту передачі, зменшуючи передбачуваність сигналу. Інтелектуальні мережі з FHSS дуже стійкі до цілеспрямованого глушіння частоти, оскільки зловмисники не можуть легко стежити за стрибками частоти.

Для досягнення цілісної безпеки квантову криптографію можна інтегрувати з протоколами цілісності сигналу. Цей багаторівневий підхід гарантує, що навіть якщо цілісність фізичного рівня порушено, квантове шифрування захищає конфіденційність і цілісність даних. Фізичний рівень може використовувати надлишкові канали та багатошляхове рознесення, щоб підтримувати з'єднання, незважаючи на перешкоди або перешкоди, тоді як QKD захищає передані дані [1]. Крім того, виявлення міжшарових аномалій може забезпечити раннє попередження про атаки.

Оскільки інтелектуальні мережі продовжують відігравати ключову роль у сучасних енергетичних інфраструктурах, безпека їхніх фізичних рівнів зв'язку стає першорядною. Хоча квантова криптографія все ще розвивається, вона багатообіцяюча у створенні недоторканних каналів зв'язку, але її розгортання вимагає подолання значних фізичних та економічних перешкод. У тандемі передові засоби забезпечення цілісності сигналу та захисту від перешкод можуть забезпечити стійкість на фізичному рівні. Рівнева структура безпеки, що включає квантову, адаптивну обробку сигналів і методи розширеного спектру, здається, є найбільш життєздатним підходом до вирішення складних проблем безпеки в інтелектуальних мережах комунікацій [2].

В епоху цифрової трансформації еволюція енергомережі в напрямку взаємозв'язку та інтелекту має супроводжуватися настільки ж прогресивним підходом до безпеки. Квантова криптографія та методи покращеної цілісності сигналу необхідні для протидії багатогранним кіберфізичним загрозам, властивим сучасним енергетичним системам. Разом вони являють собою надійну багаторівневу систему безпеки, яка не тільки захищає канали зв'язку, але й забезпечує довгострокову стійкість і стабільність енергопостачання. Оскільки енергетичні системи продовжують розвиватися в напрямку посилення децентралізації та інтеграції відновлюваних джерел, впровадження цих стратегій безпеки стане основою для забезпечення стійкого, безпечного та надійного енергетичного майбутнього, здатного протистояти як очікуваним, так і виникаючим кіберфізичним викликам.

1. Islam, S. N., Baig, Z., & Zeadally, S. (2019). Physical Layer Security for the Smart Grid: Vulnerabilities, Threats, and Countermeasures. IEEE Transactions on Industrial Informatics, 15(12), 6522–6530. https://doi.org/10.1109/tii.2019.2931436.
2. Alshowkan, M., Evans, P. G., Starke, M., Earl, D., & Peters, N. A. (2022). Authentication of smart grid communications using quantum key distribution. *Scientific Reports, 12*(1). https://doi.org/10.1038/s41598-022-16090-w.

О.А. Владимирський, І.А. Владимирський

АКУСТИЧНЕ ЗОНДУВАННЯ ТРУБОПРОВОДІВ ПРИ ПОШУКУ ВИТОКІВ КОРЕЛЯЦІЙНИМИ ТЕЧЕШУКАЧАМИ

При пошуку витоків у підземних трубопроводах широко застосовуються кореляційні течешукачі (КТ), у яких визначення координати витоку відбувається за формулою

$$L_x = \frac{L}{2} + \frac{V_Г \cdot dT}{2} \qquad (1)$$

де : L_x - відстань від одного з датчиків до витоку, L - довжина трубопроводу між датчиками; $V_Г$ - швидкість поширення по трубопроводу від витоку до датчиків акустичних хвиль, зокрема хвиль гідравлічного удару; dT - затримка за часом між приходом акустичних хвиль до одного і до другого датчиків, визначувана за максимумом взаємної кореляційної функції :

$$R(dT) = \max_T (R(T)) \qquad (2)$$

де $R(T)$ - оцінка взаємної кореляційної функції (ВКФ) сигналів $x(t)$ та $y(t)$ з датчиків.

З формули (1) випливає, що точність визначення координати L_x витоку залежить від точності завдань L, $V_Г$ І dT. значення dT завжди обчислюється у КТ. Значення $V_Г$ і L звичайно не обчислюються у КТ. Значення L вимірюється за допомогою інших пристроїв та вводиться оператором у КТ вручну. для точного визначення довжини L ділянки трубопроводу звичайно використовують індукційні трасошукачі для з'ясування спочатку фактичного положення підземного трубопроводу, після чого, по розміченій над трубопроводом траєкторії його прокладання, прокатують мірне колесо – курвіметр та в такий спосіб вимірюють L. іноді використовують виконавчу чи проектну документацію на трубопровід, але вона буває не точною. спосіб визначення L за допомогою трасошукача та курвіметра зазвичай працює чітко і проблем з цим не виникає. однак з точністю завдання $V_Г$ проблеми є. зазвичай використовується табличне, осереднене, теоретичне значення, яке запрограмовано у КТ та обирається оператором в залежності від матеріалу трубопроводу, його діаметру та типу транспортованої рідини. для металевих трубопроводів тепло- та водопостачання це сталеві та чавунні труби з діаметром в діапазоні 50-1020 мм. З водою. іноді оператором ще обирається близьке до фактичного значення температури води. по цих параметрах у КТ за таблицею швидкостей автоматично визначається $V_Г$. Однак, $V_Г$ різною мірою залежить від набагато більшої кількості факторів. Так, відповідно до [1],

розрахунки $V_Г$ за відомими формулами кортвега показали значну залежність $V_Г$ від фактичної товщини стінки трубопроводу. показано, що внаслідок корозійного стоншення стінок, фактичне значення $V_Г$ може відрізнятися від закладеного у КТ на величину до 30%. другим суттєвим чинником, який впливає на фактичне значення $V_Г$, є його частотна залежність внаслідок дисперсії акустичних хвиль від витоку, яка виникає при поширенні цих хвиль по трубопроводу до датчиків. інші фактори є менш суттєвими. оскільки теоретично, з задовільною точністю, передбачити їх вплив не можливо, розробники КТ шукають шляхи оперативного уточнення фактичного значення $V_Г$ при пошуку витоку.

У сучасних КТ передбачено два способи експериментального визначення $V_Г$.

Перший спосіб полягає у створенні штучного джерела шуму з відомою координатою та вирішенні зворотної задачі, тобто в обчисленні не координати джерела за відомою швидкістю як в (1), а навпаки, в обчисленні швидкості за відомою координатою джерела шуму. Це дуже продуктивна та проста ідея. Питання виникають при її реалізації. Бо в інструкціях з експлуатації сучасних приладів, таких як Eureka 5, AquaScan 610 та ін., у якості штучного джерела пропонують створювати штучний витік за допомогою відкриття технологічних вентилів чи клапанів. У якості типового рішення пропонується тимчасове відкриття пожежного гідранта. Для західних умов це є реальним та практичним. Але для наших зношених мереж з пошкодженими засувками, непрацюючими спускними клапанами це не так. Спектр акустичного шуму витоку залежить від величини отвору. Тому потрібно не тільки мати можливість створити штучний витік та потім його надійно відключити, а ще й відрегулювати для того, щоб він створював зондувальні шуми саме на тих частотах, на яких реєструється виток. Бо інакше не уникнути дисперсійної розбіжності між груповими швидкостями зондувальних хвиль та хвиль від витоку. Цей спосіб у наших умовах не практикується.

Другий спосіб полягає в тому, що у якості джерела шуму використовується той же шуканий виток, але крім звичайно обчисленої ВКФ шуму між двома ближчими до витоку датчиками обчислюється ще, хоча б одна ВКФ для перенесеного одного з датчиків у сусіднє МД – теплову камеру чи колодязь. тобто до рівняння (1) додається друге, аналогічне за видом рівняння, але з іншими двома значеннями L і dT, це відповідно значення L_2 і dT_2. Тоді рішення системи цих двох рівнянь дають вираз для швидкості:

$$V_Г = \frac{L_2 - L}{dT - dT_2} \qquad (3)$$

Підставляючи (3) у (1) замість $V_Г$ отримаємо відомий з теорії КТ три точковий метод визначення координати витоку за двома ВКФ без явного завдання швидкості $V_Г$. подібне обчислення швидкості та координати за кількома ВКФ реалізовано у течешукачі TriKorr. У Local200 Pc навіть реалізований фізично трьох точковий метод, тобто цей прилад може комплектуватися третім вимірювальним радіо блоком з датчиком. Іншим варіантом другого способу є встановлення обох датчиків КТ так, щоб виток опинився не між ними, а збоку, тобто на сусідній ділянці по відношенню з охопленою датчиками ділянкою. так рекомендують робити розробники AquaScan 610. Тоді швидкість обчислюється за допомогою однієї ВКФ за простою формулою:

$$V_Г = \frac{L}{dT} \qquad (4)$$

де L - довжина трубопроводу між датчиками. У КТ TriKorr реалізовано калькулятор швидкості, якщо джерело розташовано між датчиками та відома його координата та якщо джерело шуму знаходиться за межами ділянки між датчиками.

З практики виробничого пошуку витоків відомо, що іноді зазначений, другий спосіб, тобто використання шуканого витоку як джерела зондуючого сигналу для обчислення $V_Г$, працює та буває корисним. однак його не вдається застосовувати регулярно з наступних причин. по - перше, метод припускає, що значення $V_Г$ на ділянці з витоком та значення $V_Г$ на сусідній ділянці однакові чи дуже близькі, що в умовах значного корозійного зносу труб та різної кількості проведених точкових ремонтів оцінити складно. Тому невідомо, яке значення $V_Г$ дасть більш точну координату витоку L_x в (1), чи теоретичне значення $V_Г$ закладене у приладі, чи експериментальне, отримане за виразами (3) чи (4). По-друге, при збільшенні відстані від датчиків до витоку, обчислена ВКФ розмивається за часом, частково внаслідок загасань сигналів, частково внаслідок зростання розбігу за часом хвиль з різними груповими швидкостями. кореляційний сплеск, за яким у (2) визначається dT, стає менш чітким, зменшується відношення сигнал-завада. саме тому при пошуку витоків за допомогою кореляційних течешукачів для його датчиків рекомендують обирати ближчі до витоку наявні місця доступу до трубопроводу. особливо невизначеність проявляється при малому тиску у трубах, при малому витоку, на трубах з великим загасанням сигналів, наприклад з ізоляцією з бітумоперліту, на трубопроводах великих діаметрів. таким чином, намагаючись уникнути джерела однієї похибки визначення L_x ми посилюємо вплив на це визначення джерел інших похибок. Слід зазначити, що намір уточнити швидкість як раз і виникає, більш за все, при малому відношенні сигнал-завада, коли навіть у ближчих до витоку мд обчислена ВКФ має сумнівний вигляд внаслідок слабкості реєстрованого шуму витоку. Зрозуміло, що віддаляючи датчик від витоку ми погіршуємо його визначеність у ВКФ.

Враховуючи зазначені недоліки існуючих способів визначення фактичного значення швидкості $V_Г$ для (1), авторами розроблено інший спосіб. Він подібний першому способу, але у якості джерела використовується не штучний виток, а спеціальний акустичний випромінювач сигналів у стінку трубопроводу, який підключається до генератора керованого зондувального сигналу та підсилювача [2]. Створено експериментальну систему з випромінювачами потужністю 50 Вт та 100 Вт. ЦІ випромінювачі кріпляться до металевої стінки трубопроводу за допомогою супермагнітів. не зважаючи на те, що на відміну від витоку, випромінювання йде крізь стінку трубопроводу, експериментально перевірено, що створювані акустичні хвилі за частотним діапазоном та груповою швидкістю є аналогічними витребуваним акустичним хвилям гідравлічного удару $V_Г$. Це означає, що даний спосіб дозволяє без регулювання зношеної запірної арматури проводити акустичне зондування та визначати фактичне $V_Г$ саме на пошкодженій витоком ділянці і саме в тому частотному діапазоні, в якому КТ реєструє виток. Для того, щоб при зондуванні знизити вплив шуму витоку на визначене кореляційним методом значення $V_Г$, при обчисленні відповідної зондувальної ВКФ у якості одного з двох сигналів береться електричний сигнал не з датчика на трубопроводі, а зі входу випромінювача, бо у цьому сигналі немає ані шуму витоку, ані завадових акустичних відбиттів. Цього не можна досягти при використанні штучного витоку, у тому числі у вигляді відкритого гідранту. при визначенні швидкості $V_Г$, як і при пошуку витоків, використовується розроблений авторами кореляційний параметричний метод [3]. Це значно спрощує, формалізує та підвищує точність визначення швидкості $V_Г$ та координати витоку L_x. Генератор розроблявся в першу чергу для корозійного акустичного моніторингу трубопроводів як складова системи РАСТР [4] розробки ІПМЄ ім. Г.Є. ПУХОВА НАН України. Тому для використання при пошуку витоків потрібно розробити відповідну методику його застосування. Також слід інтегрувати відповідний режим у виробниче програмне забезпечення з пошуку витоків та відпрацювати його практичне застосування у польових умовах. Цю роботу проводиться при виконанні проекту 2023.04/0022 «Розроблення апаратно-програмного комплексу та методики оперативного виявлення пошкоджень систем тепло- та водопостачання з врахуванням їх зношеності та мілітарних впливів» за рахунок грантової підтримки Національного фонду досліджень України.

Слід зазначити, що виробниче застосування запропонованого акустичного випромінювача дозволить зручно та оперативно контролювати ще один важливий для пошуку витоків фактор. це повнота заповнення водою пошкодженої ділянки трубопроводу. бо тільки при повному заповненні трубопроводу можливе застосування будь-якого КТ. Питання заповнення завжди виникає у теплових мережах при пошуку місць витоків на відключених

перед цим пошкоджених відгалуженнях від магістралей. Для застосування КТ на таких ділянках потрібно не тільки створити достатній тиск водою, а ще й видалити з відгалуження повітряні міхури, які можуть утворюватись між витоком та кінцем порожнього трубопроводу при його заповненні. Для цього потрібно відкрити відповідну засувку чи клапан, що в умовах зносу чи можливого заливання споживача є небажаним. Застосування запропонованого акустичного випромінювача дозволяє безпечно з'ясувати, потрібно це робити чи ні. Для цього достатньо проконтролювати час та ступінь проходження по відгалуженню штучно створених акустичних хвиль від випромінювача. Сучасні течешукачі такої функції не мають.

1. Семенюк Д.Н. Особенности поиска утечек в подземных трубопроводах теплових сетей. *Сантехніка, опалення, кондиціонування (С.О.К)* 2006, №6, с.10-12.
2. О.А. Владимирський, І.А. Владимирський. Розробка генератора для акустичного зондування трубопроводів. *XLI науково-технічна конференція молодих вчених та спеціалістів інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України.* Збірник матеріалів конференції. Київ. 17 травня 2023р.- С. 120-121.
3. Владимирський О.А., Владимирський І.А. Кореляційні параметричні методи визначення координат витоків підземних трубопроводів// *Електрон. моделювання,* 2021, 43**,** № 3, с. 3—17.
4. Владимирський О. А., Владимирський І. А., Криворучко І. П., Савчук М.П. Розробка модернізованої системи низькочастотного діагностування стану трубопроводів РАСТР-1М. *Моделювання та інформаційні технології. З*бірник наукових праць ІПМЕ ім. Г. Є. Пухова НАН України. 2017. Вип. 78. С. 40-45.

Н.В. Заїка, В.С. Ракович, М.Ю. Комаров, А.С. Боднар

ПІДВИЩЕННЯ КІБЕРБЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: РОЛЬ АУДИТУ ТА РЕКОМЕНДАЦІЇ ДЛЯ КІБЕРФІЗИЧНИХ СИСТЕМ

Підвищення кібербезпеки критичної інфраструктури – це нагальна потреба для збереження стабільності держави, захисту від зовнішніх та внутрішніх кіберзагроз, а також забезпечення сталого функціонування кіберфізичних систем (CPS). Такі системи використовуються в енергетиці, водопостачанні, охороні здоров'я та інших галузях, де безперервність роботи є життєво важливою. Прикладом CPS у сфері енергетики є інтелектуальні електромережі або Smart Grid, системи, які інтегрують традиційні енергетичні мережі з цифровими технологіями для автоматизованого моніторингу та управління постачанням електроенергії. Кіберфізичні системи інтегрують фізичні об'єкти з цифровими компонентами, тому їх безпека залежить від ефективного поєднання технічних та управлінських рішень, до яких відноситься й аналіз загроз інформаційній безпеці.

Аналітика загроз (Threat Intelligence) охоплює процеси збору, аналізу і прогнозування потенційних кібератак. Використання багаторівневого захисту включає системи моніторингу, автоматизовані засоби реагування на інциденти, виявлення аномалій, що забезпечує інформаційне підґрунтя для оцінки стану об'єкта аудиту. Завдяки використанню даних з відкритих та закритих джерел, платформ для аналізу загроз (Threat Intelligence Platforms) та інтеграції з іншими інструментами кібербезпеки - можливо завчасно впроваджувати заходи для нейтралізації атак і загроз.

Цифрова криміналістика у CPS охоплює комплекс процесів із вилучення, збереження, аналізу та інтерпретації даних для відтворення подій, що сталися в системі, і визначення джерел потенційних або вже здійснених атак. Цей процес включає ретельний аналіз різних типів даних, зокрема системних логів, журналів подій, файлів мережевої активності та специфічних налаштувань CPS, що дозволяє виявити аномальні проблеми, сліди шкідливого коду чи сліди зловмисників [1].

Дані, отримані під час цифрової криміналістики, стають основою для проведення аудиту кібербезпеки, оскільки вони дозволяють відновити обставини інциденту та оцінити потенційні уразливості в системі. Однією з ключових вимог є забезпечення належного юридичного збереження цифрових доказів, дотримуючись коректного їх документування і захисту від модифікації, щоб вони могли бути використані у судових процесах або подальших розслідуваннях.

Регулярний аудит дає змогу оцінити захищеність CPS і виявити слабкі місця, які можуть бути вразливими до атак, шляхом періодичного аналізу журналів доступу, сканування вразливостей, перевірку відповідності стандартам кібербезпеки, наприклад, ISO/IEC 27001 для виявлення та відслідковування нових видів атак, а також стандартів NIST для забезпечення кращого захисту інформації та об'єктів критичної інфраструктури [2].

Аудит кібербезпеки в кіберфізичних системах (CPS), які інтегровані в критичну інфраструктуру, є невід'ємною складовою захисту від кіберзагроз [3]. Зростання взаємозв'язку між фізичними й цифровими компонентами в критичній інфраструктурі (енергетика, транспорт, водопостачання тощо) підвищує ризик кіберзагроз, тому регулярний аудит має вирішальне значення для виявлення вразливостей, перевірки на відповідність нормативним вимогам, оцінювання ефективності наявних заходів безпеки та підготовлених превентивних заходів.

Аудит дозволяє виявляти слабкі місця у системі, які можуть стати ціллю для кібератак. Це включає вразливості у програмному забезпеченні, недостатньо захищені мережі, неправильне налаштування апаратного обладнання, захищеність системи та наскільки ефективні існуючі заходи кібербезпеки [4]. Це дає можливість вдосконалювати політику захисту та адаптуватися до нових загроз. Критична інфраструктура повинна відповідати міжнародним і національним стандартам, таким як ISO/IEC 27001 або NIST. Аудит допомагає забезпечити відповідність цим стандартам, запобігаючи юридичним і фінансовим наслідкам у разі порушень.

Рекомендації для проведення аудиту кібербезпеки в CPS.

Багатоетапний підхід дозволяє охопити всі аспекти системи і уникнути прогалин у безпеці. Застосування багатоетапного підходу включає поетапний аналіз різних компонентів CPS — апаратного, програмного забезпечення, мережевого рівня та захисту даних.

Проведення тестів на проникнення (penetration testing) допомагає оцінити реальну захищеність системи, моделюючи можливі атаки та визначаючи, як CPS реагує на різні загрози. Постійний аналіз журналів та моніторинг аномалій у трафіку або поведінці користувачів дозволяє швидко виявляти можливі інциденти та реагувати на них [5].

Результати аудиту кібербезпеки зазвичай документуються у вигляді звіту про аудит, який визначає ті фактори ризику безпеки, що були виявлені під час аудиту, і може бути використаний для надання додаткових рекомендацій [6].

Підвищення рівня знань працівників про кібербезпеку і навчання їх реагувати на загрози є важливим елементом захисту CPS. Це включає тренінги, симуляції інцидентів і регулярні оцінки знань співробітників, поновлення актуальної інформації про нові типи атак і шкідливе програмне забезпечення. Це включає процедури безпеки, нові стандарти, і технічні вимоги для пристроїв CPS. План реагування на інциденти повинен включати чіткі інструкції для персоналу щодо заходів у разі виявлення загрози. Це дозволить уникнути хаосу під час інцидентів та мінімізувати шкоду.

Ефективний аудит кібербезпеки — це не лише виявлення і виправлення вразливостей, але й створення комплексної системи захисту, яка може адаптуватися до нових викликів та забезпечувати безперервність роботи критичної інфраструктури навіть у разі виникнення загроз.

Висновки

Аудит кібербезпеки є важливим інструментом для забезпечення захисту кіберфізичних систем критичної інфраструктури. Він дозволяє виявити потенційні вразливості, оцінити ефективність існуючих захисних заходів і вчасно впровадити необхідні вдосконалення, забезпечити своєчасну відповідність системи вимогам міжнародних стандартів кібербезпеки. На основі результатів аудиту організації можуть розробити і впровадити рекомендації для підвищення кібербезпеки, оптимізувати захисні заходи та вдосконалити процеси моніторингу і реагування на інциденти. Регулярний аудит знижує ризик виникнення інцидентів і допомагає уникнути суттєвих фінансових та репутаційних втрат, зумовлених кібератаками або збоями в роботі системи безпеки. Це підвищує стійкість об'єктів критичної інфраструктури до загроз і зменшує потенційні ризики.

1. Бойко Ю.О., Основи кібербезпеки: Захист критичної інфраструктури. Київ, 2023.
2. Riskmanagement guide for information technology systems. Recommendations of the National Institute of Standards and Technology: NIST 800-30. –Введ. 06.01.2002.– США. – 2002. – 56 с.
3. Закон України " Про основні засади забезпечення кібербезпеки України". Відомості Верховної Ради України, 2017, № 45, ст.403.
4. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова Каб. Міністрів України від 19.06.2019 р. № 518 URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text.
5. Пашорін В.І., Куклінський Д.В., Шабалін Д.С. Організація захисту інформації. Кібергігієна. Кібербезпека. Безпека держави : матеріали наукових семінарів (Київ, 27 листопада 2020 р.), Київ. нац. торг.-екон. ун-т, 2020. – 101 с.
6. Шість переваг аудиту кібербезпеки URL: https://www.isaca.org/resources/news-and-trends/industry-news/2024/six-benefits-of-a-cybersecurity-audit.

Н.Ю. Павлюк, О.Є. Маляренко, О.І. Тесленко, Г.О. Куц

ЗАМІЩЕННЯ ПРИРОДНОГО ГАЗУ ЗАЛИШКОВИМИ ПОБУТОВИМИ ВІДХОДАМИ ДЛЯ ПІДПРИЄМСТВ ТЕПЛОВОЇ ГЕНЕРАЦІЇ

Одними з головних споживачів природного газу в Україні є підприємства Теплокомуненерго (ТКЕ), які виробляють теплову енергію і надають послуги з централізованого опалення та гарячого водопостачання населенню, бюджетним організаціям і комунальним підприємствам (276 млн ТДж). Котли підприємств ТКЕ споживають біля 20% від загального споживання природного газу країни. Україна має розвинуту мережу централізованого теплопостачання, понад 1000 теплопостачальних підприємств - ліцензіатів, а централізованим теплопостачанням охоплено 40% населення. Більшість багатоквартирних будинків і деякі приватні будинки в містах і селищах підключені до мереж централізованого теплопостачання загальною протяжністю близько 21 000 км в двохтрубному обчисленні. Система централізованого комунального теплопостачання міст дозволяє замінити викопні види палива відновлювальними або альтернативними джерелами енергії [1].

За даними Міністерства розвитку громад, територій та інфраструктури України, в 2023 році в країні збиралось понад 9 млн т побутових відходів [2]. Використання енергетичного потенціалу залишкових твердих побутових відходів (ТПВ), переробка яких неможлива, є найбільш доступним в умовах України міським альтернативним джерелом енергії, наприклад, штучним паливом з ТПВ, що розташоване біля виробників теплової енергії – підприємств ТКЕ. Теплова енергія залишкових ТПВ може стати суттєвим доповненням до інших джерел заміщення природного газу (біопалива, біогазу, що вилучається зі сміттєзвалищ, тощо).

Кабінетом Міністрів України та Міндовкілля розробляється Концепція Державної цільової економічної програми будівництва 207 нових сміттєпереробних заводів та 10 ТЕЦ на RDF ((Refuse Derived Fuel, паливо з відходів після сортування) для заміщення споживання природного газу на підприємствах - виробниках теплової енергії. Це дозволить замістити біля 10% природного газу, що використовується для потреб опалення та гарячого водопостачання населення міст України з населенням понад 300 тис. мешканців.

Зокрема, в місті Києві утворюється близько 1 млн тон ТПВ на рік, що містить близько 40% висококалорійної фракції (SRF/RDF), придатної для виробництва енергії [3]. До 25% ТПВ термічно перероблялось на сміттєспалювальному заводі «Енергія» КП «Київтеплоенерго» (у 2023 р. – 11%), який працює в режимі «Котельня на ТПВ» для опалювання та гарячого водопостачання мешканців міста. Біля 5% ТПВ потрапляє на сміттєпереробні

підприємства, а біля 3% на заготівельні пункти вторинної сировини. Решта ТПВ вивозиться на полігони. Дослідження морфології змішаних ТПВ Києва, показали, що біля 30% цих ТПВ містять значний енергетичний потенціал. Його використання для потреб теплопостачання населення сприяє те, що мережа централізованого теплопостачання Києва досить розвинута та має протяжність 2780 км в двохтрубному вимірі [4].

НАК «Нафтогаз України» запланувала збудувати 9 біо-ТЕЦ та біокотелень у 8 регіонах України загальною потужністю 250 МВт теплової енергії та 52 МВт електричної, щоб відмовитись від використання природного газу до 2027 року. Перший об'єкт мав з'явитись у Львові у лютому 2023 р. (ТЕЦ на альтернативному паливі потужністю 40 МВт для забезпечення потреби у тепловій енергії чверті населення Львова) [5].

На виконання розпорядження Кабінету Міністрів України від 08.11.2017 р. № 820 "Про схвалення Національної стратегії управління відходами в Україні до 2030 року", в цілях економії викопного палива і утилізації твердих побутових відходів та виробленого з них палива для забезпечення енергетичної безпеки мешканців міста Житомир під час блекаутів та стабільного функціонування підприємства було розроблено попереднє техніко-економічне обґрунтування (ТЕО) проєкту нового будівництва під ключ ТЕЦ на альтернативних видах палива електричною потужністю 9,9 - 13,1 МВт та тепловою потужністю до 22 МВт [6]. На даний час у Житомирі побудовано сміттєпереробний завод, який має виробляти RDF з місцевого сміття. Планується запустити біо-ТЕЦ, яку проєктували на спалювання тріски, з використанням наполовину RDF власного виробництва. Інвестори переробили проєкт біо-ТЕЦ, згідно з яким 20 МВт теплової потужності планується використовувати на тріску і 20 МВт – на RDF. Крім того, її проєктна потужність передбачає 10 МВт потужності для виробництва електроенергії. Передбачається, що обсяги RDF сировини, яку можна буде виробляти зі сміття, що продукується містом, і використовувати для виробництва тепла, дозволять замістити у місті на потреби теплозабезпечення 20 млн куб. м природного газу на рік [7].

В Інституті загальної енергетики НАН України за творчою співпрацею з Інститутом технічної теплофізики НАН України виконувались оцінки економічної доцільності заміщення природного газу та іншого органічного палива ТПВ для виробництва теплової енергії за показником середньо зваженої собівартості теплової енергії за життєвий цикл. Обчислення проводились для сміттєспалювального заводу «Енергія» КП «Київтеплоенерго». Цей розрахунковий показник є високим, але з урахуванням екологічного та соціального факторів він стає прийнятним. Враховуючи досвід використання ТПВ на сміттєспалювальних заводах Європи, впровадження цього виду палива у системи паливозабезпечення систем централізованого теплопостачання міст України буде сприяти зміцненню енергетичної безпеки держави [8].

1. Сігал О.І., Павлюк Н.Ю. Використання залишкових твердих побутових відходів як альтернативного палива в системах централізованого теплопостачання. Теплова енергетика: шляхи реновації та розвитку. Збірка наукових праць XVIII Міжнародної науково-практичної конференції. Київ. 2022. С. 159-163. ISBN 978-617-7852-33-8. DOI 10.48126/conf2022.
2. Міністерство розвитку громад та територій України. Звітність 1-ТПВ розділ 1 за 2023 рік. https://mtu.gov.ua/.
3. Офіційний портал Києва. У Києві щороку утворюється близько мільйона тонн відходів, що містять до 40% калорійної фракції, придатної для виробництва енергії на ТЕЦ – Петро Пантелеєв. 29.06.2024. https://kyivcity.gov.ua/news/u_kiyevi_schoroku_utvoryuyetsya_blizko_milyona_tonn_vidkhodiv_scho_mistyat_do_40_kaloriyno_fraktsi_pridatno_dlya_virobnitstva_energi_na_tets__petro_panteleyev/.
4. Сігал О.І., Крикун С. , Павлюк Н.Ю., Сатін І.В., Плашихін С.В., Кіржнер Д.А., Семенюк М.В., Каменьков Г.Б. Дослідження кількості теплоти, що виділяється при спалюванні змішаних твердих побутових відходів м. Києва. Промислова теплотехніка. 2017. Т.39. №3. С.65-71.
5. У Львові та Житомирі зведуть ТЕЦ на альтернативному паливі. Pragmatika. 03.10. 2022. https://pragmatika.media/news/vidrazu-u-kilkoh-ukrainskih-mistah-zvedut-na-alternativnomu-palivi/.
6. Нове будівництво «під ключ» ТЕЦ, що працює на твердому відновлюваному паливі (SRF) з домішкою деревної тріски, електричною потужністю від 9,9 до 13,1 МВт з виробленням тепла від 0 до 22 МВт, за адресою: м. Житомир. DREAM проєкти. https://dream.gov.ua/ua/project/DREAM-UA-200324-57B79005/profile.
7. У Житомирі хочуть запустити біо-ТЕЦ на RDF з місцевого сміттєпереробного заводу – заступника мера. Енергореформа. 10.07.2023. https://reform.energy/news/u-zhitomiri-khochut-zapustiti-bio-tets-na-rdf-z-mistsevogo-smittepererobnogo-zavodu-zastupnika-mera-21668.
8. Kuts H.O., Maliarenko O.Ye., Pavliuk N.Yu. Estimation of the weighted average cost of thermal energy for the life cycle from a waste incineration plant under different technological schemes of production. International scientific conference «Features of innovative development in the field of technology: the comparative experience of Ukraine and the European Union»: conference proceedings (September 6–7, 2023. Wloclawek, the Republic of Poland). Riga, Latvia: “Baltija Publishing”, 2023. 72 pages. Pp. 36-39. http://baltijapublishing.lv/omp/index.php/bp/catalog/book/359.

О.І. Сігал, Н.Ю. Павлюк

БЕЗПЕКОВІ ПРІОРИТЕТИ РОЗВИТКУ ЕНЕРГОКОМПЛЕКСІВ МІСТ УКРАЇНИ (РОЗПОДІЛЕНА ГЕНЕРАЦІЯ ЯК ТЕХНІЧНИЙ, ЕКОЛОГІЧНИЙ ТА ЕКОНОМІЧНИЙ ВИКЛИК ЦЕНТРАЛІЗОВАНОМУ ТЕПЛОПОСТАЧАННЮ)

Під час повномасштабної війни в Україні пошкоджено/втрачено 24 об'єкти генерації. На сьогодні залишаються пошкодженими енергоблоки ТЕС потужністю 3,8 ГВт, 1 ГВт великих ТЕЦ, втрачено 540 МВт ГЕС та 650 МВт ГАЕС, всього близько 6 ГВт. На окупованій території залишилось 51 % потужності ТЕЦ, це біля 1,5 ГВт, 74 % ТЕС – біля 7 ГВт, та 43% АЕС – 6 ГВт. Всього для регулювання енергетики Україні необхідно замістити біля 6 ГВт зруйнованих потужностей та до 8,5 ГВт окупованих, тобто 14,5 ГВт, мін – 9 ГВт. Нагальна потреба, з урахуванням окупованих територій та мобілізації резервів необхідний обсяг розподіленої генерації має бути на рівні близько 30%, тобто 5 ГВт [1].

Існує можливість імпорту 1,7 ГВт електричної енергії з 4 країн ЄС (Польщі, Румунії, Угорщини, Словаччини).

Зважаючи на те, що найбільш типовими газопоршневими установками (ГПУ) є машини з встановленою потужністю 300 кВт – 3,5 МВт, а в сегменті великих установок 4 – 16 МВт, осереднено нам потрібно встановити від 800 до 1200 машин.

Існує можливість встановлення ГПУ на більш, як 700 великих котельнях та станціях теплопостачання, 260 з яких мають гаряче водопостачання (ГВП).

В великих містах (Київ, Харків, Одеса, Львів) можливо встановити понад 100 потужних теплоджерел, при встановленні по 2 ГПУ на ТД, усереднено по 10 МВт – всього близько 2 ГВт. Всі обласні міста мають можливість поставити когенерацію у обсязі біля 20 ГПУ, усереднено до 5 МВт потужності, це до 400 ГПУ з загальною встановленою потужністю біля 2 ГВт. Загалом близько 4 ГВт. Можливості майже достатні для забезпечення нагальної потреби.

При виборі когенераційної машини на базі поршневого двигуна слід звернути увагу на наступне (не вичерпно) [2] (табл. 1):

Таблиця 1

№	Звернути увагу на	Параметр	Що зробити	Вплив на вартість
1	Вимоги до палива (газ)	Вміст вологи, вміст твердих частинок	Необхідність компримування газу	Чим менші вимоги, тим дорожча машина

Продовження таблиці 1

2	Система подання газу у камеру згорання	Тиск газу >4 кг чи власний турбонаддув	Необхідність встановлення турбокомпресора 0,2 кг	За відсутності необхідного тиску здорожчання машини
3	Ресурс до кап. ремонту та можливість виконати його без демонтажу та відправки машини на завод-виробник	Чи гільзований двигун, чи є виїзний сервіс	Необхідність демонтажу та відправки КГУ на завод - виробник	Врахувати різницю у кап. затратах на сервіс
4	Період заміни мастила та ін.	Співвідношення ціни масла та його доступності та періоду до заміни	Необхідність заміни та резервування мастила	Чим більше термін роботи мастила, тим воно дорожче
5	Число обертів валу	1500 об/хв	Якщо вище - термін до кап. ремонту менший	Чим менше, тим дорожча машина
6	Співвідношення між вироблено ю електроене ргією та теплотою	Зазвичай 50/50	Якщо є можливість використати тепло, тоді 40/60 чи 30/70	Можливість здешевити машину
7	Утилізація теплоти	Від відхідних газів; охолоджуваль ної води;	Наявність 4-х охолоджувальн их контурів та теплообмінників	Відсутність будь-якого з контурів охолодження

Кінець таблиці 1

		надувного повітря; мастила		здешевшує машину
8	Наявність технологічних рішень зі зниженням викидів у довкілля	NOx≤100 мг/м2	Використання відхідних газів у якості газів рециркуляції	Можливість виконати екологічні вимоги
9	Рівень шуму	У пакетованій машині не перевищує нормативу	Наявність шумопоглинального кожуху	Збільшує вартість
10	Струм та напруга	Можливість роботи з мережею	Потрібен додатковий трансформатор	Збільшує вартість

Необхідні капіталовкладення

1 МВт електричної когенераційної потужності, в залежності від обладнання і виробника коштує 700-900 тис. дол. США. Відповідно, 4 ГВт коштуватиме біля 3 млрд дол. США.

Термін окупності

Ідеалізоване припущення: Вартість електроенергії по 8 грн. ($ 0,2) за кВт-год, газ для виробництва безкоштовний, - прибуток складе $ 0,1 від кВт/год, тобто окупність - 8000 годин роботи.

Реалістичні умови: При ціні газу $ 0,2/м3, це 23% (1 м3 газу - дає близько 9 кВт-год) від $ 0,1 потрібно віддати за паливо, тоді окупність складе біля 10400 годин роботи, тобто близько 2,5 опалювальних сезонів.

При реальних цінах електроенергії 4,32 грн./кВт-год – це біля трьох опалювальних сезонів, а при можливій ціні газу $ 1/м3 строк окупності сягає 15 років при терміні безперебійної експлуатації до кап. ремонту 2,5 – 3 роки.

Споживання теплової енергії

- Доцільно використовувати обладнання впродовж всього року – бажана наявність гарячого водопостачання чи будь-яких інших користувачів влітку. Саме тому буде доцільно поновити ГВП хоча б у невеликих обсягах для деяких, найближчих до джерел, користувачів, як систему утилізації теплоти та охолодження води для ГПУ.

- Доцільно розглянути дисконтування вартості такої теплоти на ГВП для користувачів хоча б до 70% від вартості тієї ж гарячої води, що готується у квартирному бойлері. Фактично підприємства теплопостачання будуть покривати ще 30% з прибутку, отриманого від продажу електроенергії на балансуючому ринку, що все одно є доцільним.

В технічному плані така *розподілена електрогенерація* не є *когенерацією*, бо *когенерація* – це вироблення електрики на тепловому споживанні. Тобто ми виробляємо електрики стільки і коли можемо, відповідно до домінантної потреби в теплопостачанні. *Розподілена електрогенерація* – це вироблення електрики для потреб регулювання енергосистеми з виробленням теплоти за принципом скиду у систему теплопостачання, як у великий акумулятор теплоти.

Заходи з впровадження *розподіленої електрогенерації* спрямовані, перш за все, на сприяння забезпеченню енергетичної безпеки України, економічні показники відходять на другий план.

Екологічні наслідки

Газопоршневі машини *розподіленої генерації* можуть бути встановлені у першу чергу на потужних котельнях, значна частина яких увійшли до переліку Національного плану щодо скорочення викидів від великих спалювальних установок (НПСВ); тобто взяли на себе зобов'язання знизити викиди оксидів азоту до ≤100 мг/м3.

При виробництві електричної енергії обсяг спожитого природного газу зросте на 40-50%, однак «запасу» по дозволам на викиди (які розраховані на роботу на максимальній потужності) було б в основному достатньо, якщо б не значні концентрації NOx, що утворюються у двигуні внутрішнього згоряння (ДВЗ) під тиском (400 – 600 мг/м3).

З урахуванням цього, виконання Україною вимог за НПСВ, і так проблематичне, ще більш ускладнюється.

Крім того, вже після перших 200 год використання ДВЗ концентрації CO у вихідних газах часто збільшується до понаднормативних значень. Тож потрібно шукати ефективні екологічні рішення для забезпечення відповідності вимогам діючого екологічного законодавства, дозволів та НПСВ.

1. DiXi Group Проходження осінньо-зимових періодів 2022-2024 рр. Стан енергосистеми - ГО "ДІКСІ ГРУП", 2024 р.- 22 с. https://dixigroup.org/wp-content/uploads/2024/04/2024_winterseasons_analysis_dixi_group_final.pdf.
2. В.Н. Клименко, А.И. Мазур, А.И. Сигал. Когенерационные системы с тепловыми двигателями. Справочное пособие ч.2. Газотурбинные когенерационные технологии. - К.; ИПЦ Алкон НАНУ, 2011. - 792 с.

О.О. Марчук

МЕТОД ТА СИСТЕМА ТРАНСФОРМЕРА НА ПІДСТАВІ CHATGPT ДЛЯ ГЕНЕРАЦІЇ ТЕКСТОВИХ ЗАПИТІВ ЧАТ-БОТУ

Розглянуто прикладні аспекти розробки метод та система трансформера на підставі chat-GPT для генерації текстових запитів чат-боту, які базуються на попередніх відповідях та складаються максимально точно до людської мови у реальному часі. Запропонована система забезпечує точну і швидку генерацію тексту відповідно до складеного запиту користувача.

Applied aspects of developing a method and system of a transformer based on chat-GPT for the generation of text requests of a chatbot, which are based on previous answers and are composed as closely as possible to human speech in real time, are considered. The proposed system provides accurate and fast text generation according to the user's request.

Сучасні чат-боти набули популярності завдяки своїй здатності вести природні та зручні для користувачів розмови. Основою для цього є архітектура трансформерів, зокрема ChatGPT, яка дозволяє обробляти текстові запити в реальному часі з врахуванням попередніх відповідей та адаптацією під стиль людської мови. Такий підхід дозволяє створювати чат-боти, які можуть легко інтегруватися у різні сфери бізнесу, забезпечуючи покращення взаємодії з користувачами [1].

Метою роботи є розробка методології генерації текстових запитів на базі трансформерів ChatGPT, що дозволить чат-боту точно та швидко реагувати на запити користувачів, враховуючи попередні відповіді та особливості природної мови. Це включає оптимізацію генерації запитів і поліпшення механізму утримання контексту у тривалих діалогах.

ChatGPT, побудований на архітектурі трансформерів, використовує механізм самозвернення для обробки тексту, який дозволяє визначати значення кожного слова в контексті попередніх фраз. Архітектура передбачає багаторівневу обробку тексту з використанням self-attention, що дозволяє моделі запам'ятовувати деталі діалогу та забезпечувати більш релевантні відповіді. Такий підхід дозволяє покращити точність і природність генерації тексту, адаптуючись до стилю розмови [2].

Основні компоненти системи трансформера на основі ChatGPT:

- Механізм самозвернення (self-attention). Застосування self-attention дозволяє моделі ChatGPT відслідковувати залежності між словами у тексті та утримувати послідовність в рамках довгого діалогу. Це забезпечує здатність чат-боту підтримувати контекст, враховуючи як нові, так і попередні запити користувача.
- Політика обробки діалогів. Для кожного запиту система адаптує відповіді на основі збережених попередніх контекстів. Це дозволяє моделі генерувати відповіді, які є релевантними до поточного етапу розмови, зберігаючи при цьому цілісність діалогу.

- Автоматизована генерація запитів. Важливим компонентом є функція, яка дозволяє автоматично генерувати текстові запити відповідно до інтеракцій, що виникають у розмові. Вона зменшує кількість помилок і забезпечує стабільність у випадках, коли чат-бот виконує тривалі розмови з користувачем.

Основні процеси системи генерації тексту включають узгодження відповідей, корекцію помилок, адаптацію стилю та інші функції, що дозволяють чат-боту вести послідовні розмови. Обробка запитів включає наступні етапи:

1. Узгодження. Підтримання узгодженості даних є ключовою частиною процесу. На кожному етапі діалогу здійснюється перевірка попередніх відповідей, щоб забезпечити точну обробку нових запитів.
2. Адаптація до стилю. Використовуючи трансформери, система автоматично налаштовується під стиль мовлення користувача, забезпечуючи точність та зручність взаємодії.
3. Автоматичне коригування помилок. Задля покращення результатів у системі запроваджено процеси, що виявляють та усувають можливі помилки у формулюваннях текстових запитів.
4. Реплікація. В процесі взаємодії система створює репліки, які можна використовувати для збереження та перевірки відповідей.

Ця система автоматизації генерації тексту дозволяє чат-ботам на базі ChatGPT швидко та природно реагувати на потреби користувача, забезпечуючи при цьому високу точність. Подальші дослідження спрямовані на розширення можливостей інтеграції з іншими платформами та покращення управління контекстом у тривалих розмовах, що дозволить підвищити ефективність чат-ботів у різних сферах [3, 4].

Отже, запропонована методологія і система трансформера на основі ChatGPT для генерації текстових запитів чат-боту забезпечує точну і швидку побудову відповідей на основі попереднього контексту. Подальші дослідження спрямовані на покращення механізмів адаптації під стиль мовлення користувачів та вдосконалення автоматизації обробки запитів, що відкриває можливості для інтеграції цієї системи в різні цифрові платформи.

1. OpenAI. "GPT-3 and the Transformer architecture.": https://openai.com/research/gpt-3.
2. Vaswani, Ashish, et al. "Attention is all you need." Advances in neural information processing systems (2017).
3. Brown, Tom B., et al. "Language models are few-shot learners." arXiv preprint arXiv:2005.14165 (2020).
4. Devlin, Jacob, et al. "BERT: Pre-training of deep bidirectional transformers for language understanding." arXiv preprint arXiv:1810.04805 (2018).

В.В. Микитенко

ГІБРИДНИЙ СЦЕНАРІЙ ПРОСТОРОВОГО ПОВОЄННОГО ВІДНОВЛЕННЯ ПІВДЕННО-СХІДНОГО ІНДУСТРІАЛЬНОГО ПОЯСУ УКРАЇНИ (ІНДУСТРІАЛЬНОГО РОМБА)

З огляду на сучасну структуру регіональної економіки західної України та її роль у межах загальноукраїнського господарського комплексу саме Південно-Східний індустріальний пояс України (індустріальний ромб) історично є економічним ядром *господарської системи України* (ГСУ), з концентрацією важкої промисловості, металургії та видобутку корисних копалин. У контексті втрат і руйнувань від військових дій в Україні важливо зберегти східний дніпровський промисловий пояс, який відіграє для нашого державного утворення ключову роль для її дієздатності. Це, по суті, придніпровський територіально-економічний підрайон, половина від колись найпотужнішого Донецько-Придніпровського територіально-економічного макрорайону, створеного ще за часів УРСР у процесі індустріалізації ХХ ст. Цей географічний кластер за форматом індустріального ромбу Запоріжжя-Дніпро-Кривий Ріг-Кременчук має конститутивно-ключове значення і від його збереження і залежатиме майбутня індустріалізація країни та, взагалі, наявність індустріального ядра національної економіки. Якщо цей ромб не розвиватиметься за формулою розбудови продуктивних сил України, сповзання до аграрно-сировинної моделі стане незворотним.

Проте, створення індустріального ядра потребує довготривалої підготовки, капіталовкладень, а також зміни структурної моделі функціонування і стратегування та культурних факторів повоєнного відродження. Це не лише виклик часу, а й потреба у створенні нових кластерних моделей і потужного державно-приватного партнерства за умов політичної та економічної підтримки з боку ЄС. Зазначене твердження є обґрунтованим і враховує реальні соціально-економічні, військові та суспільно-політичні фактори забезпечення *сталого господарювання* (СГ). Орієнтація на просторове відродження індустріального ромбу є стратегічно вірним напрямом локалізації зусиль, зважаючи на найближчі роки нагальної регенерації реального сектору та значення цього макрорегіону для української промислової стійкості і можливостей нової індустріалізації у контексті забезпечення національної безпеки та якості життя населення.

Попередньо обґрунтовані та деталізовані вісім типових сценаріїв організації реконструктивного просторового розвитку (ОРПР) ГСУ у повоєнному періоді (інноваційно-інтеграційний; децентралізовано-стабілізаційний; індустріально-економічний; екологічно-сталий; еко-резилієнтний, економіко-резилієнтний; когнітивно-інформаційний; гібридний) [1] сформовано за використання принципів адаптивної типізації, за якими систематизовано підходи до ОРПР ГСУ, враховуючи специфічні ризики, можливості та виклики, з якими країна стикатиметься у повоєнному періоді. Їх врахування дозволило: а) відобразити

здатність сценаріїв при їх типізації передбачати різнорівневі ризики, можливості та виклики, з якими країна стикатиметься до 2030 р.; б) використати гнучкість науково-прикладних підходів задля пристосування ГСУ до специфічних умов кожного макрорегіону та наростити їхню спроможність реагувати на різні фактори, які можуть змінюватися у просторі з часом. Запропоновані сценарії, охоплюючи широкий спектр соціо-екологічно-економічних, суспільно-політичних та технологічних аспектів, дозволять забезпечити гнучкість і адаптивність ОРПР. Унікальність підходу полягає у тому, що кожен із сценаріїв може використовуватись як самостійно, так і бути інтегрованим із іншими, залежно від особливостей конкретного територіального утворення (макрорегіону).

У відповідності до напрацьованого, обґрунтовано пріоритетність реалізації у повоєнному періоді до 2030 року гібридного сценарію ОРПР (ГБС-2030), типовий склад якого розроблено для шести макрорегіонів, ідентифікованих в якості Зон повоєнного відновлення і регенерації з урахуванням усіх сценарних соціо-еколого-економічних детермінант за використання при розбудові ГБС-2030 інвестиційних, технологічних, когнітивно-інформаційних та інноваційних фільтрів [2,3]. А, саме: I) Зона Активізації (Мобілізації) реконструктивного просторового відновлення – Київ та Київська область; II) Транзисторної Зони для координації просторового розвитку – Житомирська, Вінницька, Чернігівська та Полтавська області; III) Східна Регіональна Лінії (Зона Декомпресії) – Харківська, Сумська, Донецька, Луганська і Запорізька області; IV) Південної Регіональної Лінії (Зони Декомпресії) – Миколаївська, Одеська, Херсонська області та АР Крим; V) Західної Зони Збудження (Компресії) – Закарпатська, Львівська, Рівненська, Тернопільська, Івано-Франківська та Волинська області; VI) Центральної Зони модернізації – Черкаська, Кіровоградська та Дніпропетровська області. Таке розмежування і групування національних територіальних утворень відображає функціональну роль кожного макрорегіону у відновленні та реконструкції України у повоєнному періоді та враховує стратегічні напрями розвитку кожної з шести зон. Однак, зважаючи на масштабні пошкодження від військових дій 2022-2024 рр., втрати і руйнування інфраструктури та основних засобів, потреби у відновленні реального сектору економіки [4-6], маємо уточнити цілі сценарію та склад багаторівневих механізмів реалізації ГБС-2030 саме для Південно-Східного індустріального поясу України (індустріального ромбу) – Запоріжжя-Дніпро-Кривий Ріг-Кременчук. Адже, на просторовому відновленні індустріального й енергетичного сектору цього географічного кластеру суб'єкти державного та регіонального управління і мають локалізувати усі зусилля, ресурси та можливості.

Прогнозний формат ГБС-2030 ОРПР Південно-Східного географічного кластеру із елементарними сценарними складовими (і розрахунком їхніх часток), цілями сценаріїв, які входитимуть у склад ГБС-2030, відповідним складом багаторівневих механізмів реалізації ГБС-2030 – репрезентовано у табл. 1 (представлено основні сценарні складові, які інкорпоровано до ГБС, детермінанти та багаторівневі механізми його реалізації).

Таблиця 1 – ГБС-2030 для Південно-Східного індустріального поясу України (індустріального ромбу)

Сценарні складові, частка у ГБС-2030	Цілі сценарних детермінант	Багаторівневі механізми реалізації
1. Інноваційно-інтеграційний, 15%	Забезпечення інтеграції новітніх технологій та підтримка інноваційних кластерів	Інноваційні кластери, технопарки, державно-приватне партнерство
2. Децентралізовано-стабілізаційний, 10%	Підтримка стабілізаційних ініціатив на місцевому рівні та забезпечення гнучкого управління	Місцеві програми розвитку, децентралізоване фінансування, підтримка малого і середнього бізнесу
3. Індустріально-економічний, 25%	Розвиток та модернізація ключових промислових секторів регіону	Реконструкція інфраструктури, стимулювання промислового зростання, інвестування у виробництво
4. Екологічно-сталий, 15%	Підтримка екологічної сталості та запровадження ресурсозберігаючих технологій	Екологічний моніторинг, розвиток відновлюваної енергетики, мінімізація забруднення
5. Когнітивно-інформаційний, 20%	Використання цифрових інструментів та ШІ для управління промисловими процесами	Цифровізація управління, застосування великих даних та аналітики для оптимізації процесів
6. Еко-резилієнтний, 5%	Забезпечення екологічної стійкості у промислових районах та адаптація до кліматичних змін	Екологічна адаптація, програми ре- соціалізації територій, зелена інфраструктура
7. Економіко-резилієнтний, 10%	Підтримка економічної стійкості та адаптація до змін економічного середовища	Економічне прогнозування, забезпечення стабільності ринків, інструменти підтримки підприємництва

Джерело * Сформульовано, обґрунтовано та систематизовано автором

З огляду на зазначене маємо можливість надати характеристику, специфічні ознаки та переваги пропонованого для використання при регенерації й ОРПР Південно-Східного індустріального поясу України ГБС-2030, у якому поєднано елементи інноваційного, екологічного, економічного, індустріально-економічного та когнітивно-інформаційного розвитку. Реалізацію цього варіанту ГБС-2030 спрямовано на комплексне відновлення та стійкий розвиток Південно-Східного географічного кластеру, акцентуючи на цифровізації управління, підтримці екологічної стійкості, модернізації промисловості та зміцненні економічної стійкості ГСУ. Передбачається поєднання у ГБС-2030 інноваційно-інтеграційних, індустріально-економічних, екологічно-сталих, економіко-резилієнтних та когнітивно-інформаційних підходів до ОРПР. При цьому, основою ГБС-2030 Південно-Східного індустріального поясу – є реконструкція та модернізація ключових промислових потужностей у поєднанні з екологічною адаптацією та впровадженням цифрових технологій, що підвищить ефективність та гнучкість промислових процесів і пришвидшить регенерації реального сектору у посткризовому періоді. Перевагами ГБС-2030 є: стійкість до змін та ризиків; підтримка інновацій та індустріалізації; зменшення екологічного навантаження та екологічна адаптація; підвищення соціальної стабільності; забезпечення економічного зростання; економічна ефективність; розвиток цифрової інфраструктури і людського капіталу.

1. Mykytenko, V.V. Hybrid scenario of the organization of reconstructive spatial development of the economic system of Ukraine. Innovations and New Directions in Scientific Research: Proceedings of the International Scientific Conference (2024, October 14). Manchester, UK: Bookmundo, International Education Development Center, Research Europe, 2024. P.23-26.
2. Mykytenko, V.V. Synthesis of societal opportunities: experience of reconstructive strategizing in the energy sector. Trends, Issues, and Challenges in Modern Science: Proceedings of the International Scientific Conference (2024, September 13). Cambridge, UK: Bookmundo. International Education Development Center, 2024, Research Europe, 2024. P. 25-28.
3. Микитенко, В. В. Гібридний сценарій реконструкції просторового розвитку України у повоєнному періоді: когнітивно-інформаційний драйвер та інвестиційні епюри. Сучасні досягнення та перспективи науки та освіти: матеріали II Міжнародної науково-практичної конференції (Житомир, 4 жовтня 2024 р). Міжнародний гуманітарний дослідницький центр, Research Europe, 2024. С. 233-238.
4. Ukraine. Rapid Damage and Needs Assessment February 2022 – February 2023 / Ed. A. Himmelfarb. The World Bank, the Government of Ukraine, the European Union, the United Nations. March 2023, Washington, DC. 132 p. URL: https://documents1.worldbank.org/curated/en/099184503212328877/pdf/P1801740d1177f03c0ab180057556615497.pdf.
5 Updated Ukraine Recovery and Reconstruction Needs Assessment Released. URL: https://www.worldbank.org/en/news/press-release/2024/02/15/updated-ukraine-recovery-and-reconstruction-needs-assessment-released.
6. The World Bank in Ukraine. Entering into the third year, Russia's invasion of Ukraine is a tragedy with far-reaching human and economic impacts. We will continue supporting the people of Ukraine through urgent repair projects and coordination with the Government for recovery and reconstruction efforts. URL: https://www.worldbank.org/en/country/ukraine/overview.

Ю.С. Мурзін

ВПЛИВ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ НА УПРАВЛІННЯ ПЕРСОНАЛОМ ПІДПРИЄМСТВ ЕНЕРГЕТИЧНОГО СЕКТОРУ В НЕБЕЗПЕКОВИХ УМОВАХ

Цифрова трансформація суттєво змінює управлінські процеси в енергетичному секторі, особливо в умовах підвищених безпекових викликів. Цей процес передбачає не лише технологічні зміни, а й адаптацію управлінських підходів, що стає критично важливим для підтримки ефктивності бізнесу. Впровадження новітніх технологій не тільки оптимізує внутрішні процеси, але й забезпечує адаптацію до нових реалій, пов'язаних із кризовими ситуаціями, такими як воєнні або економічні нестабільності.

Основні аспекти впливу цифрової трансформації на управління персоналом у небезпекових умовах: впровадження автоматизації та інтелектуальних систем, застосування штучного інтелекту, машинного навчання та автоматизації, що дозволяє знизити завантаження на персонал, автоматизувати рутинні операції та зменшити ймовірність людських помилок. Це особливо важливо для оперативного управління ризиками в небезпечних умовах, особливо коли проблему потрібно ліквідувана та підприємствах енеогетичного сектору, яка відбулання від повномаштабного обстрілу [1].

Складові цифровізаційного процесу управління персоналом в небезпекових умовах:

1. Безпека та охорона праці:

Регулярне навчання з охорони праці.

Використання захисного обладнання.

Внутрішні інструкції та правила.

2. Психологічна підтримка та стресостійкість:

Робота з психологами та коучами.

Психологічні тренінги та мотиваційні програми.

3. Розробка та впровадження планів евакуації та дій у надзвичайних ситуаціях:

Плани евакуації.

Регулярні тренування з екстрених ситуацій.

Швидка реакція на повітряні тривоги.

Обізнаність знаходження укриття чи сховища.

4.Контроль стану здоров'я співробітників:

Медичні огляди.

Оцінка фізичної та психологічної готовності.

5. Інноваційні технології для моніторингу безпеки:

Системи моніторингу.

Впровадження аналітики великих даних.

Інформаційна безпека.

6. Гнучке управління персоналом та організація робочого часу:
Ротація кадрів.
Гнучкі графіки.
Онлайн робота (небезхпекові фактори чи стан здоров'я)
7. Розвиток цифрових компетентностей та використання технологій:
Цифрове навчання та тренінги.
Дистанційний моніторинг та управління.
Цифрова грамотність.
8. Розробка та впровадження стандартів безпеки:
Міжнародні стандарти.
Постійне вдосконалення стандартів безпеки.

Управління персоналом в енергетичному секторі, особливо в небезпечних умовах, які відбуваються в Україні (воєнний стан) є складним і багатогранним процесом. Даний процес вимагає врахування специфіку галузі, а також ризиків, пов'язаних із безпекою праці, що може вплинути на ефективність роботи, добробут співробітників та загальне функціонування самої галузі, яка приновить користь для інших галузей та держави. Всі ці фактори передбачають комплексний підхід до планування, допомоги, мотивації та розвитку персоналу з акцентом на конкретну галузь та ризики, пов'язані з роботою [2].

Цифрова трансформація енергетичного сектора є критично важливою для підвищення стійкості та ефективності роботи в умовах, які є небезпечними. Впровадження новітніх технологій і систем управління дозволяє знизити ризики, пов'язані з безпекою, та оптимізувати процеси. А також має значний потенціал підвищити стійкість і безпеку галузі. Вона забезпечує можливості для управління ризиками, оптимізації нових процесів та підвищення загальної ефективності. Проте для успішної реалізації цієї трансформації необхідно подолати ряд викликів, включаючи фінансові витрати та потреби в навчанні персоналу.

Цифрова трансформація є ключовим фактором для успішного управління персоналом в енергетичному секторі в умовах небезпеки. Вона забезпечує можливості для підвищення ефективності бізнес-процесів і залучення працівників. Проте її реалізація потребує чіткої стратегії та адаптації.

1. Iryna Kalina, Nataliia Shuliar. Strategy for the development of digital technologies for business processes at an enterprise in/under conditions of economic uncertainty: monograph. Recommended for publication by the Academic Council of the Interregional Academy of Personnel Management (Protocol No. 7 dated July 5, 2023). 2023. 168 c. URL: http://surl.li/qbwcc.
2. Каліна І.І., Шуляр Н.М., Мельник Б.Ю., Палій С.А. Управління кадровим забезпеченням діяльності аграрних підприємств: Монографія. Київ. Інтерсервіс.2024. 232 с.

М.В. Антонішин, В.Л. Леднєй, М.Ю. Мигун

ПРОБЛЕМАТИКА РОЗВИТИКУ КІБЕРБЕЗПЕКИ ЕНЕРГЕТИКИ З ТОЧКИ ЗОРУ ПОБУДОВИ КІБЕРОБОРОНИ ДЕРЖАВИ

У Законі України «Про основні засади забезпечення кібербезпеки України» є визначення кібероборони. *Кібероборона – сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії*. Кіберзахист енергетичного сектору України, як складова кібероборони держави, має певні недоліки, які обмежують її ефективність і збільшують уразливість до сучасних кіберзагроз. [1]

Міністерство енергетики України проводить роботу щодо побудови галузевої системи кіберзахисту підприємств паливно-енергетичного комплексу України. Відповідна система грунтується на концентрації зусиль в рамках функціонування двох галузевих кіберцентрів, створених на базі НЕК «УКРЕНЕРГО» та НАК «Нафтогаз України». Передбачається, що після набуття повних спроможностей в сфері кіберзахисту,відповідні кіберцентри стануть галузевими центрами кібербезпеки для електроенергетичного та нафтогазового комплексу відповідно, а в подальшому також ядерно-промислового, вугільно-промислового, торфодобувного комплексів. В рамках ядерно-промислового комплексу, вважаємо необхідним розгортання локальних кіберцентрів для кожного з об’єктів, які будуть підпорядковані галузевим кіберцентрам. [2]

В 2023-2024 роках в рамках проведення дослідження стану кібербезпеки, була проведена діагностика об’єктів критичної інфраструктури, в тому числі і енергетичного сектору за наступними критеріями: обладнання оновлене та актуальне, внутрішнє шифрування трафіку, повне покриття EDR/AV, імплементація MFA, наявність SIEM-систем, резервування даних та систем, повне проведення класифікації активів та інформації, постійне оцінювання ризиків кібербезпеки, формалізовані функції команд IT та кібербезпеки, організація повністю забезпечення фахівцями з кібербезпеки. [3]

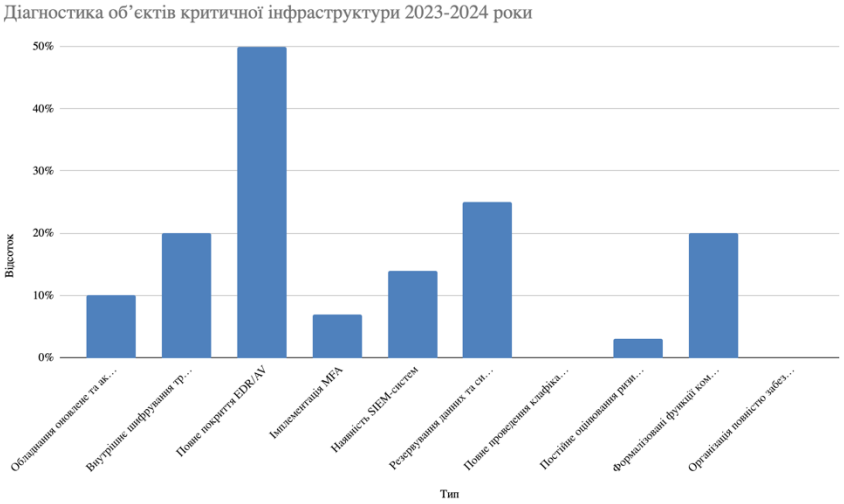


Рисунок 1 – Статистика дослідження зі стану кібербезпеки об'єктів критичної інфраструктури згідно DAI Intl

Проведений аналіз статистичних даних, який наведений на Рисунку 1, можливо виділити наступні проблеми, які заважають розвитку кібербезпеки в енергетиці:

1. ***Відсутність цілісної та єдиної кібербезпекової стратегії для енергетичного сектору***. Хоча існують загальні стратегії кібербезпеки та документи, що регламентують захист критичної інфраструктури, вони не враховують специфіку енергетичної галузі, що вимагає унікальних підходів до захисту SCADA-систем, систем автоматизованого управління та критичних промислових мереж.

2. ***Недостатня інтеграція новітніх технологій***. Багато підприємств енергетичного сектору використовують застарілі системи, що були впроваджені без врахування вновь виникаючих та сучасних кіберзагроз. Впровадження сучасних технологій моніторингу, аналізу аномалій та автоматизації кіберзахисту є обмеженим, що збільшує ризик інцидентів.

3. ***Брак кваліфікованих фахівців***. Кіберсфера вимагає наявність достатньої кількості висококваліфікованих спеціалістів, однак у державних структурах та підприємствах енергетичного сектору бракує кадрів з відповідними знаннями. На ринку праці, український енергетичний сектор не може скласти конкуренцію іноземним компаніям на ринку праці.

4. ***Недостатнє фінансування та інвестиції в кібербезпеку***. Для забезпечення виконання заходів з надійної кібероборони держави, енергетичного сектору потрібні значні фінансові ресурси на оновлення

обладнання, навчання персоналу та впровадження сучасних технологій. Проте обмежене фінансування державних підприємств та залежність від державного бюджету обмежують можливості для таких інвестицій.

5. ***Незавершена система обміну інформацією про кіберзагрози***. В Україні все ще не до кінця налагоджена система оперативного обміну інформацією між державними органами, приватним сектором та міжнародними партнерами. Через це реагування на кіберінциденти часто є несвоєчасним, що дозволяє загрозам поширюватися без належного протистояння.

6. ***Складність дотримання міжнародних стандартів кібербезпеки***. Впровадження міжнародних стандартів, таких як NIS Directive чи ISO/IEC 27001, є викликом для багатьох енергетичних підприємств через відсутність ресурсів та обмеження регуляторного середовища, що ускладнює процес стандартизації та узгодження з міжнародною практикою.

7. ***Вразливість до кібератак через низький рівень взаємодії з суміжними секторами***. Енергетичний сектор тісно пов'язаний з іншими галузями (транспорт, зв'язок, державне управління), але координація заходів захисту між ними часто є недостатньою. Низька міжсекторальна взаємодія ускладнює комплексну оборону проти кібератак.

Означена проблематика наявна у всіх галузях та сферах економіки України. Для її подолання необхідно підвищувати фінансування. З метою покращення ситуації необхідно мати окерму фінасову програму для виконання заходів з кіберзахисту, а під час бюджетування, статті витрат на побудову, підтримку та розвиток системи кібербезпеки мають формуватись окремо від сттатей витратт на забезпечення функціонування IT-підрозділів. Також необхідно постійно вдосконалювати та розширювати систему підготовки кадрів, в тому числі забезпечення постійного підвищення кваліфікації, враховуючи постійний розвиток кібертехнологій. Окремо треба забезпечити конкуретну оплату та соціальне забезпечення фахівців з кібербезпеки. Необхідно враховувати розвиток кіберзагроз, що необхідно постійне оновлення та актуалізації програмного та програмно-апартного забезпечення системи кіберзазхисту. Необхідно розвивати національні та міжнародні стандарти захисту критичної інфраструктури, а також налагоджувати більш ефективний обмін інформацією щодо кіберзагроз між зацікавленими сторонами. Ці заходи мають підвищити спроможності виконання енегетичним сектором заходів з кібероборони держави.

1. Інтерв'ю з Вадімом Леднєєм, фахівцем з кіберборотьби Генштабу ЗСУ. URL: https://lb.ua/news/2023/01/31/544318_vadim_liedniey_metoyu_diyalnosti.html.
2. Кібербезпека енергетичної галузі. Офіційний сайт Міністерства енертегити України. URL: https://mev.gov.ua/storinka/kiberbezpeka-enerhetychnoyi-haluzi.
3. Матеріали семінару DAI Intl. "Кібербезпека критичної інфраструктури", лютий 2024.

В.В. Кав'юк, Г.Л. Коростильов

ЕЛЕКТРОХІМІЧНІ ГЕНЕРАТОРИ НА ОДНОВІСНИХ НАПІВПРИЧЕПАХ - АЛЬТЕРНАТИВНЕ ДЖЕРЕЛО ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ ПОВІТРЯНИХ СИЛ УКРАЇНИ

В умовах триваючої війни та інтенсивного переходу Збройних Сил України від пострадянської до західної парадигми застосування, управління та забезпечення військ (сил) повинна бути можливість вибору різних форм та способів забезпечення життєдіяльності аеродромів ПС (Повітряних Сил), до яких належить і енергопостачання.

На даний час на аеродромах живлення електричною енергією бортових споживачів повітряних суден (ПС) здійснюється шляхом статичного перетворення струму промислової мережі в централізованих системах електропостачання на автономні.

Однак у разі ураження аеродрому противником і перебою живлення промислової мережі - виникає небезпека зриву бойового завдання. У цьому разі використовуються засоби аеродромно-технічного забезпечення польотів авіації (ЗАТЗП) такі, як авіаційні пересувні електроагрегати АПА-5Д та АПА-80, що перетворюють механічну енергію двигунів внутрішнього згоряння в електричну, в генераторах постійного струму ПР600 х 2 і генераторах змінного струму ГТ40-ПЧ6, БСГ-112 - 40. Однак ці пересувні енергетичні ЗАТЗП мають високі масо-габаритні параметри, високий рівень шуму, потребують великих експлуатаційних витрат на обслуговування в процесі роботи і значні витрати при їх технічному обслуговуванні, а також великий час для виходу на робочі режими роботи.

Тому є життєва необхідність, щодо використання автономних високомобільних джерел енергії, що мають необхідні характеристики енергопостачання на борт ПС як змінного, так і постійного струму - на всі типи літаків з можливістю модульної побудови ЕХГ (електрохімічних генераторів) на високомобільних одновісних напівпричепах і це на зараз стає дуже актуальною вимогою.

До того ж у [3] наголошується на необхідності пошуку альтернативних джерел енергії для електропостачання ПС, заснованих на нових принципах отримання енергії та на новій елементній базі. У роботах [1; 2] вказується на доцільність використання ЕХГ на паливних елементах (ПЕ). В ЕХГ використовується пряме перетворення хімічної енергії в електричну, відсутні деталі, які піддаються тертю, вони економічно перспективні. Вони легші і займають менший об'єм, ніж традиційні джерела, безшумні, менше нагріваються, більш ефективні з точки зору перетворення палива.

Основним елементом ЕХГ є паливний елемент (ПЕ) – це первинне (що не перезаряджається) джерело струму, в якому електрична енергія

безпосередньо утворюється за рахунок реакції між паливом (відновником) і окислювачем.

На відміну від гальванічних елементів реагенти в паливних елементах не поєднані з електродами, а зберігаються окремо і підводяться до них у міру протікання хімічних реакцій. Самі електроди в реакцію не вступають, але є каталізаторами цих реакцій. Їхня функція – відбір електронів від відновника і передача їх окислювачу. ПЕ – це засіб тривалого користування.

Питома енергія ПЕ значно вища, ніж у гальванічних елементів. У них використовують:

– рідкі або газоподібні відновники: водень, гідразин, метанол, вуглеводні;

– окислювачі: кисень, пероксид водню.

У паливних елементах протікає реакція окиснення палива, у результаті утворюються електроенергія, продукти окиснення палива і виділяється тепло:

– паливо + окислювач = електроенергія + продукти окислення палива + Q.

Цей процес може бути представлений у вигляді таких стадій:

– анодне окислення палива;

– катодне відновлення окислювача;

– рух іонів у розчині або сплаві електроліту;

– рух електронів від анода до катоду в зовнішньому ланцюзі.

Авіаційні ЕХГ для збільшення маневреності в умовах ведення бойових дій, доцільно розміщати на одновісних причіпних модулях, залежно від маси самого генератора, тобто пропонується перехід від застарілих базових шасі УРАЛ-4320 і ЗІЛ-131 на контейнерний або блочно-модульний принцип розміщення ЗАТЗП, а саме на одновісні причіпні модулі. Тоді можливе завчасне встановлення цих енергомодулів на аеродромах тимчасового базування. У цьому разі не потрібно перебазування ЗАТЗП, а отже, скорочується час на підготовку ПС до польотів.

Не можна, при веденні бойових дій, не звернути увагу на такий не маловажливий фактор, як маскування аеродромів, ПС і ЗАТЗП [4]. З метою маскування та протидії повітряної розвідці БПЛА (безпілотних літальних апаратів противника) з виявлення місця розташування ПС цей енергомодуль на базі маневреного одновісного причіпного модуля можна легко та швидко заховати від ракетно-бомбового ураження в замасковані підземне сховище (в авіації-капонір), тому що під час його роботи не потрібне повітря, а паливо і окиснювач надходять із систем зберігання і подачі, що входять до складу електроустановки. У такому стані енергомодуль може перебувати як завгодно тривалий час, оскільки його ресурс роботи досягає 30-40 тис. год, а споживання реагентів відбувається тільки під час вироблення електричного струму, процес саморозряду дуже малий малий. До того ж підземне зберігання та експлуатація авіаційних ЕХГ дасть змогу розв'язати питання захисту від вражаючих чинників будь-якої зброї.

Таким чином використання ЕХГ як автономного, високомобільного та високоманевреного джерела змінного та постійного струмів щодо енергозабезпечення запуску і обслуговування ПС при веденні бойових дій.

1. Багоцький В. С., Осетрова А. М., Скундин А. М. // Електрохімія. – 2003. 39. С. 127.
2. Білоус А. Г., Юнонова О, І., Солопай С. О., Коваленко Л.Л. Електролітні електродні матеріали для низькотемпературних паливних елементів // В: Фундаментальні проблеми водневої енергетики. Київ: Видавництво «Kim». 2010 – С. 409-424.
3. Резервні джерела електропостачання. Нормативна база. Електронна версію журналу ТОВ № «Охорона праці». 15.05.2022. URL: https://ohoronapraci.kiev.ua/article/news/rezervni-dzerela-elektropostacanna-normativna-baza (дата звернення: 31.10.2024).
4. Підвищення якості заходів маскування військ та об’єктів. *Методичні рекомендації військам (силам) Збройних Сил України*. Практичний посібник. Видавництво: ЦУЛ, 2024.134 с. ISBN978-611-01-3003-5.

О.Ю. Коновалов

ІІОТ ЯК ЗАСІБ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ВИРОБНИЧИХ МОДЕЛЕЙ

Широке впровадження у виробництво та різні сфери життя новітніх цифрових технологій призводить до оцифрування і обробки оцифрованої інформації. Таке явище вимагає значної модернізації, або створення специфічної ІТ-інфрастуктури і потребує підготовки спеціалістів з ІТ-технологій. Впровадження у виробничі процеси нових технологічних рішень призводить до зміни продуктивних відносин і виробничої культури. Як показала практика економічно розвинутих країн, ці процеси викликають зміни у більшості сфер економіки — від управління бізнес-процесами і впровадження нових технологій і обладнання, до нових моделей управління бізнесом [1].

Крім того технології значною мірою впливають на процеси взаємодії з клієнтами. Нові форми взаємодії значно відрізняються від тих, що були звичними для нас протягом останніх десятиліть. Цифровізація в більшості випадків допомагає переосмислити звичні нам правила і тенденції, що дозволяє ефективно реагувати на потреби ринку і вимоги клієнтів на фоні революційних інформаційних зрушень в економіці і принципах обробки інформації. Технологічна революція Industry 4.0 і технологічні інновації у сфері інформаційних технологій вплинули на виробничі відносини і призвели до «підривних інновацій» (Disruptive innovation) у багатьох сферах економіки і стали рушійною силою різких змін соціально суспільних відносин, і особливо на ринку продуктивних відносин.

Одною з ключових технологій програми Industry 4.0 вважається Інтернет Речей (IoT). Industry 4.0 означає розумне використання даних і цифрових технологій для вдосконалення бізнес-процесів і виробничих систем у виробничому секторі [2,3]. Зростаючий розвиток Індустрії 4.0 має потенціал для ще більшого впливу, відкриваючи переваги для промисловості, працівників і суспільства. Впровадження Industry 4.0 можна зробити багатьма способами, зокрема шляхом підвищення ефективності виробництва, що веде до появи більшої кількості кращих продуктів і послуг, а також відкриває можливості для підвищення кваліфікації робітників, щоб зберегти якісні робочі місця.

ІІоТ можна розглядати як складну інфраструктуру компютерного обладнання поєднаного між собою різними типами телекомунікаційних мереж. В різних місцях цієї системи знаходяться виробничі об'єкти на яких розташовані ІІоТ датчики і спеціалізоване програмне забезпечення для контролю за станом процесів, автоматизації управління і контролю параметрів і характеристик технологічних процесів. Створення такої інфраструктури досить складний процес і вимагає декількох етапів,

починаючи від монтажу датчиків, запуск і програмування контролерів, регулювання виконавчих механізмів та відладку програмного забезпечення. Тільки після цього можна виконувати моніторинг і обробку отриманої інформації. Отримані дані аналізуються і на їх основі приймаються відповідні рішення щодо стану технологічного процесу, точності вимірювання характеристик, необхідності регламентних або відновлювальних робіт і робляться висновки про стан і якість функціонування підприємства в цілому [2,3].

Основною проблемою стає питання обробки отриманих даних, і відповідна інтерпретація результатів вимірювання, або аналіз використання відповідниго обладнання при виконанні робочих завдань. Для цього використовуються спеціалізовані програмні платформи, основне завдання яких проводити збір інформації з датчиків IIoT, її обробку і керування технологічними процесами. Адміністративна оболонка (Administration Shell Industry 4.0 (AAS)) – формат стандартизованого обміну даними IoT на платформі Industry 4.0. Це сполучна ланка між матеріальними активами та світом IIoT [2,3].

AAS є інструментом, який забезпечує будь-який промисловий компонент можливостями спілкування та обміну інформацією з цифровим світом IIoT (рис. 1).

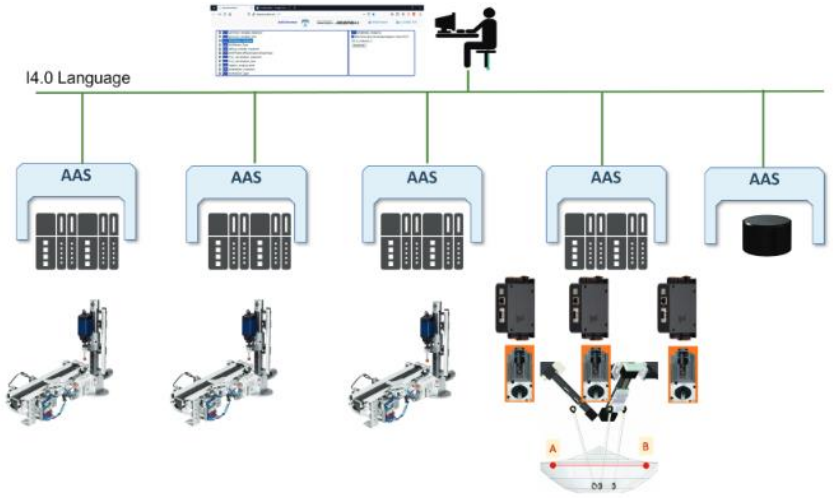


Рисунок 1 – Архітектура автоматизації станції вибору та розміщення (*Pick and Place station)*

Адміністративна оболонка (Administration Shell Industry 4.0 (AAS)) - це стандартизоване цифрове представлення активу для забезпечення взаємодії між програмами, що управляють виробничими системами. Це обмін даними,

пов'язаними з активами, між промисловими активами та між активами та системами управління виробництвом або інженерними інструментами.

Типи адміністративних оболонок (Administration Shell Industry 4.0 (AAS))

- Пасивні - прямої взаємодії з AAC не передбачено
- Реактивні - реагує на зовнішні запити взаємодії.
- Проактивні - ініціювання активної поведінки і, якщо потрібно, на запити зовнішніх учасників системи, що надсилаються AAS.

Технологія IIoT може бути розгорнута на виробництвах і дозволяє значною мірою заощаджувати кошти за рахунок автоматизації контролю і управління, а також використання безпроводових технологій і мобільних додатків на безпроводовому обладнанні з підтримкою або спеціалізованих протоколів або стеку протоколів TCP/IP. Крім того асортимент датчиків постійно розширюється за рахунок нових моделей, що мають більше функцій і можливостей підтримки широкого спектру промислового обладнання і керування ним.

Багато виробників обладнання для IIoT з кожним роком розширюють асортимент датчиків і оновленого програмного забезпечення, що дозволить вже найближчим часом змінити парадигму організації виробничого процесу, що в першу чергу призведе до скорочення витрат на підтримку технологічних операцій. Крім того стрімкий розвиток технологій штучного інтелекту дозволить винести локальні виробничі процеси якими керують програмовані контролери в хмарну інфраструктуру. Така ситуація надасть можливість оперативно керувати значними кількостями виконавчих механізмів на розподілених виробництвах по всьому світу.

Основною проблемою такого підходу до організації виробничих потужностей є слабка захищеність таких систем від зловмисників. Тому найближчим часом будуть розвиватись напрямки пов'язані з безпекою IIoT. Покращення безпеки IIoT пристроїв повинно значною мірою стимулювати дану галузь до швидкого розвитку. В першу чергу потрібно приділяти увагу спеціалізованим рішенням по сертифікації обладнання, заходів мережевого захисту периметра промислової мережі, механізми шифрування і контроля доступу до апаратних засобів IIoT розрахованих на підключення до Інтернету.

Згідно майбутнє індустріального Інтернету речей (IIoT) у 2023 році та далі відзначене кількома ключовими тенденціями [4]:

1. Більше підключених пристроїв: кількість пристроїв IIoT збільшиться щонайменше вдвічі, і вони стануть розумнішими, враховуючи ШІ, хмарні обчислення та віртуальну реальність.
2. IIoT Manufacturing as a Service: з'явиться новий підхід під назвою IIoT Manufacturing as a Service. Це схоже на модель виробництва з оплатою за використання, де компоненти можуть надходити від третіх сторін, зберігаючи певні стандарти.

3. Хмарні та периферійні обчислення: використання хмарних та периферійних обчислень швидко зростатиме. Це означає, що пристрої на межі мережі можуть збирати дані та підключатися до хмари для швидшого доступу.

4. Прогнозне технічне обслуговування: Виробники передбачають можливі проблеми ще до їх виникнення, мінімізуючи час простою та знижуючи витрати.

5. Управління даними процесу (PDM): виробники зосередяться на PDM для швидкої обробки величезних обсягів даних IIoT. Ці дані допомагають покращити роботу та захистити від кібератак.

6. Цифрові близнюки: створюються віртуальні копії фізичних об'єктів, що дозволяє здійснювати моніторинг у реальному часі, оптимізувати продуктивність, прогнозувати несправності та скорочувати час простою.

7. Відстеження місцезнаходження: потрібна для моніторингу активів, обладнання та персоналу в режимі реального часу.

8. Блокчейн для ланцюжка поставок: потрібна для прозорості ланцюжка поставок і цілісності продукту.

9. Інтелектуальне виробництво: інтелектуальне виробництво запропонує комплексне уявлення про діяльність заводу, допоможе виявити аномалії та підвищити ефективність роботи.

10. Машинне навчання. Машинне навчання відіграватиме вирішальну роль, визначаючи шаблони процесів, прогнозуючи проблеми та пропонуючи аналітику в реальному часі.

Ці тенденції свідчать про те, що IIoT швидко розвивається, дає змогу краще приймати рішення на основі даних і змінює такі галузі, як виробництво, транспорт та енергетика.

1. Everything you need to know about AI in 2023: the 6 must-read blogs https://www.weforum.org/agenda/2023/11/ai-2023-governance-summit/.
2. Six IIoT Technology Trends to Watch in 2017. (б. д.). Schneider Electric Blog. https://blog.se.com/industry/machine-and-process-management/2017/02/23/six-iiot-technology-trends-watch-2017/.
3. Digital Twin and AAS in the Industry 4.0 Framework https://www.researchgate.net/publication/336880479_Digital_Twin_and_AAS_in_the_Industry_40_Framework.
4. *Asset Administration Shell Reading Guide*. (б. д.). https://www.plattform-i40.de/IP/Redaktion/EN/Downloads/Publikation/AAS_Reference_Modelling.pdf?__blob=publicationFile&v=1.
5. WELLNUTS. (2023, 1 серпня). Trends of IoT to Keep an Eye on in 2023. LinkedIn: Log In or Sign Up. https://www.linkedin.com/pulse/trends-iot-keep-eye-2023-wellnutscg.

М.О. Теплицький

СИСТЕМА ІНТЕЛЕКТУАЛЬНОГО КЕРУВАННЯ СВІТЛОДІОДНИМ ОСВІТЛЕННЯМ ДЛЯ ПРОМИСЛОВИХ СКЛАДСЬКИХ ПРИМІЩЕНЬ

Сучасне суспільство важко уявити без світла, яке стало невід'ємною частиною нашого повсякденного життя. Освітлювальні системи не лише створюють комфортні умови для праці та навчання, а й мають значний вплив на загальний добробут людини. Близько 90% інформації про навколишній світ людина сприймає саме за допомогою зору, що підкреслює ключову роль світла у формуванні нашого візуального сприйняття.

Коли йдеться про освітлення у складських приміщеннях, часто складається враження, що цьому аспекту не приділяють належної уваги. Зазвичай обмежуються кількома точковими джерелами світла, такими як лампи розжарювання, що є застарілим рішенням. Проте сучасний науково-технічний прогрес, особливо у сфері енергоефективного освітлення, відкриває нові можливості. Розробка інтелектуальних систем освітлення для промислових приміщень стає все більш актуальною, оскільки вона пропонує низку переваг, таких як зниження енергоспоживання, підвищення ефективності роботи персоналу, а також забезпечення адаптивного та комфортного освітлення, відповідно до потреб конкретного простору [1].

Основні переваги впровадження інтелектуальної системи освітлення в громадських, складських, промислових приміщеннях це:

1. Енергоефективність: інтелектуальні системи освітлення можуть автоматично регулювати рівень освітлення відповідно до природних умов та активності в приміщенні, що дозволяє знизити споживання електроенергії на 30-70%.

2. Покращення комфорту: системи можуть адаптувати освітлення до потреб користувачів, створюючи оптимальні умови для роботи та відпочинку. Це підвищує продуктивність праці та задоволеність співробітників.

3. Збільшення терміну служби світильників: завдяки автоматизованим системам управління, які вимикають освітлення в неробочий час або зменшують яскравість при наявності природного освітлення, термін служби ламп може бути значно подовження.

4. Безпека та гнучкість: інтелектуальні системи освітлення можуть інтегруватися з системами безпеки, активуючи освітлення у відповідь на рух або інші події, що підвищує загальний рівень безпеки в приміщеннях, та легко адаптовані до змін у структурі приміщень або умовах експлуатації.

5. Зниження витрат: завдяки зменшенню споживання енергії та підвищенню ефективності, витрати на електроенергію знижуються, що в свою чергу впливає на загальні витрати на експлуатацію приміщень.

Ці переваги роблять інтелектуальні системи освітлення привабливими для широкого спектра застосувань у різних секторах.

У 2015 році близько 20% комерційних будівель були оснащені системами управління освітленням, що стало наслідком зростання популярності сертифікації "зеленого" будівництва та покращення технологій таких систем [2]. Інтеграція систем управління освітленням у новобудовах має вищий рівень впровадження порівняно з модернізацією в існуючих будівлях. Основними підходами до розробки систем управління освітленням є три ключові стратегії: впровадження енергоефективних освітлювальних пристроїв, вдосконалення методів проєктування освітлення та оптимізація систем управління для мінімізації енергоспоживання при збереженні візуального комфорту користувачів. Ці стратегії є важливими факторами, що впливають на ефективне управління освітленням у будівлях.

Історично системи управління освітленням здебільшого працювали на основі виявлення присутності, автоматично вмикаючи світильники при реєстрації людей у зоні. Попри можливість враховувати природне освітлення та регулювати яскравість залежно від денного світла, світильники залишалися увімкненими навіть тоді, коли це не було необхідно.

Новий підхід дозволяє зменшити енергоспоживання, адже світильники активуються лише за потреби, автоматично регулюються під час роботи та вимикаються після закінчення заданого часу затримки, якщо датчик не виявляє присутність. Метод виявлення відсутності нині визнаний ефективним способом енергозбереження та часто включається до рекомендацій у програмах стимулювання раціонального використання енергії. Ручне увімкнення може реалізуватися через різні типи входів управління, забезпечуючи додаткову гнучкість у використанні системи. Світловіддача всіх освітлювальних приладів з часом знижується через старіння ламп, забруднення оптичних компонентів і накопичення пилу та бруду на поверхнях приміщень. Зазвичай це враховується на етапі проєктування освітлення: початковий рівень освітленості збільшується з урахуванням планів обслуговування та очищення.

Інтелектуальні системи освітлення вирішують цю проблему, автоматично регулюючи яскравість. Спочатку вони зменшують потужність ламп, коли вони нові, щоб відповідати заданому рівню освітлення. Це дозволяє скоротити енергоспоживання на 10–20% залежно від частоти обслуговування, а також покращує візуальний комфорт, уникаючи надмірної яскравості.

1. Іоффе К. І., Черкашина О. Л. (2018). Конспект лекцій з дисципліни «Системи керування світлотехнічними пристроями» (для магістрів денної і заочної форм навчання спеціальності 141 – Електроенергетика, електротехніка та електромеханіка (спеціалізація «Світлотехніка і джерела світла»)). ХНУМГ ім. О.М. Бекетова.
2. Roohi MH, Khorsandi A, Setayesh A, Eslamieh A, Saidi H. (2015). Design and implementaion of smart building lighting system. *In international congress on electric industry automation 2015* (pp. 7-10). IEEE.

І.Д. Тимоха

РОЗРОБКА ГІБРИДНОЇ СИСТЕМИ ЕНЕРГОЗАБЕЗПЕЧЕННЯ НА ОСНОВІ СОНЯЧНИХ ПАНЕЛЕЙ І АКУМУЛЯТОРНИХ БАТАРЕЙ

З урахуванням ситуації сьогодення, відключення електричної енергії призвело до використання альтернативних джерел енергії, наприклад сонячні батареї – це важливий і значущий крок у вдосконаленні та розвитку джерел енергії, оскільки завдяки їм можна суттєво заощаджувати, зменшуючи споживання електроенергії, а також мати живлення не залежне від енергопостачальної компанії. Зважаючи на те, що вартість кіловата постійно зростає, такі технології стають ще більш актуальними.

Традиційно сфера життя людини – це середовище електроприладів та сучасних електронних гаджетів. Щорічно зростає споживання електроенергії, а природні ресурси стають все більш обмеженими. Якщо потреби людства продовжуватимуть зростати такими ж темпами, як і в попередні роки, то нафта, газ та вугілля можуть бути вичерпані. Тому важливо шукати нові джерела енергії – альтернативні, нетрадиційні та відновлювані. Зокрема, різноманітні геліосистеми використовують сонячне випромінювання як одне з альтернативних джерел енергії.

Сонячна енергетика є одним із найбільш перспективних напрямків розвитку альтернативних джерел енергії. Сучасні технології досягли такого рівня, що сонячні панелі можуть забезпечувати електроенергією заміський будинок навіть взимку, коли сонячних днів небагато, а світловий день значно коротший [1].

Принцип роботи сонячної батареї базується на здатності сонячного світла (електромагнітного випромінювання) взаємодіяти з матеріалом, передаючи енергію фотонів (світлових частинок) електронам речовини. Це перетворення енергії світла в постійний електричний струм називається фотоелектричним ефектом (фотоефектом), який був відкритий ще в 19 столітті. Для цього процесу потрібні фотоелектричні перетворювачі або фотоелементи, які працюють на основі напівпровідників [4].

Сонячна та вітрова енергія є не тільки безкоштовним джерелом енергії, але й екологічно чистим. Через їхню залежність від сонячного світла та вітру вченим довелося вирішити проблеми, щоб підвищити надійність цих джерел. Використання обох джерел з акумулятором стає все більш популярним у віддалених місцях. Акумуляторна система забезпечує резервне живлення протягом кількох днів у випадку, якщо будь-яке з джерел або обидва недоступні, що зменшує використання викопного палива, а це дуже економічно вигідний і надійніший енергетичний ресурс. Ця система називається гібридними відновлюваними джерелами енергії. Переважна кількість країн світу поставили собі за мету перейти до відновлюваної

енергетики, наприклад, Сполучені Штати Америки мають на меті досягти 80% виробництва електроенергії з відновлюваної енергії з нульовим викидом вуглецю. Однак такі системи пом'якшують проблеми переривчастості, властиві окремим відновлюваним джерелам, підвищуючи загальну надійність і стабільність виробництва енергії. Сонячна енергія демонструє пік потужності протягом світлового дня, тоді як енергію вітру можна використовувати навіть у періоди зниження доступності сонячної енергії [2]. Завдяки інтеграції цих джерел енергопостачання стає більш послідовним, зменшуючи ризик дефіциту електроенергії під час несприятливих погодних умов. Крім того, технології накопичення енергії, інтегровані в гібридні системи, сприяють накопиченню надлишкової енергії в періоди пікового виробництва, таким чином дозволяючи її використовувати на етапах низького виробництва, таким чином підвищуючи загальну ефективність системи та зменшуючи втрати. Метою даного дослідження є вивчення теоретичних та методичних основ оцінки перспектив розвитку сонячної енергетики в Україні, а також обґрунтування необхідності державних управлінських заходів щодо впровадження сонячної енергії як альтернативного джерела. Це спрямовано на забезпечення стабільного прибутку та економічної безпеки країни. Для досягнення зазначеної мети були поставлені та вирішені такі завдання:

- розглянуто міжнародний досвід реалізації стратегій сонячної енергетики для сталого економічного розвитку;
- визначено можливості адаптації європейських і американських моделей застосування «зеленого» тарифу в умовах України;
- проведено аналіз витрат і результативності встановлення сонячних електростанцій на прикладі розрахунку такої системи для приватного будинку;
- обґрунтувано доцільність реалізації проєктів домашніх і промислових сонячних електростанцій на території України.

Об'єднання фотоелектричних сонячних панелей (PV) і вітрових турбін (WT) у єдину гібридну систему відновлюваної енергії є перспективним рішенням для забезпечення електроенергією як у мережевих, так і позамережевих умовах. Така система використовує переваги взаємодоповнюваності двох джерел енергії: сонячні панелі максимально ефективні у сонячні дні, коли вітер може бути слабким, а вітрові турбіни забезпечують генерацію енергії вночі чи у хмарні дні, коли продуктивність сонячних панелей знижується.

У автономних умовах комбінована система PV+WT забезпечує більш стабільне постачання енергії, ніж використання одного з джерел окремо. Для підвищення надійності системи часто додаються акумулятори або інші засоби зберігання енергії, що дозволяє накопичувати надлишкову енергію для її подальшого використання. Це особливо важливо у віддалених районах, де немає доступу до централізованої енергомережі. Крім того, системи управління енергією дозволяють оптимізувати роботу, перемикаючись між джерелами енергії та накопичувачами, що сприяє максимальній ефективності.

Незалежно від підключення до мережі чи роботи в автономному режимі, друга модель поєднує генерацію сонячної енергії з накопиченням у батареях (ВТ), забезпечуючи збалансований підхід до енергопостачання. У мережевому режимі батареї сприяють вирівнюванню пікових навантажень, тоді як в автономному режимі забезпечують стабільність енергопостачання у періоди відсутності сонячної енергії [3].

Різні дослідження описують універсальність системи PV + ВТ, підкреслюючи її здатність адаптуватися до різних енергетичних потреб. Накопичення енергії сприяє підвищенню стабільності, надійності та автономності відновлюваних енергетичних систем. Для моделювання роботи таких систем використовують рівняння, що описують баланс енергетичних потоків, перетворення потужності, стан заряду батареї та її взаємодію з мережею або навантаженням.

Така інтеграція зробила фотоелектричні системи з накопиченням енергії привабливими як для домовласників, так і для бізнесу. Лідером у впровадженні є Німеччина, яка збільшила свої потужності з 4500 МВт у 2015 році до 7500 МВт у 2022 році. Австралія слідує зростанням із 3800 МВт до 7000 МВт за той самий період. США та Японія також демонструють значний прогрес: США збільшили потужності з 2500 МВт до 5500 МВт, а Японія – з 2000 МВт до 3680 МВт. Китай, Південна Корея, Італія, Франція, Велика Британія та Іспанія також роблять свій внесок у глобальний перехід до відновлюваних джерел енергії, хоч і в менших масштабах.

Ці показники відображають посилення міжнародної прихильності до екологічно чистих, стійких енергетичних рішень, особливо в економічно розвинених країнах.

Однак для широкого впровадження таких систем в Україні необхідно вирішити проблеми, такі як економічна доцільність, політичні рамки та технологічний прогрес. Загалом, дані дослідження представляють всебічний інтерес та розуміння альтернативної енергетики, прокладаючи шлях для майбутніх досягнень у системах відновлюваної енергії та переходах до сталої енергетики.

1. Ardashir J. F., Ghadim H. V. (2021). A PV based multilevel inverter with ultra-capacitor bank for microgrid applications. 11th Smart Grid Conference (SGC) (P. 1-5). IEEE.
2. Li J. et al. (2019). Stratified optimization strategy used for restoration with photovoltaic-battery energy storage systems as black-start resources. IEEE Access, (7), 127339-127352.
3. Tostado-Véliz M., Icaza-Alvarez D., Jurado F. (2021). A novel methodology for optimal sizing photovoltaic-battery systems in smart homes considering grid outages and demand response. Renewable Energy, (170), 884-896.
4. Маляренко В. А., Галетич І. К., Вергелес Ю. І. (2012). Відновлювані джерела енергії для Харківської області: сучасний стан, тенденції, перспективи. Енергозбереження. Енергетика. Енергоаудит, (7), 36-43.

Д.В. Бондаренко

ЕЛЕКТРИЧНЕ МОДЕЛЮВАННЯ ФОТОЕЛЕКТРИЧНИХ ДЖЕРЕЛ ЕНЕРГІЇ ДЛЯ РОЗПОДІЛЕНИХ МЕРЕЖ

Одним із кроків забезпечення безпеки енергетики є впровадження розподілених енергетичних мереж з застосуванням розподіленої генерації. Розподілені енергетичні мережі, особливо які базуються на великій кількості невеликих мереж (мікромереж) потребують організації узгодженої роботи та інтелектуального керування [1]. Сучасні пристрої, які основані на мікропроцесорній та мікроконтролерній техніці можуть здійснювати керування з урахуванням результатів імітаційного моделювання, навіть в реальному часі. Крім того, моделювання є потужним інструментом дослідження, проектування та впровадження різноманітних технологічних рішень в енергетичних системах.

Сонячна енергетика, а саме фотоелектричні джерела електричної енергії є перспективним напрямком побудови розподілених енергетичних мереж. Зазначимо, що для впровадження мікромереж з фотоелектричними джерелами енергії необхідно проводити моделювання з урахуванням усіх можливих параметрів.

Основою моделювання фотоелектричних систем є побудова електричних моделей генеруючих пристроїв. Для побудови електричної моделі сонячного фотоелектричного елемента зручно використовувати принцип аналогій. Згідно такому принципу потоку фотонів, які падають на фотоелектричний перетворювач, відповідає електричний струм електричної моделі (I), а енергії фотона, який поглинається напівпровідниковою структурою – напруга електричної моделі (U):

$$\frac{ne}{t} \to I\,, \tag{1}$$

$$\frac{h\nu}{e} \to U\,, \tag{2}$$

де n – кількість фотонів, яка поглинута напівпровідником; e – елементарний заряд; h – постійна планка; ν – частота фотона; t - час.

Треба відмітити, що ключовим елементом такого представлення на основі аналогій є потужність. Як потужність електромагнітного випромінювання сонця, так і електрична потужність, яка отримується з фотоелектричного модуля. Акцентуємо, що використання потужності є одним з основних видів представлення енергетичних процесів. Бачимо що:

$$P = UI = \frac{h\nu}{e}\frac{ne}{t}. \tag{3}$$

Зазначимо, що вираз (3) описує не потужність сонячного випромінювання, яке падає на панель, а вихідну потужність пов’язану з

поглинанням фотонів, та не враховує втрати на поглинання без створення електронно-діркових пар, втрати на відбиття фотонів, втрати на рекомбінацію носіїв заряду та інші дисипативні процеси.

Таким чином, будуємо електричну модель (Рисунок 1), яка об'єднує джерело струму і джерело напруги.

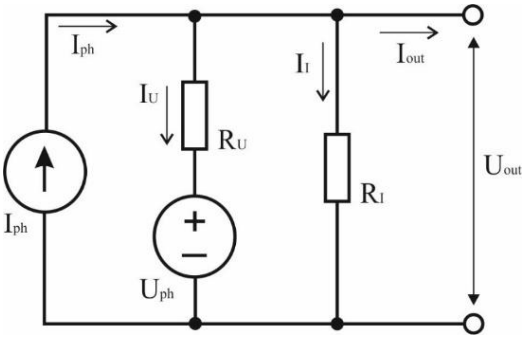


Рисунок 1 – Електрична модель фотоелектричного перетворювача

Вирази для струмів і напруг електричної моделі фотоелектричного джерела (Рисунок 1) мають вигляд:

$$I_{out} = I_{ph} + I_U + I_I , \quad (3)$$

$$U_{out} = U_{ph} + U_{Ru} , \quad (4)$$

$$U_{Ru} = I_U R_U , \quad (5)$$

де I_{ph} – струм процесу перетворення фотонів в носії заряду; I_I – струм внутрішнього опору джерела струму; I_U – струм джерела напруги; I_{out} – вихідний струм фотоелектричного джерела; R_U – внутрішній опір джерела струму; U_{ph} – напруга процесу перетворення фотонів в носії заряду; U_{Ru} – напруга на внутрішньому опорі джерела напруги; U_{out} – вихідна напруга фотоелектричного джерела.

Для подальшої побудови енергетичної системи також використовують електричну модель накопичувача, яким може бути або конденсатор, або іоністор [2], або електрохімічний акумулятор [3]. Крім того моделюється підключення навантаження.

Розподілена електрична мережа передбачає з'єднання генеруючих та зберігаючих пристроїв в мережу [4]. Електричні моделі дозволяють це робити, залучаючи в електричні кола моделей реальні електронні схеми готових пристроїв перетворення електричної енергії, таких як понижувальні чи підвищувальні перетворювачі, інвертори та конвертори.

В загальному розумінні, для утворення розподіленої мережі змінного струму з відокремлених фотоелектричних генераторів потрібно мати окрім фотоелектричних модулів (PV-module), ще й контролер заряду (MPPT-

control), вузол підвищення напруги (flyback converter), перетворювач з постійного струму в змінний (full bridge inverter) та модуль узгодження з мережею (grid control), так як такі параметри мережі, як амплітуда, частота та фаза, повинні бути узгоджені [5]. Таким чином система виглядає наступним чином (Рисунку 2):

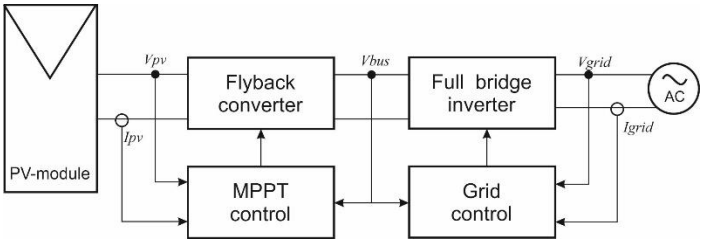


Рисунок 2 – Схема підключення фотоелектричного модуля до мережі

Отже резюмуємо, що цифрова трансформація нашої держави спонукає до використання передових технологій моделювання та сучасних керувальних систем, для реалізації потужної мережі розподіленої генерації на основі програмно керованих комплексів з застосуванням відновлюваних джерел енергії. А інструменти пов'язані з моделюванням можуть пришвидшити цей процес та застосувати ефективні рішення.

1. Bondarenko, D., Matiakh, S., Surzhyk, T., Sheiko, I., & Kravchenko M. (2024). Development trends of solar power engineering based on the materials of the scientific and practical conference "Renewable energy and energy efficiency in the 21 centuries". *Vidnovluvana Energetika*, 3(78), 76-83. https://doi.org/10.36296/1819-8058.2024.3(78).76-83.
2. Бондаренко, Д. Моделювання роботи фотоелементів з використанням іоністорів. (2020). *Відновлювана енергетика та енергоефективність у 21 столітті: Матеріали міжнародної науково-практичної конференції* (с. 288-292). Інститут відновлюваної енергетики НАН України.
3. Bondarenko, D. (2019). Equivalent circuits of electric power accumulators connected to solar photocell. *Vidnovluvana Energetika*, 3(58), 30-34. https://doi.org/10.36296/1819-8058.2019.3(58).30-34.
4. Bondarenko, D., Matyakh, S., Surzhyk, T., & Shevchuk, V. (2023). Energy unit kit for photovoltaic cluster. *Vidnovluvana Energetika*, 3(74), 53-58. https://doi.org/10.36296/1819-8058.2023.3(74).53-58 .
5. Bondarenko, D., & Matyakh, S. (2024). Using microinverters for photovoltaic cluster. *Vidnovluvana Energetika*, 1(76), 51-56. https://doi.org/10.36296/1819-8058.2024.1(76).51-56.

O.M. Dzhyhun

MODERN TRENDS IN THE DEVELOPMENT OF THE ENERGY SYSTEM OF UKRAINE

The electric power industry of Ukraine is the basic sector of the state economy and actually one of the oldest. The generation of electrical resources is based on nuclear energy, hydropower, the processes of burning fuel oil and coal, biofuel and natural gas. In addition., Ukraine already uses renewable sources such as solar energy, wind turbines and water stations. The sector is a priority for the state and forms a significant share of the national economy.

Russian aggression has had a significant impact on Ukraine's energy infrastructure. In the first year of the full-scale war alone, Ukraine lost about 44% of its nuclear generation, 25% of its renewable energy capacity, and 29% of its hydroelectric and pumped storage facilities. Thermal generation suffered the largest losses – about 65% [1]. Hostile attacks on energy facilities have caused widespread destruction, leading to power outages across the country. There is no place, no region, no type of energy infrastructure that will not be affected by these attacks. The total loss of our capacity as a result of this year's attacks, which began on March 22, exceeds 9 GW. 18 GW of generation is occupied, including HPP, TPP and the largest nuclear power plant in Europe - Zaporizhzhya NPP. Restoration of the damaged infrastructure is a priority.

The energy sector 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 in connection with the departure of the population and the termination 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. Ukraine's obtaining the status of a candidate for joining the EU poses additional challenges for the energy industry and the regulation of this industry.

One of the most severe consequences for the economy of Ukraine during the war is the results of massive attacks by Russian forces on the power system, therefore, the study of the state of this area after the criminal attacks and the measures taken by the Ukrainian government to counteract the consequences of the damage is an important and topical task. As a result of the Russian attacks on the Ukrainian electricity system, there was a significant decrease in the use of electricity by at least 50%. Enemy forces captured a certain part of the enterprises

that produced electricity, and quite a large part of the power generating capacities were completely destroyed. Most coal-fired thermal power plants (CHPs) and thermal power plants (TPPs) were shut down because many coal-fired enterprises were located in the occupied territory. All these circumstances have a destructive effect on the economy of Ukraine, which leads to a decrease in the gross domestic product and an increase in the level of poverty among the Ukrainian population. Ukraine faces problems not only in guaranteeing national security in the conditions of war with Russia, but also in the ability to ensure stable operation of the electric power sector in conditions of military aggression [2]

The rapid development of alternative energy – electricity generation from renewable energy sources (RES) has been observed throughout the world in recent years. According to current legislation, renewable energy sources include solar, wind, geothermal, hydrothermal, aerothermal energy, wave and tidal energy, hydropower, biomass energy, gas from organic waste, gas from sewage treatment plants, biogas, and secondary energy resources, to which include blast furnace and coke gases, methane gas from degassing of coal deposits, transformation of the waste energy potential of technological processes.Among the alternative fuels, an important group of solid fuels derived from municipal solid waste, in particular, recovered RDF, should be separately highlighted. The production and use of solid waste fuels in the energy sector can partially replace fossil fuels that are in short supply in Ukraine. The potential for RDF production is about 3 million tons. The energy use of such fuels can generate 3000-3500 million kWh of heat annually. The potential for replacing natural gas is about 1 billion m3, and coal – 2 million tons [3].

Among all global trends in the development and use of energy, among the key priorities for Ukraine are: rational use of energy; increasing energy efficiency and social responsibility in this area; reduction of CO2 emissions; implementation of digital technologies in the process of strategically important types of energy production; expanding the use of renewable energy sources [4].

Modern trends in the development of the energy system of Ukraine have the following features:

• Consistent increase in environmental requirements for traditional, coal-fired power plants. However, it should be noted that these power plants currently carry the main burden of daily power regulation in the power system.

•. The improvement of technical and economic indicators of various technologies for the production of electricity from RES, primarily from solar and wind energy, and the presence of state support for the development of these technologies led to a rapid increase in their installed capacity and a radical change in the structure of production capacity in European countries.

•. A feature of Ukraine's energy system is the significant scale of nuclear energy development. According to their technological properties, Ukrainian nuclear power plants cannot participate in daily load regulation.

The increase in the total share of electricity production from renewable

energy sources and nuclear power plants in the energy system of Ukrain e leads to a significant limitation of the possibilities of power regulation in the energy system and requires the reconfiguration of electric networks.

Guaranteeing energy security is a component of the problem of ensuring the national security of each country, on which its socio-economic stability and defense capability depend.In the conditions of russia's armed aggression against Ukraine, ensuring energy security becomes an important object of state policy. This requires constant and well-coordinated management in order to ensure the energy independence of the country and the reliable operation of the infrastructure, which directly affects the functioning of the economy and the lives of citizens, the study of changes in the energy markets of Ukraine and Europe, which from the point of view of economic, social and energy integration with the EU is quite urgent task.

1. Чернявський, М. В. Теплові електростанції як елементи системи регулювання режимів енергосистеми України: За матеріалами доповіді на засіданні Президії НАН України 21 лютого 2024 року. Visnik Nacional NoiAcademiiNaukUkrai Ni, 2024, 4, с.45–57. https://doi.org/10.15407/visn2024.04.045.
2. https://economyandsociety.in.ua/index.php/journal/article/view/2556.
3. Гапонич Л. С., Топал О. І., Голенко І. Л., Кобзар С. Г. Визначення потенціалу виробництва RDF для заміщення викопних палив в енергетиці України. Збірник матеріалів І Міжнародної науково-практичної конференції «Подолання екологічних ризиків та загроз для довкілля в умовах надзвичайних ситуацій – 2022», (26–27 травня 2022 року, Полтава – Львів). Полтава: НУПП, 2022. С. 173–176. https://nupp.edu.ua/uploads/files/0/events/conf/2022/i-mnpk-podolannia-eko-rizikiv/zbirnik-materialiv.pdf.
4. https://jrnl.knutd.edu.ua/index.php/bknutde/article/view/568.

E.P. Kholiavka, Yu.V. Parfenenko

DECISION SUPPORT SUBSYSTEM FOR MANAGING ENERGY MICROGRIDS IN RESOURCE-CONSTRAINED CONDITIONS

The purpose of the information system for assessing the state of energy microgrids is to ensure their autonomous operation and stability in isolated conditions. Microgrids, consisting of distributed energy resources (DERs) and energy storage systems (ESS), require effective management to maintain frequency stability, especially during power shortages. In such cases, network unloading (load shedding) is used, which can be viewed through the lens of bankruptcy problems, ensuring a fair distribution of limited resources among consumers using different allocation rules, such as constrained equal awards (CEA) and constrained equal losses (CEL) [1].

The system places particular emphasis on forming stable microgrids after extreme events, particularly in emergency situations. A proactive approach to network operation, including topology optimization and preparation for potential accidents, minimizes energy losses and ensures a reliable power supply to critical loads [2]. An important aspect involves accounting for the capacity of power lines when forming a microgrid, which contributes to frequency stabilization and reduces energy losses.

The system aims to enhance the stability of microgrids by minimizing the number of load shedding events and improving energy flow management after emergency situations [1, 2]. Through proactive planning and management, a balance between supply and demand is achieved, ensuring efficient system operation in extreme conditions and enhancing its resilience and survivability in complex scenarios.

Decision-making for the effective management of microgrids during energy resource shortages is based on innovative approaches to load management and ensuring stable microgrid operation in isolated modes. Special attention is given to managing distributed energy resources (DERs) and energy storage systems (ESS), which stabilize system operation during periods of energy shortages [1]. A key component of this process is the mechanism for reducing the load by optimizing the distribution of limited resources.

To ensure the stability of microgrids, effective tools are required for analyzing and managing their operation under dynamic conditions. An essential element of such an approach is monitoring and forecasting the state of the network, enabling the timely detection of potential issues and quick responses to emergency situations [3]. Accordingly, the availability of accurate historical data, combined with the ability to automate decisions on energy flow redistribution, helps minimize the number of emergency or planned load shedding events, thereby increasing the system's stability.

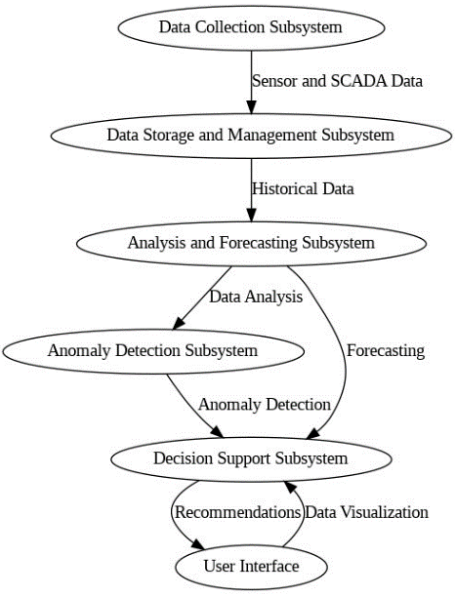


Figure 1 – Architecture of the information system for assessing the state of microgrids

The presented block diagram illustrates the architecture of the information system for assessing the state of microgrids (Fig. 1), which consists of several key subsystems.

The first subsystem is the data collection subsystem. Its main function is data collection from sensors and SCADA systems [4]. This data contains information about the state of microgrid elements, for example, voltage, current, load and other parameters.

The next part is the data storage and management subsystem, which is responsible for storing the collected data, forming a database of historical data and providing quick access for further analysis. Historical data is critical for the next stages of system operation.

The third element is the analysis and forecasting subsystem, which analyzes stored data to identify trends and patterns in the operation of microgrids. In addition, it can predict potential deviations from normal operation based on historical data.

The fourth component is the anomaly detection subsystem, the task of which is to detect anomalies in the operation of microgrids, which may indicate possible emergency situations or deviations from standard operating modes. Anomalies are detected using data analysis.

The decision support subsystem is used to make recommendations for further actions for network operators or automated control systems. It processes information about detected anomalies and predicts possible accidents, offering optimal strategies to maintain network stability.

The final element is a user interface that provides visualization of data and recommendations, allowing microgrid operators to receive all the information they need in a convenient format. This allows you to quickly react to current events and make informed decisions regarding the management of energy flows.

Predicting equipment failures is critical to maintaining stable and reliable operation of microgrids. One of the main tasks is to predict the residual useful life (RUL) of microgrid components.

Formula intensity deviation:

$$T_i = \frac{1}{\lambda_i} \tag{1}$$

where $\lambda_i$is the intensity of deviation i- and the component is the main one for estimates of the remaining service life. It allows you to determine exactly when a failure may occur, which helps to plan maintenance and avoid unforeseen failures.

Risk assessment is important to understand the potential consequences of equipment failure. In microgrids, the risks of failure include not only financial losses, but also potential power outages, which can negatively impact the grid as a whole

Risk assessment formula:

$$R_i = P_i \cdot C_i, \tag{2}$$

where P_i is the probability of failure, which can be estimated by the remaining service life:

$$P_i = 1 - e^{-\lambda_i t}, \tag{3}$$

where C_i is the cost or rejection of the negative impact. This formula helps determine which components have the highest risk of failure and, accordingly, which components should be focused on for preventive measures.

In resource-constrained microgrids, optimizing maintenance costs and risk management is critical. A mathematical model for resource optimization may include:

$$C_{total} = \sum_{i=1}^{n}(U_i \cdot x_i + R_i), \tag{4}$$

where U_i— maintenance costs of the ith $i$component; x_i-is a binary variable indicating whether the service was performed. The objective is to minimize the total cost while ensuring that the probability of failure for all components remains below an acceptable level.

This model helps strike a balance between maintenance costs and failure risks, which is critical for the efficiency and reliability of microgrid systems.

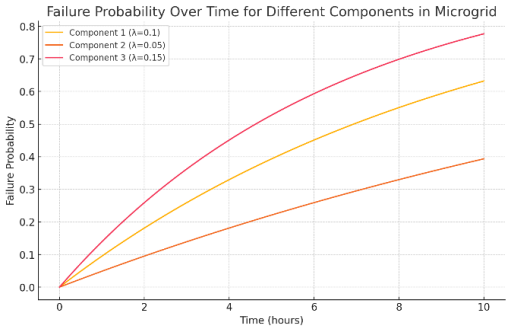


Figure 2 – Failure probabilities of three-component microgrids

Figure 2 presents the failure probability of three microgrid components over time. Each line corresponds to a component with a different failure intensity (λ): component 1 has the highest intensity (λ = 0.15), component 2 has a medium intensity (λ = 0.1), and component 3 has the lowest intensity (λ = 0.05). This model allows us to estimate how the probability of failure of individual components increases over time.

The results of the study show that effective management of the microgrid is possible thanks to the use of innovative approaches to the distribution of limited energy resources, in particular through the mechanism of load shedding. This mechanism optimizes energy distribution during shortages, ensuring stable operation of the system. A proactive approach to microgrid management has demonstrated a 15% reduction in load shedding compared to traditional methods, helping to increase system resilience after emergencies.

1. HM Kim, T. Kinoshita, Y. Lim, and TH Kim, "A bankruptcy problem approach to load-shedding in multiagent-based microgrid operation," *Sensors*, vol. 10, no. 10, pp. 8888–8898, Sep. 2010. [Online]. Available: https://doi.org/10.3390/s101008888
2. H. Haggi, W. Sun, JM Fenton, and P. Brooker, "Proactive rolling-horizon-based scheduling of hydrogen systems for resilient power grids," *IEEE Transactions on Industry Applications*, vol. 58, no. 2, pp. 1737–1746, Mar.–Apr. 2022. [Online]. Available: https://doi.org/10.1109/TIA.2022.3146848 .
3. D. Miao and S. Hossain, "Improved gray wolf optimization algorithm for solving placement and sizing of electrical energy storage system in micro-grids," *ISA Transactions*, vol. 102, pp. 376–387, Jul. 2020. [Online]. Available: https://doi.org/10.1016/j.isatra.2020.02.016 .
4. S. Li, B. Jiang, X. Wang, and L. Dong, "Research and application of a SCADA system for a microgrid," *Technologies*, vol. 5, no. 2, p. 12, Mar. 2017. [Online]. Available: https://doi.org/10.3390/technologies5020012 .
5. MY Arafat, MJ Hossain, and MM Alam, "Machine learning scopes on microgrid predictive maintenance: potential frameworks, challenges, and prospects," *Renewable and Sustainable Energy Reviews*, vol. 190, p. 114088, Feb. 2024. [Online]. Available: https://doi.org/10.1016/j.rser.2023.114088 .

М.Л. Дранік

ОСОБЛИВОСТІ ВСТАНОВЛЕННЯ ТЕПЛОВИХ НАСОСІВ У ЗАКЛАДАХ СОЦІАЛЬНОЇ ІНФРАСТРУКТУРИ ДЛЯ ЗАБЕЗПЕЧЕННЯ СТАЛОГО ЕНЕРГОПОСТАЧАННЯ

1. Вступ

Заклади соціальної інфраструктури, такі як лікарні, школи та дитячі садки, споживають значну кількість енергії для опалення, охолодження та гарячого водопостачання. У сучасних умовах енергетичної нестабільності важливою стає модернізація таких закладів із впровадженням енергоефективних технологій.

Україна є імпортером енергоресурсів, тому її енергетична політика, цілі та механізми реалізації останньої не можуть бути подібними до пріоритетів політики країн – виробників енергоресурсів. Україна має забезпечити імпорт необхідних обсягів енергоресурсів зі світових ринків, виграючи цінову конкуренцію за ресурси в інших країн-споживачів, що можливо лише за високої конкурентоспроможності національної економіки на світових ринках.[1].

За даними Київської школи економіки, з лютого 2022 року по травень 2024 року було пошкоджено або зруйновано загалом 18 великих ТЕЦ, а також 815 котелень, 152 центральних теплових пунктів і 354 кілометри труб теплопостачання. Прямі збитки в результаті цих атак (без урахування соціальних та економічних витрат) оцінюються в 2,4 мільярда доларів США, причому більше половини припадає на атаки на ТЕЦ. [2]

Міжнародна енергетична агенція розробила план дій для подолання енергетичної кризи в Україні. Одним з пунктів плану вони пропонують негайно запровадити енергозберігаючі заходи для підвищення енергетичної безпеки та теплового комфорту. Існують швидкі та недорогі дії, які можуть підвищити ефективність житлових будинків, на які припадає близько третини загального кінцевого споживання енергії в країні.[3]

Використання теплових насосів (ТН) є одним із найбільш ефективних рішень для забезпечення сталого енергопостачання, дозволяючи скоротити витрати на енергію, зменшити навантаження на енергетичну мережу, зменшити залежність від викопного палива та знизити викиди парникових газів.

2. Технологічні рішення для підвищення ефективності теплових насосів (ТН) у закладах соціальної інфраструктури

Теплові насоси можуть значно покращити енергоефективність, якщо їх інтегрувати з відповідними технологіями та правильно адаптувати до особливостей об’єкта. Нижче описані ключові технологічні рішення, які забезпечують оптимальну роботу теплових насосів у закладах соціальної інфраструктури.

2.1. Використання буферних ємностей. Буферні ємності (теплові акумулятори) є важливим компонентом у системах з тепловими насосами, особливо для закладів з непостійним графіком споживання теплової енергії.

Призначення:

- Накопичення тепла: зберігають надлишкову теплову енергію, вироблену ТН під час низького споживання.
- Стабілізація системи: запобігають частому включенню та виключенню компресора, що продовжує термін служби обладнання.
- Покриття пікових навантажень: забезпечують теплом у години підвищеного споживання, коли ТН працює на максимальній потужності.

Технічна реалізація:

- Резервуари зі спеціальними теплоізоляційними матеріалами, об'ємом від 200 до 2000 літрів (залежно від масштабу об'єкта).
- Установлення датчиків температури для автоматичного управління зарядом і розрядом ємності.

Приклад використання:

У школі тепловий насос нагріває воду в буферній ємності вночі, використовуючи дешеву електроенергію за нічним тарифом. Удень ця гаряча вода використовується для опалення або ГВП.

2.2. Інтеграція з системами управління енергоспоживанням (EMS)

Системи енергоменеджменту (Energy Management Systems) координують роботу ТН, оптимізуючи споживання енергії на основі даних про споживання, температуру та умови зовнішнього середовища

Можливості EMS:

- Оптимізація роботи ТН: керує його роботою в залежності від прогнозованого попиту та доступної енергії.
- Прогнозування енергоспоживання: використовує дані історії енергоспоживання та погодні умови для ефективного планування.
- Інтеграція з іншими джерелами енергії: забезпечує ефективну роботу ТН у поєднанні з сонячними панелями чи акумуляторами.
- Моніторинг і звітність: дає змогу відстежувати ефективність системи через веб-інтерфейс або мобільний додаток.

Приклад використання:

У лікарні EMS аналізує пікові години споживання тепла й налаштовує роботу ТН, забезпечуючи мінімальне споживання енергії вночі й оптимальне використання енергії вдень.

2.3. Рекуперація тепла. Рекуперація дозволяє використовувати теплову енергію, що втрачається в процесах вентиляції або охолодження, для додаткового підігріву теплоносія.

Призначення:

- Підвищення ККД системи: повернення частини енергії, яка інакше була б втрачена.

- Зменшення енергоспоживання: зниження навантаження на ТН, оскільки частина тепла надходить із систем рекуперації.

Технічна реалізація:

- Установлення пластинчастих або роторних теплообмінників у системах вентиляції.

- Інтеграція рекуператорів із тепловим насосом для підігріву води чи повітря в системах опалення.

Приклад використання:

У дитячому садку тепло з вентиляційної системи використовується для попереднього нагріву води для опалення, що скорочує витрати на електроенергію.

2.4. Використання комбінованих систем. Теплові насоси можуть бути інтегровані з іншими джерелами енергії, такими як сонячні панелі, для підвищення загальної ефективності системи.

Комбінація ТН і сонячних панелей:

- Електроживлення: сонячні панелі забезпечують енергію для роботи ТН.
- Теплова підтримка: за допомогою сонячних колекторів можна підігрівати воду, зменшуючи навантаження на ТН.

Технічна реалізація:

- Інтеграція ТН із фотоелектричними панелями через EMS.

- Використання інверторів для конвертації енергії сонячних панелей для живлення компресорів ТН.

Приклад використання:

У школі сонячні панелі вдень живлять ТН, який нагріває воду в буферній ємності для використання вночі.

2.5. Інтелектуальні теплові насоси. Нові моделі ТН оснащені вбудованими інтелектуальними алгоритмами, які адаптують їхню роботу залежно від умов.

Можливості:

- Самонавчання: система аналізує історію роботи та адаптується для підвищення ефективності.

- Взаємодія з мережею: інтелектуальні ТН можуть працювати в системах "розумної мережі" (Smart Grid), забезпечуючи балансування енергоспоживання.

Приклад використання:

Інтелектуальний ТН автоматично переходить на роботу від акумулятора в години пікових тарифів і повертається до стандартного режиму в період низьких тарифів.

3. Виклики впровадження

3.1. Фінансові бар'єр. Необхідність високих початкових інвестицій може стримувати впровадження, що вимагає державної підтримки.

3.2. Брак обізнаності. Керівники закладів соціальної інфраструктури часто не мають достатньої інформації про можливості ТН.

3.3. Потреба у кваліфікованих спеціалістах. Якісне проєктування та монтаж є ключовими для забезпечення ефективності системи.

4. Висновки

Дослідники в США підрахували, що в національному масштабі для їхньої країни, теплові насоси скоротять енергоспоживання домашнього домогосподарства в середньому на 31% до 47% залежно від рівня ефективності та на 41% до 52% у поєднанні з модернізацією будівлі, наприклад з кращою ізоляцією. Теплові насоси скоротять викиди парникових газів у житловому секторі на 36–64%, включаючи викиди від нового виробництва електроенергії. Ці ж дані можуть бути актуальними і для України.[4]

Інтеграція теплових насосів в існуючі системи опалення на основі газових або твердопаливних котлів дозволяє значно підвищити енергоефективність, зменшити витрати на енергі, навантаження на енергетичну мережу та покращити екологічні показники. Правильний вибір методу інтеграції залежить від специфіки об'єкта, кліматичних умов, доступності відновлюваних джерел енергії та фінансових можливостей.

1. Енергетична безпека України: методологія системного аналізу та стратегічного планування: аналіт. Е61 доп. / [Суходоля О. М., Харазішвілі Ю. М., Бобро Д. Г., Сменковський А. Ю., Рябцев Г. Л., Завгородня С. П.]; за заг. ред. О. М. Суходолі. – Київ: НІСД, 2020. – 178 с. https://niss.gov.ua/sites/default/files/2020-12/sukhodolia_energy_security_sayt-1.pdf.
2. Київська школа економіки: Оцінка прямих збитків та непрямих втрат енергетичного сектору України внаслідок повномасштабного вторгнення росії., травень 2024 р., URL: https://kse.ua/ua/about-the-school/news/zbitki-ta-vtrati-energetichnogo-sektoru-ukrayini-vnaslidok-povnomasshtabnogo-vtorgnennya-rosiyi-perevishhili-56-mlrd-otsinka-kse-institute-stanom-na-traven-2024-roku/.
3. «Ukraine's Energy Security and the Coming Winter», International Energy Agency, September 2024, URL: https://iea.blob.core.windows.net/assets/cec49dc2-7d04-442f-92aa-54c18e6f51d6/UkrainesEnergySecurityandtheComingWinter.pdf.
4. News Release: Benefits of Heat Pumps Detailed in New NREL Report. Feb. 12, 2024. https://www.nrel.gov/news/press/2024/benefits-of-heat-pumps-detailed-in-new-nrel-report.html.

В.О. Ходаківський, Д.С. Карпенко

ОЦІНЮВАННЯ РІВНЯ ЕФЕКТИВНОСТІ ВПРОВАДЖЕННЯ МІНІ-ТЕЦ ДЛЯ РЕЗЕРВУВАННЯ СИСТЕМИ ЕЛЕКТРО- І ТЕПЛОПОСТАЧАННЯ

Дослідження спрямоване на оцінку ефективності виробництва теплової та електричної енергії на основі різних технологій, таких як котельні, когенераційні установки та міні-ТЕЦ (ОРС-цикл). Особлива увага приділяється порівнянню з існуючими автономними та індивідуальними системами енергозабезпечення. Для оцінки використовуються методологічні підходи, які враховують економічну доцільність та технічну ефективність кожної технології. Також аналізує впровадження когенерації та Power-to-Heat технологій для оптимізації роботи централізованих систем теплопостачання, що підвищить загальну ефективність. Запропоновано шляхи пошуку інвестицій, враховано вплив на ефективність теплових та електричних мереж, зниження викидів вуглецю та оптимізацію витрат.

Матеріал і результати досліджень економічної ефективності різних видів теплопостачання для опалення включає оцінку споживання теплової енергії, собівартості виробництва та впливу на довкілля. Метою є визначення ефективності виробництва теплової й електричної енергії з використанням котелень, міні-ТЕЦ, когенераційних установок, а також автономних і індивідуальних систем. Методологія враховує вплив технологій на енергоефективність централізованого опалення та аналізує можливості модернізації для інтеграції інновацій, зокрема когенераційних систем, із акцентом на зниження викидів та економічну доцільність.

Розрахунки для визначення вартості 1 Гкал теплоти, оцінка економічності різних джерел енергії, зокрема кількість палива, електроенергії для виробництва теплової енергії розглянуто в [1-3].

Методика та приклади розрахунку, що описані в [1]:

Витрата палива за певний термін часу – $\tau_{розр}$ на одержання від джерела теплопостачання відповідної кількості теплової енергії визначається за формулою:

$$B_\tau = \frac{Q_\tau \times 10^6}{\eta_\tau^{Дж} \times Q_н^р} \quad (1)$$

де B_τ - витрата палива (природній/біо- газ (м³) або тверде/біо- паливо (кг); Q_τ - потужність ТЕЦ (ГВт), $\eta_\tau^{Дж}$ - ККД теплогенератора (%); $Q_н^р$ - теплотворна здатність палива (природній/біо- газ (кДж/м³) або тверде/біо- паливо (кДж/кг).

Витрата електричної енергії (electrical energy – EE) визначається за формулою еквіваленту електроенергії і теплоти:

$$W_\tau = \frac{Q_\tau \times 10^6}{860 \times \eta_\tau^{e.агр}} \quad (2)$$

де: 10^6 – співвідношення між “ккал” теплоти і “Гкал”; 860 – співвідношення між “кВт.год” і “ккал”: (1 квт.год = 860 ккал); $\eta_\tau^{e.агр}$ – тепловий ККД електричного егрегату (теплої підлоги, тепловентилятора, тощо), що генерує теплоту, використовуючи електричну енергію.

Загальна вартість теплової енергії з природного газу (natural gas – NG) визначається за формулою:

$$(CV_{he})^{NG} = B_t \times C_{NG} \quad (3)$$

де: $(CV_{he})^{NG}$ - загальна вартість теплової енергії з NG (грн); C_{NG} — ціна NG (грн/м³).

Загальна вартість теплової енергії з біопалива (biofuel – BF) визначається за формулою:

$$(CV_{he})^{BF} = B_t \times C_{BF} \quad (4)$$

Загальна вартість теплової енергії з ЕЕ обчислюється за формулою:

$$(CV_{he})^{EE} = W_\tau \times C_{EE} \quad (5)$$

де: $(CV_{he})^{EE}$ - загальна вартість теплової енергії з ЕЕ (грн); C_{EE} — вартість ЕЕ спожитої агрегатом перетворювачем, (грн/(кВт·год).

В той же час для вибору кількості CHP згідно USAID для покриття теплового навантаження міста або району використовують формулу [2]:

$$n = \frac{k \cdot Q}{Q_{КГУ}}, \quad (6)$$

де n – обрана кількість КГУ; k – поправочний коефіцієнт на використання пікового водогрійного котла (k ≈ 0,85÷0,95); $Q_{КГУ}$ – встановлена теплова потужність прийнятої когенераційної установки, кВт. Необхідна кількість CHP становить 2 або більше і обирається таким чином, щоб забезпечити максимальне число годин використання встановленої потужності.

Витрата палива за певний термін часу – $\tau_{розр}$ на одержання від когенераційної установки відповідної кількості теплової енергії визначається за формулою:

$$B_\tau^{КГУ} = \frac{B_{КГУ}}{Q_{КГУ}} \quad (7)$$

де $B_{КГУ}$ - годинна витрата NG когенераційною установкою згідно з паспортними даними на установку, м3 /год;

Загальна вартість теплової енергії з когенерації визначається за формулою:

$$(\mathrm{CV}_{he})^{\mathrm{КГУ}} = B_{\tau}^{\mathrm{КГУ}} \times C_{NG} \quad (8)$$

де: $(\mathrm{CV}_{he})^{NG}$ - загальна вартість теплової енергії з когенерації (грн); C_{NG} — ціна NG (грн/м³).

При розрахунку парціанальних витрат палива виробництві теплової енергії на ТЕЦ або когенерації можна використовувати:

$$B_{\mathrm{E}}^{\mathrm{КГУ}} = B_{\mathrm{E}}^{*} - m_E \times \Delta B \quad (9)$$

$$B_{H}^{\mathrm{КГУ}} = B_{H}^{*} - m_H \times \Delta B, \quad (10)$$

де B_{E}^{*}- порціальна витрата палива на виробництво електроенергії; B_{H}^{*}- порціальна витрата палива на виробництво теплоти; ΔB – економія палива; m_E – коєфіцієнт віднесення економії палива на виробництво електроенергії; m_H – коєфіцієнт віднесення економії палива на виробництво теплоти.

Наведені залежності дають можливість зрозуміти прямі витрати на вироблення теплової енергії з різних технологій [1-6].

Для оцінки доцільності різних систем DH з урахуванням сучасних викликів, наслідків війни та процесів відновлення, слід брати до уваги експлуатаційні витрати, енергетичні, екологічні та економічні вимоги, безпеку, обслуговування, а також інтереси споживачів, постачальників і держави. Основними вимогами для міст є:

- Скорочення енергоспоживання без втрати комфорту;
- Зменшення впливу на довкілля та викидів парникових газів;
- Оптимізація економічних витрат;
- Забезпечення безпеки теплопостачання;
- Якісне обслуговування теплових і електричних систем.

Цей підхід поєднує екологічні, економічні та соціальні аспекти в розвитку DH. Модернізація ЦТ із впровадженням газових і біогазових CHP, міні-ТЕЦ (ОРС) на деревній щепі дозволяє ефективно поєднувати виробництво теплової та електричної енергії, що є актуальним для регіонів із високим попитом на енергоносії, як у Бурштині. В останні десятиліття місцеві влади багатьох українських міст, таких як Івано-Франківськ, рекомендують перехід на індивідуальне опалення. Аналогічний процес триває у місті Бурштин, яке поступово переходить на локальні системи, навіть маючи поблизу ТЕЦ.

У результаті дослідження підтверджено, що інтеграція когенераційних технологій та міні-ТЕЦ на їх базі в DH суттєво підвищує ефективність, зменшує викиди та поліпшує стабільність енергопостачання в Україні.

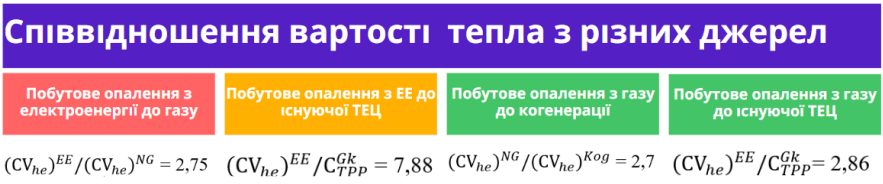


Рисунок 1 - Співвідношення вартості тепла з різних джерел

В Україні собівартість опалення електричними котлами залишається високою, особливо з огляду на зростання цін на електроенергію. Газові котли є вдвічі дорожчими від міні-ТЕЦ та когенераційних установок. Важливо зберегти цілісність і модернізувати тепломережі для зниження втрат, що наразі перевищують нормативні 12% [7-8].

1. Філоненко В.М. Когенерація // УДК 621.1/.3. URL: https://dspace.nuft.edu.ua/server/api/core/bitstreams/8461ff89-1307-4582-ab6b-a07b2e5ac58c/content.
2. USAID Проєкт енергетичної безпеки (ПЕБ) у співпраці з Мінрегіоном. Керівництво з розробки схем теплопостачання. URL: https://energysecurityua.org/ua/zvity.
3. Маляренко В. А., Шубенко О. Л., Андрєєв С. Ю., Бабак М. Ю., Сенецький О. В. Когенераційні технології в малій енергетиці: монографія. Харків: ХНУМГ ім. О. М. Бекетова, 2018. 454 с. ISBN 978-966-695-448-3. URL: https://core.ac.uk/download/pdf/162019489.pdf.
4. Song, W. H., Wang, Y., Gillich, A., Ford, A., Hewitt, M. Modelling development and analysis on the Balanced Energy Networks (BEN) in London // Applied Energy. 2019. №233–234. С. 114–125. DOI:10.1016/j.apenergy.2018.10.054.
5. Karpenko D., Yevtukhova T. O. MARKET FEATURES OF HEAT PRODUCERS CONTRIBUTION TO LOSSES IN DISTRICT HEATING SYSTEM NETWORKS // General Energy Institute of NAS of Ukraine. 2024. DOI: 10.32782/2663-5941/2024.3.1/37.
6. Babak V., Kulyk M. Increasing the efficiency and security of Integrated Power System operation through heat supply electrification in Ukraine // Science and Innovation. 2023. Т. 19, №5. С. 100–116. DOI: 10.15407/scine19.05.100.
7. Національна комісія, що здійснює державне регулювання у сферах енергетики та комунальних послуг. URL: https://www.nerc.gov.ua/news/nkrekp-sproshchuye-umovi-dlya-roboti-kogeneracijnih-ustanovok-yaki-vikoristovuyutsya-v-yakosti-rezervnogo-dzherela-energiyi-dlya-obyektiv-kritichnoyi-infrastrukturi.
8. Кабінет Міністрів України. Постанова від 15.12.2023 №1320. URL: https://zakon.rada.gov.ua/laws/show/1320-2023-%D0%BF#Text.

М.С. Дунаєвський, С.Б. Сулейманов

АРХІТЕКТУРА ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ЕНЕРГЕТИЧНОГО СЕКТОРУ УКРАЇНИ

Вступ. Цифровізація енергетичного сектору на сьогодні є фундаментальним інфраструктурним фактором стимулювання економічного зростання, впровадження інноваційних рішень, створення нових робочих місць, підтримки конкурентоспроможності, відкритості до міжнародних ринків та сумісності з ними задля успішної інтеграції та кооперації [1]. В цей же час, процеси цифрової трансформації пов'язані з викликами щодо забезпечення кібербезпеки, захисту даних та конфіденційності, адміністрування доступу до даних, зростання енергоспоживання ІКТ сектору.

Мета та завдання. Метою цієї роботи є дослідити сучасні кращі практики та стратегії цифрової трансформації енергетичного сектору Європи та тезисно сформувати архітектуру такої трансформації для України.

Виклад основного матеріалу. Насамперед зазначимо, що стратегія цифровізації ЄС (DDPP 2030) [1, 2] здійснюється в рамках Європейського зеленого курсу (European Green Deal). Україна підтримує такий підхід та впроваджує принципи сталого розвитку, зокрема відводить все більшу роль використанню відновлювальних джерел енергії.

Загалом, архітектурно можемо визначити чотири системні рівні цифрової трансформації. Рівень фізичної інфраструктури, який представлений такими об'єктами як електростанції (звичні та на основі відновлювальних джерел енергії), електромережі, пристрої інтернету речей (Internet of Things). Рівень інформаційно-цифрової інфраструктури, представлений автоматичними системами контролю та збору даних (SCADA), хмарними платформами (cloud platform), системами підтримки прийняття рішень на основі технологій штучного та генеративного інтелекту (AI & GenAI), системами накопичення та збереження великих за обсягом та слабоструктурованих даних (Big Data, Data Lake). Рівень операційної методології та управління з відповідними засобами управління електромережею, платформами для здійснення ринкових угод, інструментарієм прогнозування та моделювання. Рівень законодавчо-нормативного регулювання (національні закони щодо регулювання енергоринку, протоколи ЄС, протоколи кібербезпеки, екологічні нормативи). Кожному рівню відповідають визначені трансформаційні процеси та поставлені цільові значення ключових показників успішності (KPI) цифрової модернізації (табл. 1) [1]. Також, є ряд інноваційних технологічних рішень та ініціатив, які сприяють досягненню поставлених орієнтирів. Таким чином запропонована концептуальна архітектура трансформації визначена структурно та з причинно-наслідковими зв'язками між її компонентами. Для орієнтиру наведено значення ключових показників та основні заходи

цифровізації Європи за програмою DDPP 2030 [1]. Зауважимо, що ініціативи спрямовані не тільки на підвищення доступності, а й на підвищення навиків користування сучасними технологіями (фактор людського капіталу не менш важливий ніж фактор фізичної інфраструктури). Орієнтуючись на Європейський ринок маємо орієнтуватися і на ці показники, хоча, перед Україною насамперед буде ще виклик повноцінного відновлення енергетичної інфраструктури, зруйнованої та пошкодженої рашистами.

Таблиця 1 – Структура цифрової трансформації енергетичного сектору

Системний рівень	**Технологічні рішення**	**Ключові показники та заходи DDPP 2030 [1]**
Законодавчо-нормативне регулювання	Електронні державні послуги	Ключові громадські сервіси 100% доступні онлайн для громадян (в тому числі eHealth) та бізнесу 100% громадян мають цифровий підпис (digital ID)
Операційна методологія та управління	Цифрові двійники (Digital Twins) Однорангова торгівля та місцеві енергетичні ринки	Мінімум 80% населення володіють базовими цифровими навиками Мінімум 90% малого та середнього бізнесу використовують цифрові технології базового рівня 20 млн. працевлаштованих ІКТ фахівців
Інформаційно-цифрова інфраструктура	Хмарні платформи (cloud platform) AI для енергоефективних дата центрів	75% компаній використовують Cloud AI та Big Data Гігабітні інтернет мережі Зростання кількості технологічних «компаній-єдинорогів» Квантові обчислення
Фізична інфраструктура	Енергоефективні мережі (Sustainable Networks) Power over Enthernet (PoE)	Покриття 5G Оптоволокно до будинку (FTTP) Подвоєння обсягу виробництва напівпровідників Встановлення 10000 екологічно нейтральних крайових вузлів (edge nodes)

Україна гармонізує законодавче регулювання енергоринку у відповідності до стандартів ЄС, включаючи лібералізацію ринку електроенергії та пріоритизацію розвитку альтернативних джерел енергії. Значним успіхом України на шляху до енергетичної інтеграції з країнами ЄС стало об'єднання її енергосистеми з європейською системою ENTSO-E в

березні 2022 року. Варто зауважити, що на території Румунії значні обсяги електроенергії, згенерованої з відновлювальних джерел, накопичуються в регіоні Добруджа. Їх не так просто експортувати. Відповідно, приєднання Української енергосистеми до ENTSO-E має потенціал розв'язати цю проблему, і в той же час забезпечити Україну екологічною енергією [3].

Загалом, програмою DDPP 2030 передбачено зниження викидів парникових газів на 55% та досягнення 45% частки відновлювальних джерел енергії [1]. Енергетична система повинна бути досить інтелектуальною, динамічною та інтерактивною для підтримки таких змін. Збільшення частки відновлювальних джерел енергії означає більш децентралізовану та більш гнучку систему в якій крім традиційних джерел енергії сотні тисяч сонячних панелей, вітрових турбін та загалом малих електростанцій (а також енергоакумулюючих батарей). Задля успішного управління такою системою в режимі реального часу й необхідне активне впровадження сенсорів (IoT) та сучасних 5G мереж, що передаватимуть потокові дані від них до (хмарних) центрів управління, реалізуючи моніторингово-управлінську концепцію системи цифрових двійників (Digital Twins). Варто зауважити що мережа нового покоління 5G надає не тільки кращі технологічні переваги (наприклад в рази чи навіть десятки раз вищу пропускну здатність), але й є менш енерговитратними. Так, спільне дослідження Ericsson та Vodafone вказує на зниження енергоспоживання сучасним поколінням 5G до 55% [4]. Цифрова хмарна платформа дозволяє в реальному часі відслідковувати стан балансу на ринку (виробництво/споживання електроенергії) та підтримувати укладення відповідних угод між ключовими учасниками ринку [5]. Малі електростанції потенційно додають енергосистемі децентралізованості, а отже і підвищеної стійкості. Інвестиційні проекти щодо їх побудови можуть бути потенційно цікавими територіальним громадам, які мають недовикористаний фактор капіталу чи праці [6].

Не варто забувати, що швидка цифровізація енергетичної системи також підвищує ризики кібератак, – відповідно виникає необхідність в механізмах захисту даних та алгоритмів функціонування системи [2]. Кібербезпека має вирішальне значення при модернізації енергомережі, оскільки забезпечує її надійну, стійку та ефективну роботу [7]. Потрібні інвестиції у формування кібербезпекових спроможностей та професійний розвиток для підвищення стійкості критичних енергетичних систем до кіберзагроз. До прикладу, в ЄС зауважують необхідність цільового виділення діапазонів частот 400 та 450 МГц саме задля безпечного спеціалізованого зв'язку регіонального чи національного рівня [2]. Саме такі нижні діапазони частот найкраще відповідають потребам критично важливих комунікацій. Відповідна інфраструктура забезпечує роботу, управління та контроль мереж критичного значення з належним рівнем системної стійкості та захищеності. Практично виключена ймовірність підключення до мережі неавторизованих пристроїв. Впроваджуються механізми моніторингу та попередження перевантаження

мереж в надзвичайних ситуаціях. Зауважимо, що більшість мереж зв'язку є публічними, та не створені для підтримки критичних цифрових додатків, однак це не заважає використати їх для некритичних застосувань як от надсилання загальних моніторингових даних. Технології сегментації пропускної здатності мережі дозволяють виділити частину потужностей на пріоритетне обслуговування інформаційно-комунікаційних запитів енергетичних мереж. Загалом, для успішної цифрової трансформації енергетичного сектору потрібна якісна співпраця уряду, приватного сектору, освітніх установ, активна залученість громадян.

Висновки. Сучасні, кращі практики та стратегії цифрової трансформації енергосектору Європи насамперед орієнтовані на екологічність, модернізацію інфраструктури, підвищення залученості громадян та бізнесу до новітніх технологій, побудову інтелектуальних інформаційних систем управління, створення електронних сервісів для покращення рівня комфорту життя. На ці практики варто орієнтуватись й Україні. Одночасно з відновленням енергетичної інфраструктури намагатись (де можливо) модернізувати її на основі високотехнологічних рішень на всіх системних рівнях, інвестувати в професійний кадровий склад та найкращі підходи управління в цифрову еру.

1. Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030 (2022) https://eur-lex.europa.eu/eli/dec/2022/2481/oj.
2. DigitalEurope. DIGITALEUROPE's roadmap for Europe's energy ecosystem digital transformation – The time to transform is now. (2023) https://cdn.digitaleurope.org/uploads/2023/06/DIGITALEUROPEs-roadmap-for-Europes-energy-ecosystem-digital-transformation.pdf.
3. Sabadus A. (2023, 19th of December). Wartime Ukraine's European energy integration continues. *Atlantic Council*. https://www.atlanticcouncil.org/blogs/ukrainealert/wartime-ukraines-european-energy-integration-continues/.
4. Ericsson, Vodafone. Powering network efficiency: Showing how embracing sustainability doesn't mean sacrificing performance (2021) https://www.ericsson.com/4ae1be/assets/local/about-ericsson/sustainability-and-corporate-responsibility/environment/07122021-ericsson-vodafone-4page-web_fin.pdf.
5. Gaivoronski A., Gorbachuk V., Dunaievskyi M., Suleimanov S.-B. (2022) Digital platforms to close the information asymmetry gaps. *Problems of Control and Informatics*. № 6. 67–82.
6. Дунаєвський М.С. (2019) Економічне зростання суміжних районів за децентралізації. *Теорія оптимальних рішень*, №18. 94-99.
7. Горбачук В.М., Лупей М.І., Дунаєвський М.С. (2022) Підходи до резильєнтності критичних інфраструктур. *Science and education for sustainable development*. A.Ostenda, V.Smachylo (eds.). Poland: University of Technology, Katowice. 87–95. DOI:10.54264/M005
http://www.wydawnictwo.wst.pl/uploads/files/6ea021fc2983bafe60afd42fd5d707a2.pdf

A. Davidenko, V. Lubin

OPTIMIZATION OF ENERGY-EFFICIENT OBJECT RECOGNITION ALGORITHM FOR THE K510 CHIP

Spiking Neural Networks (SNNs) represent a novel approach in artificial neural networks, inspired by the biological processes of the human brain. Unlike traditional artificial neural networks (ANNs) that rely on continuous signal processing, SNNs operate on discrete events called "spikes". However, training SNNs poses several challenges, such as achieving stability and performance while handling temporal consistency. Researchers are addressing these challenges by developing strategies to improve the temporal consistency of spikes and enhancing the overall stability of the networks. Energy-efficient object recognition models like Spiking-YOLO also face integration challenges. One major issue is optimizing these models to maintain high performance while reducing energy consumption. To address this, the integration of modules such as RepNIBMS, which replaces traditional components like the C2f module in feature extraction networks, has shown promise. This module is designed to process objects of varying scales while retaining useful information, thereby optimizing performance during both training and inference. Moreover, multi-scale feature fusion modules like WFPN enhance the model's ability to identify small objects, which are typically difficult to detect due to their size and subtle features. In terms of hardware optimization, the Kendryte K510 chip, a RISC-V based edge AI chip, has demonstrated significant improvements in energy efficiency for object recognition tasks. This chip employs original data flow computing technology, enhancing computing power by approximately three times compared to its predecessors, while maintaining a high level of customization and flexibility for various applications such as UAV high-definition aerial photography and robotics. Furthermore, analog AI chips present a promising solution for reducing power consumption during AI tasks. These chips combine computation and memory storage within the same unit, mimicking the human brain's efficiency and significantly reducing energy usage compared to traditional digital processors. IBM's latest analog AI chip, for instance, offers GPU-level performance for AI inference tasks while markedly improving power efficiency by eliminating the need for constant data movement between memory and processing units.

Training Spiking Neural Networks (SNNs) presents several significant challenges, primarily due to their unique operational mechanism that relies on discrete events or "spikes" rather than continuous signal processing. One of the primary challenges is the difficulty in designing efficient learning algorithms that can effectively handle the temporal dynamics of spikes. Unlike traditional artificial neural networks (ANNs) that use gradient-based learning methods, SNNs require specialized techniques to manage the timing and order of spikes, making the training process more complex and computationally intensive. Another major

challenge is the issue of stability and performance in SNNs. The temporal consistency of spike patterns is crucial for the reliable operation of SNNs. To address this, researchers have focused on enhancing temporal consistency, which improves both the stability and performance of the networks. Additionally, knowledge transfer strategies have been developed to improve the performance of SNNs by leveraging pre-trained models from the static domain, thereby facilitating more efficient training and better accuracy in the event domain.

Integrating energy-efficient object recognition models like Spiking-YOLO into existing systems presents several challenges that need to be addressed to ensure effective deployment and performance. One significant challenge is the optimization of computational resources while maintaining high performance. The integration of Spiking Neural Networks (SNNs), which are inherently different from traditional Artificial Neural Networks (ANNs), necessitates significant modifications in both hardware and software architectures to leverage their energy efficiency fully. The development and deployment of these models require robust support for various scales and types of objects. For instance, the RepNIBMS module, designed to replace the C2f module in the YOLOv8n feature extraction network, improves the processing of objects of varying scales while retaining critical information. This optimization reduces memory usage and increases inference speed, which is crucial for energy efficiency. Additionally, the WFPN cross-level multi-scale feature fusion module addresses the challenges of detecting small objects by expanding the neck component to accommodate supplementary feature maps, thus enhancing small object detection capabilities. Moreover, the adoption of analog AI chips has shown promising results in reducing power consumption. IBM's recent analog AI chip, for instance, offers significant energy efficiency improvements over traditional GPUs. These chips can compute and store memory in the same location, mimicking brain functions and reducing data movement between memory and processing units, thereby lowering power usage and increasing computational speed. This contrasts with current digital chips like the Kendryte K510, which, despite being optimized for edge AI tasks, still consume substantial power due to constant data movement. Finally, the shift towards analog AI chips like those being developed by Sageance highlights the potential for further energy savings. These chips promise to run large models like Llama 2-70B at a fraction of the power required by traditional systems, emphasizing the importance of innovative chip architectures in addressing the power consumption challenges posed by large-scale AI models. Such advancements are crucial as the demand for energy-efficient AI solutions continues to grow.

Spiking Convolutional Tracking Networks (SCTN) leverage data from event cameras to enhance object tracking through the integration of energy-efficient deep convolutional spiking neural networks. These networks process visual information in a manner analogous to the human brain, leading to significant improvements in

both energy efficiency and processing speed. Event cameras capture changes in the scene at a very high temporal resolution, which allows SCTNs to operate efficiently by processing only the salient information necessary for object tracking, thus minimizing redundant computations and reducing energy consumption. In the context of Unmanned Aerial Vehicles (UAVs), edge-based energy-efficient object detection systems, such as E-UAV, have been developed to address the energy consumption challenges inherent in UAV-based object detection tasks. These systems balance various aspects, including computational load and energy use, to design practical solutions that enhance operational efficiency. The Kendryte K510 chip further exemplifies advancements in energy-efficient processing for real-time object recognition tasks. This RISC-V based edge AI chip incorporates original data flow computing technology, which optimizes memory access patterns and significantly reduces latency and energy consumption. The Kendryte K510's high computational power, coupled with its energy efficiency, makes it suitable for a range of applications including UAV high-definition aerial photography, robotics, and smart city projects. Its deployment in smart cities has notably reduced operational costs and improved response times in real-time surveillance systems.

1. Kendryte Datasheet. Canaan Inc. [Electronic resource]. – Access mode: https://github.com/kendryte/k510_docs.

О.В. Васильєв, В.В. Чьочь

ОСНОВНІ РИСИ ПУБЛІКАЦІЙНОГО ТА ПАТЕНТНОГО ЛАНДШАФТУ ПРОБЛЕМИ «АТАКИ НУЛЬОВОГО ДНЯ

Атаки нульового дня належать до найбільш небезпечних інцидентів кібербезпеки, що зачіпають як звичайних користувачів, так і корпоративні мережі. У 2021 році кількість таких атак досягла рекордного рівня. Це дослідження спрямоване на аналіз сучасного стану, уточнення поняття атак нульового дня та детальне вивчення цього явища. Загрози такого типу, часто уникають традиційних антивірусних систем. Такі кібератаки можуть серйозно порушити діяльність компаній, призводячи до втрати часу, фінансових збитків або витоку конфіденційної інформації. Через свою природу антивірусні рішення, які базуються на сигнатурах, не здатні зупинити невідомі загрози.

На основі масиву науково-технічних публікацій (результату інформаційного пошуку у БД SCOPUS за допомогою пошукової формули TITLE-ABS-KEY ("Zero-Day Vulnerability")) обсяг якого складає 343 документів на кінець листопада 2024 року був проведений контент аналіз і кластеризація тематики вибраних документів. Хронологічний діапазон публікацій складає майже 23 років, але значне зростання їх кількості спостерігається починаючи з 2018 року. В інтервалі 2017 -2023 року темпи такого зростання збільшилися на 20 відсотків.

Додатково були знайдені та проаналізовані опубліковані патенти за допомогою патентної пошукової системи PatBase та проведений патентний аналіз. Документальний масив був визначений за допомогою пошукової формули - DSC=("Zero-Day Vulnerability") і його розмір склав 179 патентних сімейств (1726 окремих патентів у різних країнах та міжнародних заявок). Патентування починається у 2004 році, а значне зростання щорічної кількості патентів починається з 2013 року (що демонструє «промислову придатність рішень цієї проблеми).Динаміка патентування демонструє стабільне зростання з 2013 року на 15% щорічно.

По результатах проведених досліджень наукових та патентоздатних рішення (патентів та наукових публікацій) можливо визначити декілька ключових трендів еволюції даної проблеми :

1. . **Збільшення кількості виявлених вразливостей [1-2]:**

• У 2021 році було зафіксовано 57 випадків використання вразливостей нульового дня, що майже вдвічі більше порівняно з попереднім роком.

• У 2023 році кількість таких вразливостей зросла до 87, порівняно з 52 у 2022 році, що свідчить про активізацію зловмисників у використанні цих вразливостей.

2. **Розширення цілей атак (по матеріалах бібліографічних та патентних досліджень):**

• Зловмисники все частіше спрямовують атаки на критичну інфраструктуру, включаючи енергетичні системи, телекомунікації та транспорт.

• Збільшується кількість атак на популярні програмні продукти, такі як веб-браузери (наприклад, Google Chrome) та платформи для відеоконференцій (наприклад, Zoom).

3. **Ускладнення методів атак (по матеріалах бібліографічних та патентних досліджень):**

• Зловмисники використовують складніші техніки для виявлення та експлуатації вразливостей, що ускладнює їх виявлення та нейтралізацію.

• Зростає використання автоматизованих інструментів для пошуку вразливостей у популярних програмних продуктах.

4. **Збільшення ринку вразливостей нульового дня [1]:**

• Існує чорний ринок, де хакери продають виявлені вразливості, а зловмисники купують їх для проведення кібератак.

• Деякі брокери купують дослідження вразливостей нульового дня від імені своїх клієнтів, зберігаючи анонімність покупців та продавців.

5. **Недостатня ефективність традиційних засобів захисту [3]:**

• Традиційні рішення безпеки, такі як системи виявлення вторгнень (IDS) та антивірусні програми, часто не здатні ефективно протидіяти атакам нульового дня через їхню новизну та непередбачуваність.

6. **Підвищення уваги до вразливостей у популярних платформах:**

• У 2021 році Google Chrome зіткнувся із серією загроз нульового дня, що призвело до активного випуску оновлень для усунення цих вразливостей.

• Платформи для відеоконференцій, такі як Zoom, також стали об’єктами атак нульового дня, що вимагало швидкого реагування та випуску патчів.

Ці тенденції підкреслюють необхідність постійного вдосконалення засобів кіберзахисту та підвищення обізнаності про потенційні загрози серед користувачів і організацій.

1. Zero day: що таке вразливість нульового дня? .- Електронний ресурс: https://itedu.center/ua/blog/articles/zero-day/?utm_source=chatgpt.com.
2. Основні тенденції у кібербезпеці на 2024 рік: які виклики стоять перед бізнесом / Володимир Боянжи .- Електронний ресурс: https://www.issp.ua/post/main-cybersecurity-trends-in-2024?utm_source=chatgpt.com.
3. Зростання вразливостей нульового дня .- Електронний ресурс: https://www.oksim.ua/2024/10/15/zrostannya-vrazlivostej-nulovogo-dnya/?utm_source=chatgpt.com.

О.В. Васильєв, В.В. Васильєв, В.В. Чьочь, С.Я. Гільгурт

АПАРАТНА РЕАЛІЗАЦІЯ НА ПЛІС СИСТЕМ ДРОБОВОГО ПОРЯДКУ

Технічні системи, в яких здійснюються обчислення дробового порядку, тобто виконуються операції диференціювання та інтегрування нецілої кратності, можуть використовуватися для вирішення широкого кола прикладних задач від ефективного стиснення інформації та виділення корисного сигналу на тлі перешкод до ідентифікації параметрів динамічних систем [1]. Якщо йдеться про автономні застосування, наприклад, мобільні пристрої або безпілотні апарати, обладнання яких обмежено за продуктивністю, програмна реалізація на традиційних процесорах відносно складних розрахунків, притаманних обчисленням дробового порядку, стає викликом. Прийнятною платформою виявляються програмовані логічні інтегральні схеми (ПЛІС), які поєднують в собі швидкодію спеціалізованих процесорів з гнучкістю, майже як у програмних рішень, при помірному енергоспоживанні.

З кількох відомих операторів дробового порядку для апаратної реалізації у вигляді типового диференціатора/інтегратора найчастіше використовують формулу Грюнвальда–Летнікова [2]:

$$ {}_{a}^{GL}D_t^q x(t) = \lim_{h\to 0} \frac{1}{h^q} \sum_{j=0}^{\lfloor (t-a)/h \rfloor} w_j^{(q)} x(t - jh) \qquad (1) $$

$$ w_0^{(q)} = 1,\ w_j^{(q)} = \left(1 - \frac{q+1}{j}\right) w_{j-1}^{(q)} ,\ \text{j} = 1, 2, 3 \qquad (2) $$

де $w_j^{(q)}$ – біноміальні коефіцієнти, h – розмір кроку, q – дробовий порядок.

Вивчення літератури свідчить про велику кількість розробок, присвячених побудові цифрових схем обчислення оператора. Узагальнена структура дробового оператора Грюнвальда–Летнікова, запропонована в одній з останніх робіт в цьому напряму [2], базується на підході, при якому використовується фіксоване вікно, що дозволяє здійснювати на апаратному пристрої операції як диференціювання, так і інтегратора [3].

Розглянемо в якості прикладу структуру реалізації подібної схеми на ПЛІС, наведену у [2]. Схема складається з Головного модуля, що реалізує власне принцип фіксованого вікна, Генератора біноміальних коефіцієнтів та Генератора степеневої функції (рис. 1).

Головний модуль здійснює додавання за формулою (1), в якій задіяні значення степеневої функції h^q і біноміальних коефіцієнтів $w_j^{(q)}$ для такого

ж розміру вікна, який використовується для генерації коефіцієнтів. Вхідний сигнал має 32-бітну розрядність та інтерпретується як число з фіксованою комою, що має цілу частину розміром 8 бітів та дробову частину довжиною 24 біти. Вихідні дані також мають розрядність 32 біти.

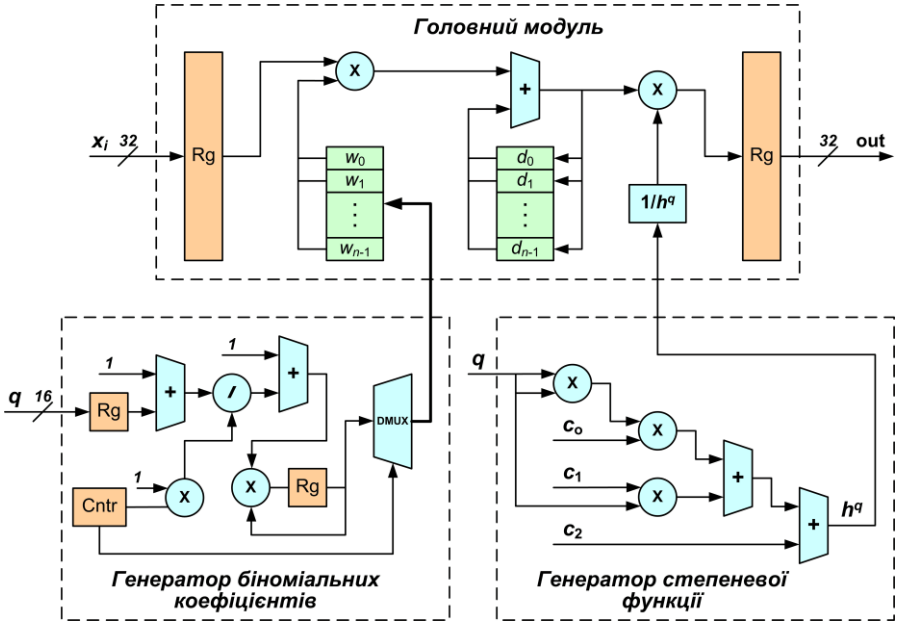


Рисунок 1 – Реалізація на ПЛІС оператора Грюнвальда–Летнікова згідно [2]

Біноміальні коефіцієнти розраховується за формулою (2), використовуючи змінну q як вхідне значення. Ця змінна зберігається в регістрі та має формат з фіксованою комою, що має цілу частину розміром 4 біти та дробову частину довжиною 12 бітів. Обчислення здійснюються ітераційно для значень $j = 1, 2, 3 \ldots L$, де L – розмір цільового вікна, що в данному прикладі може сягати значення 1024.

Генерація степеневої функції h^q здійснюється шляхом квадратичної апроксимації. В зв'язку з тим, що вихідне значення h^q при цьому змінюється дуже швидко, для підвищення точності апроксимації діапазон зміни її аргументу q розбивається на піддіапазони, для кожного з яких використовується свій власний набір коефіцієнтів квадратичної апроксимації c_0, c_1 і c_2. Рекомендації щодо оптимального розбиття на піддиапазони в сенсі підвищення точності та зниження апаратних витрат можна знайти, наприклад, в роботах [4] та [5]. Опубліковані в [2] результати свідчать, що

відносна похибка апаратної реалізації за такою схемою не перевершує 4 % для всього діапазону зміни q.

Тестування на базі ПЛІС XC7A100T сімейства Artix-7 від Xilinx показало, що максимальна відносна похибка, яка була отримана для режиму диференціювання, дорівнює 5% для цільового вікна розміром $L = 1024$ та 22% для $L = 32$. Режим інтегрування показав набагато гірші максимальні значення відносних похибок: 140% та 170% відповідно [2]. Слід зауважити, що, наприклад, в роботі [6] були отримані схожі результати.

Отже, розглянутий приклад підтверджує життєздатність ідеї створення відносно універсальних диференційних/інтегруючих схем дробового порядку на базі ПЛІС. Огляд літературних джерел свідчить, що розробники подібних систем найчастіше використовують оператор Грюнвальда–Летнікова. Такі пристрої можуть використовуватися для вирішення різних технічних задач – від оцінювання сигналів та їх похідних довільного порядку до створення схем динамічного шифрування.

Практичне застосування схем дробового порядку на базі ПЛІС можливо при створенні керуючих пристроїв мобільних та безпілотних систем з низьким енергоспоживанням та широкими функціональними можливостями.

1. Васильев В. В., Симак Л. А., Васильев А. В. Обработка сигналов и моделирование динамических систем дробного порядка на основе операционного исчисления аппроксимационного типа. *Електронне моделювання*. 2016. Том. 38, № 4. С. 13-34. URL: https://doi.org/10.15407/emodel.38.04.013.
2. A unified FPGA realization for fractional-order integrator and differentiator / M. S. Monir et al. *Electronics*. 2022. Vol. 11, no. 13:2052. URL: https://doi.org/10.3390/electronics11132052.
3. FPGA implementation of two fractional order chaotic systems / M. F. Tolba et al. AEU - *International journal of electronics and communications*. 2017. Vol. 78. P. 162–172. URL: https://doi.org/10.1016/j.aeue.2017.04.028.
4. FPGA implementation of the fractional order integrator/differentiator: two approaches and applications / M. F. Tolba et al. *IEEE transactions on circuits and systems I: regular papers*. 2019. Vol. 66, no. 4. P. 1484–1495. URL: https://doi.org/10.1109/tcsi.2018.2885013.
5. Reconfigurable FPGA realization of fractional-order chaotic systems / S. M. Mohamed et al. *IEEE access*. 2021. Vol. 9. P. 89376–89389. URL: https://doi.org/10.1109/ access.2021.3090336.
6. Fractional order integrator/differentiator: FPGA implementation and FOPID controller application / M. F. Tolba et al. *AEU - international journal of electronics and communications*. 2019. Vol. 98. P. 220–229. URL: https://doi.org/10.1016/j.aeue.2018.10.007.

Т.Г. Голоцукова, П.В. Ламонов

ЦИФРОВЕ ПІДПРИЄМСТВО ТА ЦИФРОВІ ДВІЙНИКИ: ВИКЛИКИ ТА МОЖЛИВОСТІ ІНТЕГРАЦІЇ

У сучасному світі цифровізація стає ключовим фактором конкурентоспроможності [1, с. 31]. Підприємства прагнуть досягти більшої економії витрат, конкурентних переваг і оптимізації операційної діяльності. У міру освоєння технологій організації відчувають зростаючу потребу в нових технологічних рішеннях, що іноді призводить до прискореного їх прийняття. Це явище сприяє виникненню *«цифрового розриву»*, оскільки різні організації засвоюють нові технології з різною швидкістю. Така технологічна нерівність впливає на конкурентну динаміку ринку, надаючи переваги для тих підприємств, які досягають операційної вигоди завдяки впровадженню інновацій, та створюючи труднощі для тих, хто ще не адаптувався до змін [2].

За Кеннетом С. Лаудоном цифрове підприємство (ЦП) – це організація, яка функціонує через цифрові мережі та використовує технології та інформаційні системи для підтримки основних бізнес-процесів, таких як управління ланцюгами постачання, відносинами з клієнтами, планування ресурсів підприємства та інших [3, с. 41]. Інформаційні системи відкривають можливості для децентралізації операцій, прискорення виходу на ринок, покращення взаємодії з клієнтами та підвищення ефективності в різних бізнес-функціях. Така цифровізація бізнес-процесів створює динамічні інформаційні системи, які підвищують продуктивність і сприяють ефективному управлінню організацією.

Цифровізація бізнес-функцій і послуг відкриває можливості для:

- безперервного функціонування бізнесу («Time Shifting»);
- роботи на глобальному ринку («Space Shifting») [3, с. 42];
- адаптації бізнес-стратегій до ринкових потреб;
- підвищення ефективності управління запасами та ланцюгами постачання [4];
- збільшення організаційної продуктивності;
- створення цінності для бізнесу через інвестиції в технології;
- покращення управління відносинами з клієнтами [3, с. 41].

Наприклад, системи бізнес-аналітики в реальному часі забезпечують стратегічну платформу для прийняття рішень, аналізуючи операційні події в момент їхнього виникнення. Вони зазвичай взаємодіють із системами управління ризиками, дозволяючи організації відстежувати продуктивність діяльності і оцінювати можливі загрози [5].

Цифрові двійники (Digital Twins) стали ключовим елементом в еволюції ЦП, дозволяючи організаціям створювати точні віртуальні копії реальних об'єктів або процесів для їх моніторингу, аналізу і оптимізації. Вони надають

підприємствам можливість працювати з великими обсягами даних в реальному часі, прогнозувати майбутні результати і приймати обґрунтовані рішення, що значно підвищує ефективність і конкурентоспроможність бізнесу [6].

Можливості використання цифрових двійників (ЦД):

1. *Оптимізація операційних процесів.* Однією з основних переваг ЦД є можливість моніторингу і оптимізації бізнес-процесів у реальному часі. Завдяки інтеграції з технологіями Інтернету речей, великих даних та штучного інтелекту (ШІ), ЦД допомагають підприємствам приймати ефективні рішення щодо виробництва, логістики, управління запасами та технічного обслуговування. Вони здатні виявляти потенційні проблеми до їх виникнення, що знижує ризики і витрати, пов'язані з аваріями або поломками [7]. Наприклад, завдяки зібраній інформації з ЦД керуюче програмне забезпечення може приймати рішення без втручання людини в режимі реального часу [8].

2. *Інновації та адаптація до змін.* ЦД сприяють інноваціям в бізнесі. Вони дозволяють підприємствам створювати віртуальні моделі продуктів, послуг або виробничих ліній, що дає змогу швидко тестувати нові ідеї і оцінювати їх ефективність ще до того, як вони будуть впроваджені на практиці. Завдяки цим моделям можна адаптувати бізнес до змін на ринку або в технологічному середовищі, що сприяє постійному розвитку і адаптації до нових умов [6].

3. *Прогнозування та стратегічне планування.* Застосування ЦД дозволяє підприємствам проводити точне прогнозування результатів і планувати дії в довгостроковій перспективі. Вони здатні виявляти зміни в умовах роботи і надавати рекомендації щодо оптимізації стратегій в реальному часі. Це допомагає підприємствам швидко реагувати на зовнішні і внутрішні виклики [7].

Проте, попри переваг, впровадження ЦД також має певні виклики:

1. *Складність інтеграції з існуючими системами.* Одним з найбільших викликів є інтеграція ЦД в уже існуючі інфраструктури підприємств. Це потребує значних інвестицій у модернізацію обладнання, оновлення програмного забезпечення та інтеграцію з іншими технологіями, що може бути складним і витратним процесом. Додатково, необхідність збору і обробки величезних обсягів даних може вимагати значних обчислювальних потужностей і ресурсів для підтримки належної роботи системи.

2. *Безпека даних.* ЦД опираються на великі масиви даних, і забезпечення їх безпеки стає критично важливим. У випадку порушення безпеки або витоку даних підприємства можуть зазнати значних фінансових та репутаційних втрат. Необхідність розробки надійних механізмів для захисту даних і забезпечення їх конфіденційності є ключовим викликом при впровадженні технології [9].

3. *Кваліфікація кадрів.* Щоб ефективно використовувати ЦД, підприємствам необхідно мати висококваліфікованих фахівців, здатних працювати з новими технологіями. Це включає не тільки фахівців з даних і аналітики, але й тих, хто володіє знаннями в області IT, Інтернету речей та ШІ. Однак на ринку праці ще недостатньо кадрів, що володіють потрібними навичками, що ускладнює впровадження цієї технології.

Виокремимо такі основні етапи створення ЦД:

1. *Формулювання мети та очікуваного результату.* Чітке визначення, які завдання вирішуватиме ЦД, та ключових результатів, які потрібно отримати.

2. *Аналіз об'єкта моделювання.* Визначення основних параметрів, сил і факторів, які впливають на об'єкт або процес. Формулювання припущень для спрощення моделі.

3. *Розробка математичної моделі.* Запис рівнянь, що описують фізичні, хімічні, біологічні чи інші процеси, пов'язані з об'єктом. Уточнення вихідних даних та обмежень [10].

4. *Апроксимація та дискретизація.* Складання наближених рівнянь для комп'ютерної реалізації. Вибір чисельних методів для розв'язання рівнянь.

5. *Проєктування програмної архітектури.* Розробка структури програмного забезпечення, вибір платформ, бібліотек і мов програмування.

6. *Реалізація ЦД.* Написання коду, інтеграція алгоритмів і моделей у програму. Перевірка сумісності різних компонентів.

7. *Проведення обчислювальних експериментів.* Тестування роботи ЦД на основі модельних або реальних даних. Порівняння результатів моделювання з реальними характеристиками об'єкта.

8. *Валідація та калібрування моделі.* Внесення коректив у модель для досягнення максимальної точності.

9. *Оптимізація та адаптація.* Повторне тестування до стабільної роботи ЦД у реальних умовах.

10. *Впровадження та інтеграція.* Використання ЦД для моніторингу, прогнозування, оптимізації або автоматизації роботи реального об'єкта.

11. *Забезпечення оновлення моделі в реальному часі.*

Цифрові двійники продовжують розвиватися і впроваджуватися в різних галузях, включаючи виробництво, містобудування, охорону здоров'я, енергетику і транспорт [7]. Також ЦД застосовують в секторі торгівлі для моделювання та покращення клієнтського досвіду [8]. У майбутньому їх використання буде сприяти більш тісній інтеграції з іншими цифровими технологіями, такими як 5G, блокчейн і автономні системи. З розвитком цих технологій ЦД стануть ще більш ефективними, дозволяючи підприємствам не тільки адаптуватися до змін, а й передбачати майбутні події, що дасть їм значну перевагу на ринку.

Отже, хоча впровадження цифрових двійників в цифрові підприємства супроводжується певними викликами, їх можливості значно перевищують ризики. Технології постійно вдосконалюються, і вже зараз можна стверджувати, що цифрові двійники є важливим інструментом для побудови успішних цифрових підприємств.

1. Ковбасюк, Ю., Грицяк, Н., & Семенченко, А. (Ред.). (2014). Електронне урядування. НАДУ.
2. Єрмоленко, О., Власенко, Т., & Шаповалова, І. (2023). Наслідки цифрового розриву та шляхи його подолання. Modeling the development of the economic systems, (1), 79–84. https://doi.org/10.31891/mdes/2023-7-11.
3. Laudon, K. C., Laudon, J. P. (2009). Management Information Systems: Managing the Digital Firm (11 ed.). Prentice Hall/CourseSmart.
4. Bartel, A., Ichniowski, C., & Shaw, K. (2007). How Does Information Technology Affect Productivity? Plant-Level Comparisons of Product Innovation, Process Improvement, and Worker Skills. The Quarterly Journal of Economics, 122(4), 1721–1758. https://doi.org/10.1162/qjec.2007.122.4.1721.
5. Azvine, B., Cui, Z., Nauck, D., & Majeed, B. (2006). Real Time Business Intelligence for the Adaptive Enterprise. The 8th IEEE International Conference on E-Commerce Technology and the 3rd IEEE International Conference on Enterprise Computing, E-Commerce, and E-Services (CEC/EEE'06). 29. DOI:10.1109/CEC-EEE.2006.73.
6. Haag, S., Anderl, R. (2018). Digital twin – Proof of concept. Manufacturing Letters, 15, 64-66. https://doi.org/10.1016/j.mfglet.2018.02.006.
7. What is a digital twin? (б. д.). IBM. Взято 27 листопада 2024 з https://www.ibm.com/topics/what-is-a-digital-twin.
8. Chen, Y., Weiming, Sh., & Xianbin, W. (2018). The Internet of Things in Manufacturing: Key Issues and Potential Applications. IEEE Systems, Man, and Cybernetics Magazine, 4(1), 6-15. DOI:10.1109/MSMC.2017.2702391.
9. Шевченко, Л. (2024, 7 жовтня). Цифрові двійники – новий етап ШІ: що це таке, як працюють і чим допоможуть людині. 24 Канал. Взято 27 листопада 2024 з https://24tv.ua/tsifrovi-dviyniki-shho-tse-take-yak-pratsyuye-yaka-korist-dlya_n2657188.
10. Digital Twins. (б. д.). IT-Enterprise. Взято 27 листопада 2024 з https://www.it.ua/knowledge-base/technology-innovation/cifrovoj-dvojnik-digital-twin .

В.М. Горбачук, Г.В. Голоцуков, Д.І. Ніколенко, В.В. Годлюк, Д.О. Рибачок

ПОСЛУГИ З ПОГЛЯДУ ЦИФРОВОГО ДЕСЯТИЛІТТЯ

Технологічні зміни створили і продовжують формувати сучасну енергетику, електрифікацію, інформатизацію, цифровізацію, а також нові проблеми та відповіді на них [1]. Послуги стають ближчими до споживачів.

Програма політики ЄС Цифрового десятиліття (Digital decade, DD) передбачає, серед іншого, конкурентний, суверенний і резильєнтний ЄС на основі свого технологічного лідерства [2], підтримку цифрових екосистем ЄС загалом і розширення масштабів інноваційних підприємств. Кардинальні моменти та цілі DD: цифровізація бізнесу (хмара/ШІ/великі дані (аналітика даних), цифрова інтенсивність МСП, єдинороги/стартапи). Цілі DD:

розбудова взаємопов'язаних цифрових екосистем (розробка комплексної та самопідтримуваної екосистеми інтероперабельної цифрової інфраструктури, де високопродуктивні, периферійні, хмарні, квантові обчислення, ШІ, менеджмент даних і підключеність до мережі працюють у когеренції та конвергенції; сприяння поширенню цифрових технологій підприємствами);

конкурентоспроможність (регуляторне середовище для підтримки здатності підприємств ЄС, особливо МСП, добросовісно конкурувати у глобальних ланцюгах вартості; сприяння екосистемі стартапів; досягнення високого рівня цифрової інтенсивності та інновацій на підприємствах ЄС, зокрема в стартапах і МСП; посилення синергій між приватними та громадськими інвестиціями, між використанням фондів ЄС і національних фондів, розроблення передбачуваних регуляторних та допоміжних підходів із залученням регіонального та місцевого рівнів; забезпечення координації та сумісності політик і програм для досягнення цілей DD, уникаючи дублювання та мінімізуючи адміністративне навантаження);

резильєнтність (зміцнення колективної стійкості держав-членів ЄС);

цифрові права та принципи, справедливе цифрове середовище (за свободою вибору).

У цифровій трансформації підприємств ЄС вирішальним елементом успіху й зростання економіки ЄС є їх цифровізація. Цифровізація є ключем до зміни бізнес-моделі підприємств, досягнення більшої ефективності у виробничих процесах, вивчення нових можливостей, генерування нових продуктів і послуг з новими потоками доходів. Запровадження передових цифрових технологій, таких як передова хмара, ШІ або аналітика даних, позитивно впливає на продуктивність підприємств. Фірми, які впроваджують передові цифрові технології, є продуктивнішими і зростають швидше, ніж менш цифровізовані фірми. Оскільки цифровізація є особливо важливою для підприємств, що стикаються з такими викликами, як інфляція, збільшення витрат на енергію, стагнація чи повільне зростання економіки, то цифровізація є важливою також для поліпшення резильєнтності. Крім того,

дослідження показують, що інвестиції в цифрові інновації та цифрову трансформацію є менш чутливими до економічних циклів: компанії збільшили свої інвестиції в цифровізацію після кризи COVID-19, і цей інвестиційний тренд продовжувався, незважаючи на економічний спад [3].

Як підкреслюється в опитуванні Європейського інвестиційного банку (заснований у 1958 р. з набуттям чинності Римського договору), ЄС повільно просувається в скороченні відставання від США за цифровізацією, де частка оцифрованих підприємств більша, ніж у ЄС. Хоча ЄС залишається головним глобальним гравцем у сфері досліджень і розробок (ДіР) та інновацій, частка компаній ЄС у провідних світових інвесторах у ДіР з часом спадає: компанії ЄС не мають очікуваних позицій у сфері цифрових інновацій [4].

Щоб посилювати цифровізацію в ЄС, програма політики DD встановила амбітні цілі ЄС для цифровізації бізнесу, які мають бути досягнуті до 2030 р. (90% МСП мають досягнути базового рівня цифрової інтенсивності, 75% МСП – використання ШІ, великих даних або хмари; кількість єдинорогів ЄС має подвоїтися). У 2023 р. лише 54,6% підприємств у ЄС застосовували принаймні одну з цільових цифрових технологій (хмарні обчислювальні послуги, аналітика даних, ШІ), причому більша кількість підприємств застосовувала поєднання цих трьох цифрових технологій.

Основні цілі програми DD включають побудову потужних цифрових екосистем, підтримку здатності підприємств ЄС (особливо МСП) впроваджувати інновації та добросовісно конкурувати в глобальних ланцюгах вартості, сприяння екосистемі стартапів. Вимірюються щорічний прогрес, зусилля ЄК та держав-членів ЄС щодо досягнення показників і цілей DD, а також поточні перспективи до 2030 р.

Цифрова трансформація впливає майже на кожний аспект життя, зокрема на розширення можливостей (empowering) людей і суспільства ЄС. З розвитком (гібридної) людської діяльності у віртуальному просторі стає імперативом розширювати можливості кожного користатися перевагами цифрових технологій, захищати людей і суспільства ЄС, зміцнювати та відстоювати такі фундаментальні елементи ЄС, як повага до основних прав людини і демократія. В Європейській декларації про цифрові права та принципи DD [5] ЄС виклав своє бачення, а також конкретні зобов'язання щодо застосування прав і свобод, закріплених у законодавчій базі ЄС, а також цінностей ЄС у цифровому трансформованому світі.

Це починання означає супроводжувати людей у цифровій трансформації, озброювати їх навичками та засобами, необхідними для повного її застосування. Це починання є також необхідним для з'ясування цифрових розривів, що зберігаються через різні фактори і відображають (якщо не посилюють). Багато груп у суспільстві ЄС часто зіштовхуються з низьким доступом до цифрових комунікацій. Такими групами є люди з низькими доходами, люди з низькою цифровою грамотністю, маргіналізовані громади чи меншини (наприклад, роми, які живуть у сегрегованих поселеннях), люди старшого віку, особи з обмеженими можливостями. Цим

групам часто бракує недорогих і доступних пристроїв і доступу до Інтернету; ці групи стикаються з бар'єрами під час навігації інтерфейсами користувача; ці групи не мають доступу до захищеної інформації та/або відповідних місцевих послуг місцевими мовами [6]. Наприклад, ромські громади присутні серед подібних груп: «дистанційне навчання через цифрову освіту найчастіше недоступне та/або дороге для маргіналізованих ромських дітей, яким не вистачає адекватного чи будь-якого ІТ-обладнання та/або підключення до Інтернету або часом електрики» [7].

Слід також зважати на небажання суспільства сприймати нові технології, спричинене питаннями довіри, викликаними міркуваннями безпечності й безпеки, неготовністю до швидкого розвитку і застосування технологій загалом.

Водночас цифрові технології, онлайн-платформи та відповідні бізнес-моделі ведуть до нових викликів: користувачі смартфонів стають вразливими до негативних проявів у віртуальному просторі, до контенту, який не відповідає статусу користувача, до незаконного контенту, до розпалювання ворожнечі, до дезінформації. Необхідні також спеціальні зусилля для забезпечення захисту від неправомірного використання персональних даних або маніпулятивних практик (наприклад, так званих темних шаблонів), гарантування ефективного захисту споживачів онлайн, посилення прозорості онлайн-послуг (включно з кращою інформацією про умови та положення стосовно таких послуг, з прозорістю систем, що використовуються для модерації контенту, і прозорістю алгоритмів, що використовуються для рекомендації контенту чи продуктів користувачам).

Дезінформація та викривлення інформації (misinformation) в Інтернеті можуть мати значний вплив на демократії ЄС, перешкоджаючи здатності громадян приймати інформовані рішення, сприяючи поляризації думок у суспільствах ЄС і кидаючи виклики демократичним процесам.

Програма політики DD чітко закликає до подолання цифрових розривів та сприяє «людино-центричним, основаним на фундаментальних правах людини, інклюзивним, прозорим і відкритим цифровим середовищам», створюючи засади Європейської декларації про цифрові права та принципи [1], яка доповнює згадану програму та сприяє цифровій трансформації, яка орієнтується на людей, надаючи їм новітні можливості, розвиваючи справедливе та інклюзивне суспільство й економіку ЄС. Розділ I: Висунення людей у центр цифрової трансформації [8] зазначає, що «технології мають служити та приносити користь усім людям, які живуть у ЄС, і надавати їм можливості реалізовувати свої прагнення у повній безпеці та повазі до їхніх основних принципів». Розділ II: Солідарність та інклюзія [8] стверджує, що «технології слід використовувати для об'єднання, а не для роз'єднання людей. Цифрова трансформація має сприяти справедливому та інклюзивному суспільству й економіці в ЄС». Декларація [8] також підкреслює, серед іншого, необхідність захисту конфіденційності та індивідуального контролю над даними (Розділ V: Безпечність, безпека та розширення можливостей) і

необхідність збереження свободи вибору, в тому числі в контексті взаємодії з алгоритмами та системами ШІ (Розділ III: свобода вибору), а також те, що «доступ до різноманітного контенту сприяє плюралістичному публічному обговоренню та ефективній участі в демократії в недискримінаційний спосіб» (Розділ IV: Участь у цифровому публічному просторі) [9].

Зазначені положення Декларації [8] становлять основу значних поточних зусиль ЄК щодо супроводу і підтримки людей у цифровій трансформації, розбудови безпечних цифрових середовищ, де захищаються фундаментальні права людини, люди висуваються у центр уваги, захищаються такі основоположні цінності ЄС, як демократія і свобода слова.

Розширення можливостей людей і наближення цифрової трансформації до їхніх потреб вимірюється кардинальними точками та цілями DD (цифрові навички та цифровізація публічних послуг (ключові цифрові публічні послуги та електронна ідентифікація (eID)).

1. Горбачук В.М., Єрмольєв Ю.М., Єрмольєва Т.Ю. Двоетапна модель еколого-економічних рішень. Вісник Одеського національного університету. Економіка. 2016. Т. 21. Вип. 9. С. 142–147.
2. Digital Decade in 2024: Implementation and perspective. Commission Staff Working Document (SWD) 260 final. Part 1/2. 2.7.2024 Brussels: European Commission, 2024. 248 p.
3. Teruel M., Bauer P., Coad A., Domnick C., Harasztosi P., Rückerte D., Weisse C. Dgitalisation and high-growth enterprises in Europe. Technology Analysis & Strategic Management. 2024. 14 p. https://doi.org/10.1080/09537325.2024.2394771
4. Brunori B., Harasztosi P., Merante C., Rückert D., Weiss C. Digitalisation in Europe 2022–2023. Evidence from the EIB Investment Survey. Luxembourg: Economics Department; European Investment Bank, 2023. 80 p.
5. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions establishing a European Declaration on Digital Rights and Principles for the Digital Decade. SWD 14 final. COM 27 final. 26.1.2022. Brussels: European Commission, 2022. 7 p.
6. Report on access to essential services in the EU. SWD. 28.06.2023. Brussels: European Commission, 2023. 74 p.
7. A Union of Equality: EU Roma strategic framework for equality, inclusion and participation and its accompanying proposal for a revised Council recommendation on national Roma strategic frameworks for equality, inclusion and participation. Analytical document accompanying the Communication from the Commission to the European Parliament, the Council. SWD 530 final. COM 620 final − COM 621 final. 7.10.2020. Brussels: European Commission, 2020. 79 p.
8. European Declaration on Digital Rights and Principles for the Digital Decade. COM 28 final. 26.1.2022. Brussels: European Commission, 2022. 7 p.
9. Lupei M., Mitsa O., Sharkan V., Vargha S., Gorbachuk V. The identification of mass media by text based on the analysis of vocabulary peculiarities using support vector machines. International Conference on Smart Information Systems and Technologies (SIST) (April 28−30, 2022, Nur-Sultan, Kazakhstan). IEEE, 2022. P. 1−6. https://doi.org/10.1109/SIST54437.2022.9945774.

І.П. Каменева

ЕКСПЕРТНІ МЕТОДИ ТА БАЗИ ЗНАНЬ ДЛЯ ПЕРЕДБАЧЕННЯ ТЕХНОГЕННИХ АВАРІЙ І КАТАСТРОФ

В останні кілька років спостерігається занадто швидке зростання кількості катастрофічних подій, що мають руйнівні наслідки. Тому проблема передбачення і завчасного інформування населення про небезпечні події та нові загрози набуває особливого значення.

Відомо, що більшість катастроф та інцидентів виникає на фоні підвищеної сонячної активності, сонячних спалахів і практично безперервних магнітних збурень. Найбільша кількість жертв спостерігається під час землетрусів, цунамі та процесів активізації вулканічної діяльності. Адже в останні роки зафіксовано просто вражаючу кількість катастроф, безліч жертв і руйнувань в різних частинах світу, що відбулися як наслідок надзвичайно високої сонячної активності та глобальних кліматичних змін. Так, в багатьох країнах Європи в 2024 році влітку люди страждали від небувалої спеки та жахливих лісових пожеж, а потім розпочався період непрогнозованих дощів і паводків, які затопили багато міст і провінцій. Зрозуміло, що всі ці події привели до жахливих наслідків для природних систем та довкілля.

Кількісні та якісні методи прогнозування.

Незважаючи на широку практику використання статистичних методів та наявність великих обчислювальних ресурсів, їх практичне застосування принципово обмежується лише випадками обробки ретроспективних даних кількісного характеру, які монотонно змінюються, або так званих "розмитих" даних. Іншими словами, при застосуванні кількісних методів прогнозування прогноз майбутнього фактично буде продовженням або екстраполяцією минулого. Ця обставина суттєво обмежує можливості статистичних методів, адже ми живемо у світі, де постійно відбуваються якісно нові, не властиві минулому події. Сюди насамперед відносяться різноманітні біфуркації або стрибкоподібні зміни, пов'язані з розривами монотонності.

Підкреслимо, що універсальних та досконалих підходів до вирішення проблеми передбачення ще не винайдено. Запропоновано багато засобів побудови можливих сценаріїв розвитку тих чи інших явищ у майбутньому. Але важливою відмінністю від типової практики вирішення подібних задач залишається той факт, що окрім кількісних методів моделювання бажано використовувати засоби, спрямовані на аналіз якісних характеристик.

Наразі відомо багато різних методів якісного характеру, які певною мірою можуть використовуватись на окремих етапах передбачення подій і ситуацій з майбутнього. Але в повному обсязі жоден із них не вирішує цієї проблеми. Саме тому передбачення досліджується як процес застосування окремих методів у певній послідовності, із встановленням чітко визначених

взаємозв'язків між ними згідно з методологією системного аналізу [1]. На рис.1 показано схему, де відомі методи прогнозування впорядковані за ступенем їх формалізації.

Якщо формалізовані методи засновані на проведенні математичного (або статистичного) аналізу тенденцій, зокрема, виявлення критичних точок або біфуркацій в поведінці певної системи, то більшість неформальних моделей зосереджено на виявленні ознак, прикмет або факторів, які вказують на можливу небезпеку (на свідомому або підсвідомому рівні). Отже, спостереження за відповідними ознаками або значеннями окремих показників допомагають завчасно виявити небезпечні зміни й збільшують шанси передбачити майбутні руйнівні події та підготуватись до них.

Рисунок 1 – Одна із можливих схем класифікації методів прогнозування

Методи експертних оцінок.

Експертні методи використовують для аналізу об'єктів і проблем, розвиток яких повністю або частково не піддається математичній формалізації, тобто для яких важко розробити адекватну модель. Це пояснюється невизначеністю та складністю явищ, що прогнозуються, необхідністю кількісно оцінити події, для характеристики яких відсутня необхідна інформація, а також в тих випадках, коли важливо враховувати не тільки об'єктивні тенденції розвитку ситуації, але й реакцію учасників подій на рішення, які приймаються.

В основі використання експертних методів лежать глибокі знання спеціалістів, уміння узагальнити свій та світовий досвід досліджень даної області, наявність відповідних знань та умінь, що формується в процесі певних видів діяльності, зокрема, уміння оцінити з певною вірогідністю терміни виникнення або прояву небезпечної події. Можливості застосування експертних методів і експертних систем для задач екологічної безпеки та оцінювання екологічних ризиків аналізуються в роботі [2].

Розроблено дві групи методів експертних оцінок: методи індивідуальних експертних оцінок і методи колективних експертних оцінок. До перших відносять метод інтерв'ю, аналітичний метод, метод побудови сценаріїв, метод генерації ідей. Коротко охарактеризуємо найбільш відомі методи побудови колективних експертних оцінок.

Дельфійський метод запропонований ще в 60-ті роки минулого сторіччя компанією Rand Corporation (США) як методика для побудови сценаріїв розробки та застосування нової зброї. Метод отримав свою назву від імені знаменитого грецького провидця Delphos. Особливість даного методу полягає в тому, що певна кількість незалежних експертів (до 20 експертів, які не знають один одного) може краще передбачити окремі події, оскільки такий підхід дозволяє уникнути зіткнень між представниками протилежних позицій і виключити безпосередній контакт експертів між собою, тобто зменшує груповий вплив на окремих індивідів.

Метод Сааті, або метод аналізу ієрархій розроблений американським математиком Томасом Л. Сааті (Thomas L. Saaty) [3]. На відміну від інших методів, що використовуються в цій сфері знань, ідея методу Сааті полягає в обов'язковій умові «фокусування» або «сходження» до єдиного рішення стосовно висновків всіх експертів, а також дій виконавців щодо процесу передбачення певних подій. Метод Сааті включає використання ієрархічних мереж для побудови моделі, призначеної для розрахунку ймовірностей виникнення кожного з можливих сценаріїв у майбутньому.

Моделі Байеса. Застосування моделі Байєса (Bayesian model technique) не орієнтоване на передбачення можливих сценаріїв майбутнього. Для групи попередньо визначених сценаріїв необхідно провести оцінювання, які з них більш реальні (точніше, мають вищу ймовірність). Загалом цей метод можна розглядати як інструмент для підтримки прийняття рішень, що забезпечує можливість досить точно орієнтувати дослідників щодо вибору можливих варіантів і подальшого прийняття ефективного рішення [4].

Для візуалізації тенденцій, пов'язаних з кожним із можливих сценаріїв розвитку майбутніх подій, отримані результати доцільно представити графічно. На основі аналізу цих результатів за допомогою експертів вже можна зробити остаточні висновки щодо того, які з досліджуваних сценаріїв мають бути найбільш реалістичними і адекватними.

Моделі Байеса загалом визнано найбільш послідовними і корисними для задач з невизначеністю, оскільки вони надають можливість для кількісного

опису невідомих величин, які можна враховувати в розподілі прогнозу через інтегрування або усереднення [5, 6]. Наразі цей метод одержав могутню підтримку завдяки швидкому розвитку сфери байесовських обчислень.

Одна з переваг моделей Байеса – можливість врахування семантичних аспектів багатовимірної інформації, що досліджується в роботах [7, 8].

В [7] визначено імовірнісні моделі репрезентації знань, де семантичні аспекти складної ситуації можна описати у термінах імовірності небезпеки. Розроблено методи перетворення даних екологічного моніторингу, надані в вигляді таблиць, в семантичний простір ризику, де визначено імовірнісну міру небезпеки (міру ризику), яка вказує належність випадкових подій до відповідних рівнів небезпеки. Для підтримки прийняття рішень в галузі енергетичної та екологічної безпеки запропоновано імовірнісні моделі аналізу даних і побудови баз знань, що включають експертні методи передбачення небезпечних подій з використанням моделі Байеса. Окремі приклади побудови імовірнісних розподілів ризиків для населення від певних рівнів техногенного забруднення наведено в роботах [7, 8].

1. Згуровський М.З., Панкратова Н.Д. Основи системного аналізу. – К.: Видавнича група BHV, 2007. – 544 с.
2. Лисиченко Г.В., Хміль Г.А., Барбашев С.В. Методологія оцінювання екологічних ризиків: монографія. – Одеса: Астропринт, 2011. – 368 с.
3. Saaty Th. RWS. Fundamentals of Decision Making and Priority Theory with the Analytic Hierarchy Process. – Pittsburgh, 1994. – 527 c.
4. Кини Р. Теория принятия решений // Исследование операций: в 2-х томах, т. 1. М.: Мир, 1981, с. 481 – 512.
5. M. Martin, David T. Frazier, Worapree Maneesoonthorn and others. Bayesian forecasting in economics and finance: A modern review – International Journal of Forecasting, Volume 40, Issue 2, Pages 811-839. https://www.sciencedirect.com/journal/international-journal-of-forecasting/vol/40/issue/2#article-15.
6. Li Li, Yanfei Kang, Feng Li. Bayesian forecast combination using time-varying features – International Journal of Forecasting, Volume 39, Issue 3, Pages 1287-1302 (July–Sept.2023) https://www.sciencedirect.com/science/article/abs/pii/S0169207022000930?via%3Dihub.
7. Каменева И.П., Артемчук В.А., Яцишин А.В. Вероятностное моделирование экспертных знаний с использованием методов психосемантики // Електронне моделювання, 2019, 41, № 2, с. 81–96.
8. Каменева І.П., Артемчук В.О., Яцишин А.В, Владимирський О.А. Імовірнісні моделі подання знань для підтримки прийняття рішень в умовах ризику та невизначеності на прикладі галузі охорони атмосферного повітря // Електронне моделювання, 2024, 46, № 1, с. 3 –20.

А.В. Ковилін

АНАЛІЗ ПОТЕНЦІЙНОГО ЗАСТОСУВАННЯ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ ПРИХОВАНИХ КІБЕРЗАГРОЗ НА ОБ'ЄКТАХ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ

Кібератаки на критичну інфраструктуру, зокрема на об'єкти енергетики, є серйозним викликом сьогодення. До зростання кількості та витонченості зловмисних дій додаються терористичні та мілітарні загрози. З іншого боку, розвиток комп'ютерних технологій і, як наслідок, інтенсивна цифровізація виробництва водночас з відомими перевагами призводять до переносу ризиків кібербезпеки з інформаційної галузі на підприємства генерації, транспорту та розподілу електричної енергії.

Відомі підходи, що базуються на використанні сигнатурного аналізу або традиційних методів виявлення аномалій не в повній мірі дозволяють врахувати згадані вище особливості кіберзахисту об'єктів критичної інфраструктури. Тому останнім часом дослідники, спеціалісти з безпеки комп'ютерних систем та дата-аналітики все більш активно використовують методи штучного інтелекту та машинного навчання (англ. Machine Learning – ML) [1].

Використання алгоритмів ML для виконання завдань захисту інформації дозволяє значно підвищити ефективність розпізнавання та ідентифікації потенційних загроз. Крім того, застосування моделей ML дозволяє підвищувати точність розпізнавання ознак зловмисної активності та суттєво зменшувати кількість хибних спрацювань (false positive), що тривалий час вважалося основним недоліком підходу розпізнавання атак на основі виявлення аномалій [2].

До популярних моделей ML можна віднести:

- ***Моделі з вчителем*** (Supervised Learning Models) [3] базуються на попередньо оброблених даних, що дозволяє їм навчитися розрізняти нормальну і аномальну активність.
- ***Моделі без вчителя*** (Unsupervised Learning Models) [3] на відміну від моделей з вчителем не потребують попередньо оброблених (розмічених) даних і часто використовуються у випадках, коли мітки для аномалій не доступні.
- ***Напів контрольовані моделі*** (Semi-Supervised Learning Models) [4] поєднують елементи контрольованого та неконтрольованого навчання, дозволяючи навчатися на частково розмічених наборах даних.
- ***Моделі з підкріпленням*** (Reinforcement Learning Models) [5], такі як Q-Learning і Deep Q Networks (DQN), а також Policy Gradient Methods, використовуються для сценаріїв, де модель навчається шляхом взаємодії з середовищем.

- ***Ансамблеві методи*** (Ensemble Learning Models) [6], такі як Boosting (наприклад, XGBoost, AdaBoost), Bagging та Stacking, поєднують кілька моделей для досягнення кращих результатів, ніж з використанням однієї моделі.
- ***Глибоке навчання*** (Deep Learning Models) [7] забезпечує високу гнучкість і здатність шукати складні патерни у великих обсягах даних.

Розглянуті моделі та підходи можуть бути використані для виявлення закономірностей в поведінці інформаційних систем, спираючись на результати аналізу мережевого трафіку та записи в системних журналах.

В якості основного засобу розробки програмного забезпечення для проведення експериментів з метою оцінки кількісних характеристик алгоритмів ML, що аналізувалися, було створено програму з допомогою мови програмування Python та широким певним набором бібліотек, в тому числі – для аналізу даних, побудови нейронних мереж та машинного навчання.

Основним джерелом інформації для дослідження став відкритий набір даних **Network Traffic Analysis for Cybersecurity** (від University of New South Wales (Australia)) [8], доступний для вільного використання, містить детальну інформацію про мережеві з'єднання та аномальні події, що можуть виникати в комп'ютерних мережах. Набір поданий у табличній формі (у вигляді CSV-файлу) та включає такі атрибути, як тривалість з'єднання (dur), тип протоколу (proto), статус з'єднання (state), кількість пакетів, що були відправлені та отримані (spkts, dpkts), обсяг переданих даних (sbytes, dbytes), швидкість передачі (rate), час виявлення (sttl, dttl), а також інформацію про трафік (sload, dload), втрати пакетів (sloss, dloss) та середні затримки (tcprtt, synack, ackdat).

Набір даних також містить інформацію про певні характеристики сесій, як-от використані TCP порти (swin, dwin), глибину передачі (trans_depth), а також різні статистичні показники, наприклад, кількість джерел/цілей для певного сервісу (ct_srv_src, ct_srv_dst). Поля is_ftp_login та ct_ftp_cmd надають інформацію щодо активності, пов'язаної з FTP, а ct_flw_http_mthd описує кількість HTTP запитів, використаних у сесії.

Крім того, набір містить атрибути, які описують тип атаки (attack_cat) та мітку, що вказує на те, чи є цей запис аномальним (label).

В якості засобів виявлення прихованих атак та аномалій для забезпечення безпеки об’єктів критичної інфраструктури в даному дослідженні було протестовано кілька алгоритмів машинного навчання з вчителем (supervised) та без вчителя (unsupervised), напів контрольованого навчання (semi-supervised), ансамблева модель (Ensemble Learning Models), глибоке навчання (Deep Learning Models). Основною метою експериментів було оцінити та порівняти ефективність різних алгоритмів щодо виявлення аномалій, пов’язаних з мережевими атаками та нестандартною поведінкою мережевого трафіку.

Проаналізуємо результати, отримані під час проведення експериментів (табл. 1).

Таблиця 1 – Результати, отримані під час проведення експериментів

Model	Precision	Recall	F1-Score	Specificity	FPR	FNR	Cohen Kappa	AUC
Isolation Forest	0.70247	0.03096	0.0593	0.972053	0.02794	0.969	0.00195	0.5015
KMeans	0.82258	0.64482	0.72293	0.703625	0.29637	0.3551	0.3105	0.6742
DBSCAN	0.96774	0.00251	0.00501	0.999821	0.00017	0.9974	0.00149	0.5011
LOF	0.669074	0.02949	0.05649	0.968910	0.03108	0.9705	-0.00103	0.4992
MLP Classifier	0.999974	0.99989	0.99993	0.999946	5.36E-05	0.0001	0.9998	0.9999
Label Propagation	0.999848	0.99491	0.99737	0.999678	0.00032	0.005	0.99182	0.9972
Deep Learning Model	0.999941	0.99989	0.99992	0.999875	0.00012	0.0001	0.99975	0.9998
Ensemble Model	0.999932	0.99999	0.99996	0.999857	0.00014	8.38E-06	0.99988	0.99992

Таблиця 2 – Порівняння швидкості аналізу даних за допомогою різноманітних ML моделей та технік

Model	Technique Type	Execution Time (s)	Anomalies Detected
Isolation Forest	Unsupervised	1.549451113	5260
KMeans	Unsupervised	4.722438097	93551
DBSCAN	Unsupervised	86.40836883	310
LOF	Unsupervised	44.28485823	5261
MLP Classifier	Supervised	12.9622159	119332
Label Propagation	Semi-supervised	30.56289482	118752
Deep Learning Model	Deep Learning	5.664246082	119336
Ensemble Model	Ensemble	130.3820982	119348

Ансамблева модель та глибока модель (MLP) показали найвищі результати з точки зору всіх метрик, включаючи точність, повноту та узгодженість. Ці моделі забезпечують найбільш точну та надійну класифікацію аномалій, хоча ансамблева модель потребує більше часу для виконання. Label Propagation також показує хороші результати, але трохи поступається MLP та ансамблевій моделі. Класичні моделі для кластеризації та виявлення викидів (Isolation Forest, KMeans, DBSCAN, LOF) значно поступаються за ефективністю порівняно з моделями, що навчаються. Ці моделі демонструють низькі значення Recall та F1-Score, що робить їх менш ефективними для виявлення аномалій. MLP та моделі глибокого навчання рекомендуються, якщо важлива висока точність і чутливість, а також потрібно мінімізувати хибні спрацювання та пропуски.

Висновок. Результати проведеного дослідження свідчать, що використання алгоритмів машинного навчання розширює можливості дата-аналітиків та спеціалістів з безпеки комп'ютерних систем, та можуть бути ефективно використані для виявлення прихованих кіберзагроз на об’єктах енергетичної інфраструктури.

Проведений теоретичний і практичний порівняльний аналіз майже десятка алгоритмів машинного навчання з використанням публічного набору даних **Network Traffic Analysis for Cybersecurity** (від University of New South Wales (Australia)), дозволив виявити з них найбільш перспективні для виявлення аномалій у вхідних даних. Отримані для різних моделей характеристики точності та швидкодії дозволили виокремити алгоритми, найбільш придатні для різних умов використання в системах захисту інформації. Для випадків, коли потрібна висока швидкодія обробки даних, більш прийнятними виявилися алгоритми K-Means та Isolation Forest (unsupervised), а для менш критичних за часом застосувань ефективні більш точні алгоритмами MLP Classifier (supervised), Label Propagation (semi-supervised). Найкраще себе показали Deep Learning Model (deep learning на базі sequential) та Ensemble Model (яка має в своїй реалізації логістичну регресію (Logistic Regression), метод опорних векторів (SVM) та метод найближчих сусідів (KNN), які об'єднуються в класифікатор з голосуванням (Voting Classifier)) які тримають хороший баланс між кількістю виявлених аномалій, точністю та швидкістю виконання.

В подальших дослідженнях планується проведення експериментів з більш тонкими налаштуваннями досліджених алгоритмів з метою ще більшого покращення досягнутих показників.

1. Abiodun, O. I., Jantan, A., Omolara, A. E., Dada, K. V., Mohamed, N. A., & Arshad, H. (2018). State-of-the-art in artificial neural network applications: A survey. Heliyon, 4(11), e00938. https://doi.org/10.1016/j.heliyon.2018.e00938.
2. Afrifa S, Varadarajan V, Appiahene P, Zhang T, and Domfeh E. A. Ensemble Machine Learning Techniques for Accurate and Efficient Detection of Botnet Attacks in Connected Computers. 2023; 4(1):650-664. https://doi.org/10.3390/eng4010039.

3. Numadiah Zamri et al. A comparison of unsupervised and supervised machine learning algorithms to predict water pollutions. Procedia Computer Science 204 (2022) 172–179. https://doi.org/10.1016/j.procs.2022.08.021.
4. Vivian Lay Shan Lee, Keng Hoon Gan, Tien Ping Tan, Rosni Abdullah (2020). Semi-supervised Learning for Sentiment Classification using Small Number of Labeled Data. Procedia Computer Science Volume 161, 2019, 577-584. https://doi.org/10.1016/j.procs.2019.11.159.
5. Ashish Kumar Shakya, Gopinatha Pillai, Sohom Chakrabarty. Reinforcement learning algorithms: A brief survey. Expert Systems with Applications Volume 231, 30 November 2023, 120495. https://doi.org/10.1016/j.eswa.2023.120495.
6. Azal Ahmad Khan, Omkar Chaudhari, Rohitash Chandra. A review of ensemble learning and data augmentation models for class imbalanced problems: Combination, implementation and evaluation. Expert Systems with Applications Volume 244, 15 June 2024, 122778. https://doi.org/10.1016/j.eswa.2023.122778.
7. Shams Forruque Ahmed, Md. Sakib Bin Alam, Maruf Hassan, Mahtabin Rodela Rozbu, Taoseef Ishtiak, Nazifa Rafa, M. Mofijur, A. B. M. Shawkat Ali & Amir H. Gandomi. Deep learning modelling techniques: current progress, applications, advantages, and challenges. Volume 56, pages 13521–13617, (2023). https://doi.org/10.1007/s10462-023-10466-8.
8. https://www.kaggle.com/code/akritiupadhyayks/cyber-attack-detection-with-random-forest/input?select=UNSW_NB15_training-set.csv.

С.А. Ликов

МОДЕЛЮВАННЯ СИСТЕМИ ОСВІТЛЕННЯ ФУТБОЛЬНОГО ПОЛЯ

У 129-ій школі, де я раніше навчався, на задньому дворі, раніше був футбольний майданчик з воротами, але без розмітки. На даний момент він розібраний (зняли ворота) і запущений (заріс травою). Я вважаю, що його треба поновити для комфорту і фізичного розвитку учнів.

Рисунок 1 – вигляд шкільного футбольного майданчика на данний момент

Зараз поле вкриває природня трава. Такий тип покриття погано підходить для футбольного майданчика бо потребує серйозного догляду. Тому це покриття необхідно замінити на штучну траву.

Штучна трава має багато переваг це: м'якість покриття що знижує навантаження на хребет, суглоби і ноги гравця, а також дозволяє їм м'яко і легко переміщатися по полю; можливість регулювання відскоку м'яча (від повільного до дуже швидкого); можливість повороту і ковзання; стійкість до температурних перепадів від -30°С до +50°С, без шкоди технічним характеристикам: не вицвітає, не вигоряє, не ламається при замерзанні; висока пропускна здатність води, до 60 л/хв; висока зносостійкість, довговічність і надійність експлуатація, тривалість експлуатації покриття "штучна трава", за умови правильного догляду 10-15 років.

Спортивна штучна трава відрізняється від декоративної тим що має менш щільний ворс, бо для спортивного варіанту використовують засипання. Для спортивних майданчиків і особливо, для футбольних полів необхідна засипна або напів-засипна трава. Таке покриття без засипки підходить лише для використання у декоративних цілях.

Штучна трава з висотою ворсу 35-39мм. засипають лише кварцовим піском. І це оптимальний варіант для універсального спортивного майданчика, шкільного стадіону або міні-футбольного поля. А ворс з висотою 40мм. і вище засипається спочатку піском, а потім гумовим гранулятом. Саме гумовий гранулят пом'якшує падіння і запобігає отриманю травм і опіків при ковзанні. Це підходить для футбольного поля як бюджетний варіант, якщо на ньому не планують проводити офіційні змагання.

Освітлення важлива частина будь-якої спортивної споруди для комфорту гри.

Для освітлення шкільного стадіону ми використаємо 8-ми щоглову систему. Є ще лінійна і змішана системи але через особливості нашого поля в них немає необхідності. А саме наше поле маленьке 45х25м.

При лінійній системи освітлення прожектори установлюють уздовж довгих сторін ігрового поля на козирку над трибунами, або на спеціальних металоконструкціях. Суцільна або лінія що складається з окремих груп прожекторів дозволяє забезпечити потрібні зорові умови і вимоги телебачення. Глибина тіней при цій системі також зменшується. Їх обмежує умова розміщення прожекторів, при якому сліпуча дія зменшується.

За кількістю опор часто використовується система із 4-ма щоглами розставлених по кутам поля. Такий спосіб застосовується для освітлення невеликих спортмайданчиків, де висота щогл невелика. Також залежно від поля і розташування щогли вони можуть бути більше як кількістю так і розміром. Їх висота може досягати 80м. і більше. І ще ця система може використовуватись в поєднанні з групами прожекторів, встановлених на козирках, опорах або інших будівельних елементах для поліпшення якості освітлення.

Освітлення спортивних майданчиків регулюється відповідно до вимог нормативних документів в Європейському стандарті EN 12193:1999. Цей документ визначає параметри освітлення для проєктування і контролю встановлення спортивного освітлення, таких як: освітленість, рівномірність освітлення, сліпуча дія і колірні властивості джерел світла. Стандарт містить перелік основних вимог: освітлення ігрових закритих і відкритих майданчиків для різних видів спорту та багатоцільових спортивних споруд; освітлення глядацьких трибун; освітлення безпеки; аварійне освітлення для продовження спортивного заходу; обмеження сліпучої дії; колір і властивості відбивання поверхонь.

Застосування більшої кількості прожекторних щогл (6-8 і більше освітлювальних опор) спрощує завдання отримання регламентованих показників освітлення але це збільшує вартість освітлення. Такий спосіб використовується при освітленні невеликих спортмайданчиків, де висота щогл невелика.

Також при проектуванні освітлення футбольних стадіонів крім мінімальної яскравості необхідно враховувати рівномірність світлового потоку. Якщо гра буде транслюватися по телебаченню то вимоги будуть іншими. Для кольорового телевізійного сигналу в Європі встановлюються норми освітлення в межах 1200лк.-1400лк. - у вертикальній площині, для цього використовують щоглові системи, лінійні світильники або змішані системи.

1. Регламент інфраструктури стадіонів та заходів безпеки проведення змагань з футболу. https://upl.ua/uploads/2002/Da5_5AJwOaQjy3uCJS17lYq7ArM1q2b_.pdf.
2. Спортивні та фізкультурно-оздоровчі споруди ДБН В.2.2-13-2003. http://kyiv-heritage.com/sites/default/files/%D0%94%D0%91%D0%9D%20%D0%92.2.2-13~2003%.pdf.
3. Комп'ютерне проектування освітлення спортивних споруд. https://eprints.kname.edu.ua/28630/1/% pdf.

Л.О. Митько

ЕНЕРГЕТИЧНА БЕЗПЕКА З ТОЧКИ ЗОРУ КОГНІТИВНИХ ФУНКЦІЙ ПЕРСОНАЛУ ПРИ СУЧАСНОМУ РОЗВИТКУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Безпека енергетичної галузі на фоні розвитку інформаційних технологій тісно пов'язана з когнітивними функціями персоналу, який задіяний на всіх етапах її функціонування, починаючи з видобутку та підготовки палива, виробництва та трансформації енергії, транспортування, розподілу, зберігання та споживання, обліком і управлінням. До появи цифрових технологій процеси прийняття рішень формувались людиною на безпосередньому контакті з середовищем, де відбувався аналіз наявної інформації, пошук нових знань та контактів з іншими людьми. Процес прийняття рішень вимагав від людини, крім аналізу інформації, ще й автоматичного залучення критичної складової.

З появою цифрових пристроїв, різнопланових платформ медіа та розробок в сфері штучного інтелекту (ШІ), які забезпечили зручність, зв'язок і швидкість, зробили життя людей простішим і ефективнішим. В той же час виявилось, що сучасні цифрові технології впливають на роботу мозку та когнітивні здібності людини, які пов'язані з пам'яттю, увагою, залежністю від інших думок, пошуком новизни та сприйняттям інформації, прийняттям рішень, здатністю до навчання, критичним мисленням.

З'явились нові проблеми, що стосуються когнітивних здібностей людини, і тому вплив сучасних інформаційних технологій на людину став об'єктом дослідження когнітивної психології в останні роки. В результаті таких досліджень було показано, що людина має обмежену здатність до постійної уваги та може бути зосередженою лише на певному завданні чи стимулі протягом обмеженого часу. При чому ця здатність не може бути фіксованою і залежить від таких факторів, як самого завдання та зацікавленості особи в цьому завданні, мотивації та особистого досвіду [1].

У цифровому світі за увагу людини конкурують сповіщення, оновлення соціальних мереж, електронні листи, твіти, календарні нагадування, текстові повідомлення та стрічки новин. І результатом таких процесів стали симптоми перевантаження уваги людини в цифровому світі, який назвали феноменом «безперервної часткової уваги» [2]. Безперервна часткова увага відноситься до стану безперервного розподілу та переміщення уваги особи на численні задачі або стимули без повного занурення в них і розглядається як часткова участь в будь-якому. Така практика досить часто призводить до поверхневого розуміння інформації та зниження здатності зосередитися на конкретному завданні чи частині інформації. В результаті досліджень було показано, що надмірне використання цифрових технологій може змінити структуру та функції мозку, що призводить до ряду когнітивних порушень, а інтернет-залежність пов'язана зі зниженою щільністю сірої речовини у

фронтальній корі головного мозку, яка відповідає за прийняття рішень і контроль імпульсів. Залежність від смартфонів також пов'язана зі зниженою активністю префронтальної кори, яка відповідає за прийняття рішень і контроль імпульсів, а надмірне використання цифрових пристроїв сприяє когнітивним порушенням, подібним тим, що спостерігаються при деменції. Цікаво, що ці ефекти все частіше спостерігаються у молодих людей, які, як правило, не зазнають вікової нейродегенерації, пов'язаної зі старістю [3].

Цифрові технології в енергетичній галузі значно вплинули на когнітивний процес прийняття рішень, впливаючи на те, як збирається, обробляється і оцінюється інформація. Ці впливи мають як розширення можливостей, так і потенційно руйнівні наслідки, особливо на фоні постійного розвитку ШІ, якому все частіше делегуються не лише рутинні завдання, а й складні когнітивні процеси. Така тенденція сприяє формуванню у персоналу стану, коли розумовий апарат поступово втрачає здатність до самостійного вирішення задач, критичного мислення та творчого осмислення проблем.

Енергетична галузь висуває вимоги в здатності персоналу швидко адаптуватися до нових умов з розвитком навичок критичного мислення. Тому важливо, щоб персонал мав можливість встановлювати таймери для зосередження на цілеспрямованих завданнях, бо саме такі моменти можуть допомогти зменшити цифрові відволікання, а отже зменшити вимоги до їхніх ресурсів уваги та ефективніше зосередитися на виконанні поточного завдання. Зосередження на одному завданні за раз може покращити продуктивність і зменшити відчуття стресу [4], що сприятиме прийняттю кваліфікованих рішень. Для персоналу, який задіяний на енергетичних об'єктах, бажано б організовувати семінари, на яких розв'язувалися складні завдання, головоломки, тощо, які б паралельно вимагали розширення когнітивних можливостей та розвитку критичного мислення. Такі семінари допомогли б персоналу, задіяному не тільки в енергетичній галузі, підтримувати мозок у тонусі, зберігати когнітивну гнучкість та критичне мислення.

1. Oberauer, K. (2019). Working memory and attention - a conceptual analysis and review. J Cogn. 2, 36. doi: 10.5334/joc.58.
2. Chen, H., Dong, G., and Li, K. (2023). Overview on brain function enhancement of Internet addicts through exercise intervention: based on reward-execution-decision cycle. Front. Psychiatry 14, 1094583. doi: 10.3389/fpsyt.2023.1094583.
3. Manwell, L. A., Tadros, M., Ciccarelli, T. M., and Eikelboom, R. (2022). Digital dementia in the internet generation: excessive screen time during brain development will increase the risk of Alzheimer's disease and related dementias in adulthood. J. Integr. Neurosci. 21, 28. doi: 10.31083/j.jin2101028.
4. Ophir, E., Nass, C., and Wagner, A. D. (2009). Cognitive control in media multitaskers. Proc. Natl. Acad. Sci. 106, 15583–15587. doi: 10.1073/pnas.0903620106.

В.Р. Сенченко, А.В. Бойченко

ЗАСТОСУВАННЯ СЦЕНАРНОГО АНАЛІЗУ ПРИ ДОСЛІДЖЕННІ КАСКАДІВ ПОВ'ЯЗАНИХ КРИТИЧНИХ ІНФРАСТРУКТУР

В умовах агресії рф проти України забезпечення стійкості мереж критичної інфраструктури (КІ) набуває особливої ваги.

Потенційний вплив каскадних ефектів на КІ перебуває в центрі уваги чисельних вітчизняних та зарубіжних науковців. Досліджуються, зокрема питанням імітації мереж взаємозалежних інфраструктур для прогнозування їх стійкості за різних сценаріїв збоїв і відновлення [1, 5].

Прикладом підходу до аналізу взаємопов'язаних ризиків, створених каскадними небезпеками є використання моделювання на основі методів теорії гіперграфів, що дозвооляє відображати невизначеність параметрів моделі [2].

Іншим піходом є використання моделей взаємозалежностей, що визначають, як та якою мірою втрата керованості після збоїв впливає на КІ, дозволяють побудувати схеми балансування, які використовуються для пом'якшення наслідків каскадних подій [3].

В літературі є багато посилань на моделюванню каскадних збоїв в пов'язаних КІ мережевими методами – Баєса, Петрі, Маркова. Вибір конкретного методу залежить від характеристик КІ та типу необхідного аналізу [6].

Для поглибленого дослідження впливу каскадних ефектів (КЕ) на функціональну стійкість взаємодіючих КІ пропонується методологія, заснована на засадах сценарного аналізу. Замість формування єдиного результату моделювання, вона передбачає створення ряду вірогідних сценаріїв розвитку КЕ на основі різних припущень і змінних, що визначають каскадний процес. Методологія включає наступні кроки [4]:

– визначення взаємозалежностей між КІ (фізичних, функціональних, технологічних, операційних зв'язків тощо).

– визначення типів подій, які можуть ініціювати КЕ в пов'язаних КІ;

– розроблення моделі взаємодії між КІ, яка враховує їх реакцію на події, часові затримки, зворотні цикли та механізми поширення;

– моделювання та дослідження різних сценаріїв розвитку КЕ, починаючи з найбільш імовірної події. Оцінка реалістичності подій та аналіз впливу на КІ. Попередня оцінка наслідків каскадного ефекту;

– виявлення вузлів та компонентів КІ, що викликають КЕ з найвищим ступенем вірогідності;

– кількісна оцінка наслідків КЕ (економічні втрати, збої в роботі послуг, ризики для громадської безпеки, соціальні наслідки тощо);

– розробка стратегій мінімізації наслідків КЕ (резервування, покращення зв'язку та координації між КІ, розробка планів швидкого реагування тощо);

– перевірка ступеню резильєнтності КІ методом розрахунку різних варіантів стратегій мінімізації наслідків КЕ;

– вдосконалення та дослідження моделі для отримання повного розуміння КЕ (коригування параметрів, дослідження різних сценаріїв, аналіз «що, якщо»);

– вироблення управлінських рішень на основі всебічного аналізу моделі КЕ для підвищення резильєнтності КІ та мінімізації негативних наслідків.

Головною складністю покращення якості мережевих моделей є відсутність достатньої вибірки даних (експертних оцінок) для призначення чисельних змінних, що описують процеси КІ і які саме й дозволяють налаштувати модель КЕ та зробити її більш реалістичною. Для подолання цього недоліку пропонується застосування сучасних технологій, заснованих на знаннях, зокрема OWL2 або Knowledge Graph NEO4J+Cypher (Рис.1).

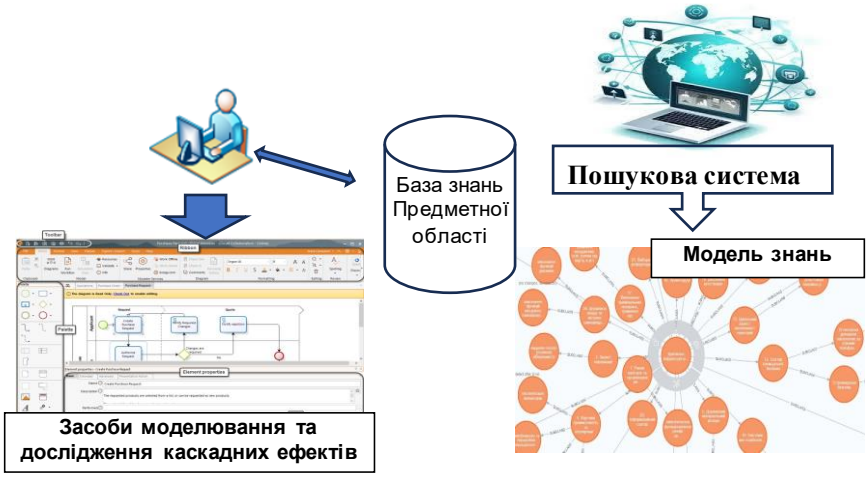


Рисунок 1 – Застосування бази накопиченого досвіду при дослідженні каскадів

Важливим кроком запропонованої методології є побудова графової моделі розвитку КЕ, яка дозволяє представити об'єкти КІ та зв'язки між ними у графовій базі даних. Це дає можливість використовувати вже існуючі інструментальні засоби побудови моделей та метрики аналізу графових структур, які суттєво прискорюють процес дослідження розвитку КЕ. За допомогою цих засобів можна оцінювати поведінку КІ при виникненні різних сценаріїв розвитку КЕ та виявити найбільш вразливі вузли КІ, що впливає на прийняття рішень.

Розширення таким чином байєсівських моделей поліпшує логічний висновок за рахунок уточнених зв'язків між змінними. Удосконалення мереж Петрі зменшує неоднозначність у взаємодії між компонентів моделі більш ефективно інтерпретуючи нюанси каскадних збоїв. Посилення марковських моделей знаннями дозволяє більш повно визначити стани в моделях Маркова, вказуючи умови, які впливають на ймовірність переходу, дозволяючи більш детально зрозуміти, як каскадні ефекти розгортаються з часом

Використання даного підходу дозволяє здійснювати аналіз каскадних ефектів пов'язаних критичних інфраструктур на базі моделюючого комплексу Інституту проблем реєстрації інформації НАН України. Результати моделювання, мають дозволити приймати більш обґрунтовані управлінські рішення.

1. Cassottana, B., Biswas, P. P., Balakrishnan, S., Ng, B., Mashima, D., & Sansavini, G. (2022). Predicting resilience of interdependent urban infrastructure systems. IEEE Access, 10, 116432-116442.
2. Dunant, A., Robinson, T. R., Densmore, A. L., Rosser, N. J., Rajbhandari, R. M., Kincey, M., ... & Dadson, S. (2024). Impacts from cascading multi-hazards using hypergraphs: a case study from the 2015 Gorkha earthquake in Nepal. EGUsphere, 2024, 1-28.
3. Ghasemi, A., & de Meer, H. (2023). Robustness of interdependent power grid and communication networks to cascading failures. IEEE Transactions on Network Science and Engineering, 10(4), 1919-1930.
4. Сенченко В.Р., Бойченко А.В., Коваль О.В., Бисько Р.М. & Хоменко О.М. (2024). Огляд методів і технологій сценарного аналізу каскадних ефектів. Реєстрація, зберігання і обробка даних, 26(1), 24-54. DOI: 10.35681/1560-9189.2024.26.1.308506.
5. Бойченко А.В., Сенченко В.Р. Дослідження взаємозв'язків об'єктів критичної інфраструктури. Міжнародна науково-практична конференція «Живучість та резильєнтність – 2023». Збірник матеріалів конференції. Київ. 2023. – с. 102-103.
6. Хоменко О.М., Сенченко В.Р., Коваль О.В. Мережевий підхід при дослідженні каскадних ефектів критичних інфраструктур ISSN 1560-9189 Реєстрація, зберігання і обробка даних, 2024, Т. 26, № 2, Сс 44-71.

Т.В. Пучко

МЕТАЕВРИСТИЧНІ АЛГОРИТМИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ ОПТИМІЗАЦІЇ СТРУКТУРИ ГЕНЕРУЮЧИХ ПОТУЖНОСТЕЙ ЕЛЕКТРОЕНЕРГЕТИЧНИХ СИСТЕМ

У сучасних умовах терористичних і воєнних загроз критично важливим є пошук ефективних способів оптимізації структури генеруючих потужностей енергетичних систем. Атаки на енергетичну інфраструктуру спричиняють перебої в електропостачанні, що негативно впливає на національну безпеку, економіку та суспільство. Водночас відновлювані джерела енергії (ВДЕ) відіграють ключову роль у підвищенні енергетичної безпеки, однак їхня непередбачуваність і некерованість ускладнюють управління системами, особливо в кризових умовах [1].

Задачі оптимізації, пов'язані з плануванням генеруючих потужностей, часто формулюються як задачі змішаного цілочисельного лінійного програмування (MILP) та потребують високопродуктивних обчислювальних ресурсів. Розподілене використання ВДЕ та систем зберігання енергії сприяє надійності енергосистем, але для їх планування необхідно розробляти паралельні алгоритми, здатні ефективно розв'язувати задачі великої розмірності. Це робить дослідження методів паралельної оптимізації надзвичайно актуальним.

Одним із підходів до розв'язання задач MILP великої розмірності є метод декомпозиції [2]. Завдяки особливостям задачі оптимізації структури генеруючих потужностей, її можливо розділити на підзадачу першого рівня, яка визначає кількість генеруючих блоків і вартість їх встановлення, та множину підзадач другого рівня, які враховують технологічні умови навантаження блоків і операційні витрати. У цьому підході перший рівень доцільно розв'язувати за допомогою метаевристичного алгоритму, тоді як підзадачі другого рівня можуть бути розв'язані паралельно з використанням будь-яких доступних MILP-солверів.

Метою цього дослідження було оцінити ефективність з точки зору часу виконання та надійність різних алгоритмів, зреалізованих у програмному пакеті Metaheuristics [3], при їх використанні на першому рівні розділеної задачі, оскільки саме цей рівень значною мірою визначає загальну ефективність розв'язання задачі. У рамках дослідження проведено порівняння продуктивності восьми метаевристичних алгоритмів із результатами, отриманими за допомогою лише солвера SCIP [4]. Це дозволило оцінити потенціал метаевристичних підходів у задачах оптимізації структури генеруючих потужностей.

Для проведення експериментального дослідження задачу оптимізації структури генеруючих потужностей локальної мережі було сформульовано як задачу MILP. Спочатку її було розв'язано лише за допомогою солвера SCIP, щоб отримати розв'язок та час розв'язування для порівняння з результатами

наступних експериментів. Щоб усунути сторонні чинники було виконано десять незалежних запусків солвера та зафіксовано розв'язок та час розв'язування задачі. Після цього задачу було розділено та розв'язано з використанням солвера SCIP і тих алгоритмів у пакеті Metaheuristics, які призначені для оптимізації однієї цільової функції. Додатковим критерієм вибору алгоритмів було одночасне обчислення цільової функції для багатьох потенційних розв'язків задачі, що необхідно для паралельного розв'язування великої кількості підзадач, як показано на рис. 1.

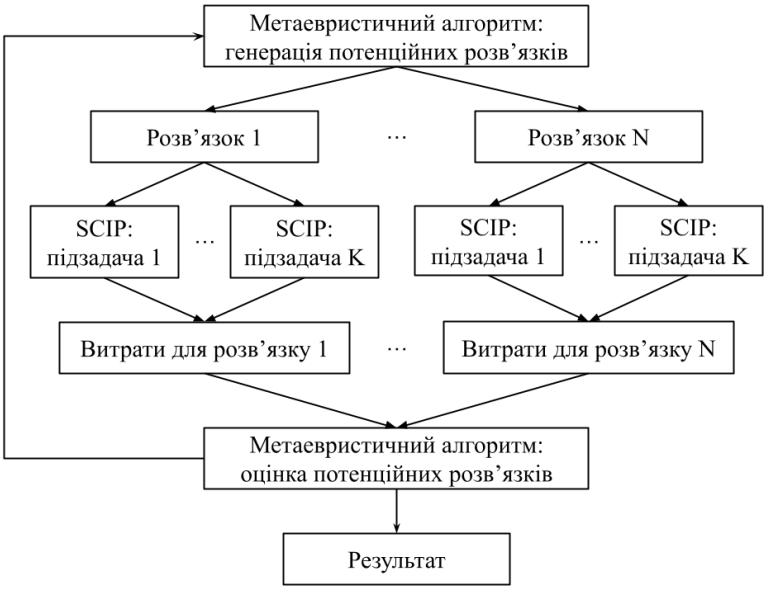


Рисунок 1 – Узагальнений алгоритм розв'язування задачі MILP з використанням метаевристичного алгоритму та солвера SCIP

Експеримент проводився на комп'ютері, оснащеному 768 ГБ оперативної пам'яті та двома процесорами AMD EPYC™ 9124, що працюють на частоті 3,0 Гц і разом мають 32 ядра. При ініціалізації кожного алгоритму використовувалися типові параметри, призначені для розв'язування задач з цілочисельними змінними. Оскільки тривалість розв'язування задачі метаевристичним алгоритмом залежить від випадково згенерованих чисел, було заплановано виконання кожного алгоритму 100 разів, використовуючи значення від 0 до 99 для ініціалізації генератора випадкових чисел. Під час кожного запуску фіксувалися час пошуку розв'язку та успішність виконання, при цьому загальний час роботи алгоритму був обмежений 10 годинами на всі спроби. Оцінювання алгоритмів проводилося за трьома критеріями: успішністю знаходження оптимального розв'язку, середнім часом виконання та стандартним відхиленням часу виконання.

У результаті експерименту було отримано дані, наведені в табл. 1. Усі алгоритми було виконано по 100 разів, за винятком GA, який через обмеження на загальний час роботи алгоритму вдалося виконати лише 35 разів. Алгоритм εDE не включав градієнтну мутацію.

Таблиця 1 – Результати дослідження

Алгоритм	Успішність (%)	Середній час виконання (с)	Стандартне відхилення часу виконання (с)
лише SCIP	100	58,22	0,24
алгоритм еволюційних центрів (ECA) [5]	100	29,81	7,20
диференціальна еволюція (DE) [6]	99	112,48	12,71
метод рою часток (PSO) [7]	15	44,71	20,32
алгоритм гравітаційного пошуку (CGSA) [8]	11	73,93	42,55
алгоритм оптимізації за допомогою китів (WOA) [9]	0	49,46	11,98
генетичний алгоритм (GA) [10]	94	1025,69	27,97
ε-обмежена диференціальна еволюція (εDE) [11]	100	112,31	13,12
генетичний алгоритм зі зміщеними випадковими ключами (BRKGA) [12]	0	6,29	1,95

Як показали результати експерименту, алгоритм еволюційних центрів (ECA) продемонстрував найкращу ефективність, стабільно знаходячи оптимальний результат і перевершуючи солвер SCIP за швидкістю у два рази завдяки паралелізації обчислень. Алгоритми диференціальної еволюції (DE та εDE), хоча й не перевершили SCIP, показали результат, близький до нього, із високим рівнем успішності. Генетичний алгоритм (GA), попри високий рівень успішності, виявився найповільнішим серед усіх розглянутих. Інші алгоритми лише зрідка знаходили оптимальний розв'язок.

Оскільки ефективність метаевристичних алгоритмів значною мірою залежить від їхніх параметрів і специфіки розв'язуваної задачі, некоректно було б однозначно стверджувати, що алгоритми з низьким рівнем успішності чи тривалим часом виконання є непридатними для оптимізації структури генеруючих потужностей електроенергетичних систем. Однак, хоча це дослідження не передбачало підбору оптимальних параметрів для кожного алгоритму, воно дозволило виділити найбільш перспективні алгоритми для розв'язання таких задач.

Таким чином, алгоритм еволюційних центрів продемонстрував найкращі результати, перевершивши солвер SCIP за швидкістю роботи. Алгоритми диференціальної еволюції також можуть бути ефективними за умови належного підбору параметрів або для задач іншої розмірності. Загалом, результати свідчать про перспективність метаевристичних алгоритмів у розв'язуванні задач оптимізації структури генеруючих потужностей електроенергетичних систем.

Крім пошуку ефективних методів підбору оптимальних параметрів для метаевристичних алгоритмів, подальші дослідження будуть спрямовані на масштабування комбінованого підходу, що інтегрує метаевристичні алгоритми та MILP-солвер, для виконання в середовищах із розподіленою оперативною пам'яттю. Особливу увагу буде приділено оцінці ефективності цього підходу для задач планування розвитку електроенергетичних систем, які мають більшу розмірність порівняно із задачами оптимізації структури генеруючих потужностей.

1. Hong, Y. Y., & Apolinario, G. F. D. (2021). Uncertainty in unit commitment in power systems: A review of models, methods, and applications. *Energies*, *14*(20), 6658.
2. Rahmaniani, R., Crainic, T. G., Gendreau, M., & Rei, W. (2017). The Benders decomposition algorithm: A literature review. *European Journal of Operational Research*, *259*(3), 801-817.
3. Mejía-de-Dios, J. A., & Mezura-Montes, E. (2022). Metaheuristics: A Julia package for single-and multi-objective optimization. *Journal of Open Source Software*, *7*(78), 4723.
4. Bolusani, S., Besançon, M., Bestuzheva, K., Chmiela, A., Dionísio, J., Donkiewicz, T., ... & Xu, L. (2024). The SCIP Optimization Suite 9.0. *arXiv preprint arXiv:2402.17702*.
5. Mejía-de-Dios, J. A., & Mezura-Montes, E. (2019). A new evolutionary optimization method based on center of mass. *Decision Science in Action: Theory and Applications of Modern Decision Analytic Optimisation*, 65-74.
6. Price, K. V. (2013). Differential evolution. In *Handbook of optimization: From classical to modern approach* (pp. 187-214). Berlin, Heidelberg: Springer Berlin Heidelberg.
7. Kennedy, J., & Eberhart, R. (1995, November). Particle swarm optimization. In *Proceedings of ICNN'95-international conference on neural networks* (Vol. 4, pp. 1942-1948). IEEE.
8. Mirjalili, S., & Gandomi, A. H. (2017). Chaotic gravitational constants for the gravitational search algorithm. *Applied soft computing*, *53*, 407-419.
9. Mirjalili, S., & Lewis, A. (2016). The whale optimization algorithm. *Advances in engineering software*, *95*, 51-67.
10. *Just another Genetic Algorithm Framework*. Metaheuristics.jl. https://jmejia8.github.io/Metaheuristics.jl/stable/algorithms/#GA.
11. Takahama, T., & Sakai, S. (2010, July). Constrained optimization by the ε constrained differential evolution with an archive and gradient-based mutation. In *IEEE congress on evolutionary computation* (pp. 1-9). IEEE.
12. Gonçalves, J. F., & Resende, M. G. (2011). Biased random-key genetic algorithms for combinatorial optimization. *Journal of Heuristics*, *17*(5), 487-525.

К.В. Таранець, О.І. Тесленко

МОДЕЛЮВАННЯ ЗМІН ЕЛЕКТРОСПОЖИВАННЯ ПРИ ДЕКАРБОНІЗАЦІЇ СТАЛЕЛИВАРНОГО ВИРОБНИЦТВА

Сталеливарне виробництво (СВ) відноситься до найбільш енергоємних галузей промисловості із значними обсягами викидів парникових газів (ПГ) в світі та в Україні: до 7% загальносвітових викидів ПГ продукується при виробництві чавуну та сталі, а в Україні цей показник досягає 14% (або майже 57% щорічних викидів ПГ в промисловості країни) [1, 2]. Вуглецеємність викидів ПГ при традиційних технологіях СВ варіюється від 1,37 до 2,3 т $CO_{2\text{-екв}}$/т сталі. В перспективі передбачається зниження цього показнику майже до нуля із використанням відновлювальних джерел енергії (ВДЕ) та інноваційних технологій СВ.

Перспективний прогноз декарбонізації СВ України, історично орієнтованого на переробку руд Криворізького залізорудного басейну, передбачає поступову заміну традиційної аглодоменної технології СВ з застосуванням кисневого конвертора (АД+КК) на технологію прямого відновлення заліза воднем і з використанням електродугової сталеплавильної печі (H_2+ЕП) (рис.1). В якості варіанту проміжної (перехідної) технології в процесі цієї заміни може використовуватись аглодоменна технологія виробництва сталі із застосуванням електродугової сталеплавильної печі (АД+ЕП).

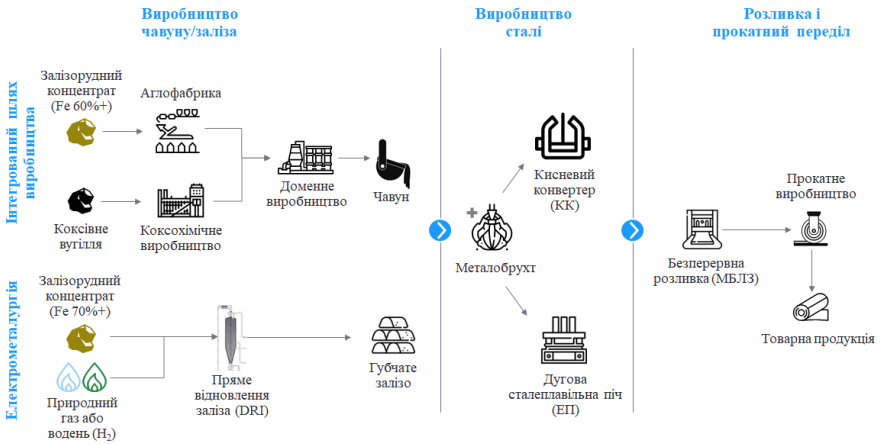


Рисунок 1 – Шляхи технологічної декарбонізації сталеплавильного виробництва

Застосування новітніх технологій потребуватиме значних обсягів електроенергії для забезпечення основних технологічних процесів: електролізу водню, прямого відновлення заліза воднем та плавлення сталі в

електродугових печах. Фактично передбачається електрифікація СВ. Моделювання змін енергоспоживання внаслідок процесу технологічної декарбонізації СВ є предметом даного дослідження.

Розрахункова модель визначення змін споживання електроенергії та викидів ПГ для варіативних співвідношень часток виробництва сталі з використанням різних технологій в процесі декарбонізації СВ застосовує наступні математичні залежності.

Загальне річне споживання електроенергії $E^{заг}$ при виробництві сталі з використанням кількох технологій

$$E^{заг} = \sum_{j=1}^{J} e_j^{ел} \cdot b_j \cdot C^{заг}, \text{ млрд кВт·год/рік;} \quad (1)$$

де j, J – порядковий номер j та загальна кількість J використаних технологій виробництва сталі, одиниць;

$e^{ел}_j$ – питоме електроспоживання при виробництві сталі за технологією j, кВт·год/т сталі;

$b_j = C_j/C^{заг}$; $\Sigma b_j = 1$ – частка виробництва сталі з використанням технології j в загальному річному виробництві сталі,-;

C_j –· річне виробництво сталі з використанням технології j, млн. т/рік;

$C^{заг}$ –·загальне річне виробництво сталі з використанням технологій J, млн. т/рік.

Потужність електрогенерації $P^{ст}$ для забезпечення потреб СВ

$$P^{ст} = \frac{E^{заг}}{1000 Д \cdot Г} \cdot \frac{k_{нв} \cdot k_з}{(1-k_{тр})}, \text{ ГВт;} \quad (2)$$

де $k_{нв}$ – коефіцієнт неврахованих витрат електроенергії при виробництві сталі, -;

$k_{тр}$ – коефіцієнт врахування втрат електроенергії при її транспортуванні до металургійних підприємств, -;

$k_з$ – коефіцієнт нерівномірності споживання електроенергії при виробництві сталі, -;

$Д = 365$ – кількість діб в році, діб/рік;

$Г = 24$ – кількість годин в добі, год/добу.

Загальні річні обсяги викидів парникових газів $G^{заг}$ при виробництві сталі з використанням кількох технологій

$$G^{заг} = \sum_{j=1}^{J} g_j^{пг} \cdot b_j \cdot C^{заг}, \text{ млн т } CO_{2\text{-екв}}\text{/рік;} \quad (3)$$

де $g^{пг}_j$ – питомі обсяги прямих технологічних викидів ПГ, а також непрямих викидів ПГ, пов'язаних з генерацією електроенергії, споживаної при СВ за технологією j, т $CO_{2\text{-екв}}$ /т сталі;

інші позначення згідно з формулою (1).

Як вихідні дані розрахункового моделювання була використана інформація щодо питомого електроспоживання при виробництві сталі за різними технологіями та питомих обсягів технологічних викидів ПГ, що супроводжують ці технологічні процеси, наведених в [3].

Результати варіантного моделювання для сталеливарного виробництва 10 млн т сталі на рік демонструють (рис.2), що внаслідок загального переходу на електролізну технологію отримання водню, технологію прямого відновлення заліза та електродугову сталеплавильну технологію електроспоживання зросте з 2,74 млрд кВт·год/рік до 35,13 млрд кВт·год/рік (в 12,84 рази) порівняно із традиційною аглодоменною технологією виробництва сталі з застосуванням кисневого конвертора. Результати розрахунків також вказують на необхідність зростання встановленої генерації електроенергії з 0,48 ГВт до 6,15 ГВт (еквівалент загальної потужності Запоріжської АЕС). Зважаючи на безперервний технологічний процес виробництва сталі, на поточний стан розвитку енергетичної системи України таку потужність електрогенерації здатні гарантовано забезпечити тільки атомні електростанції.

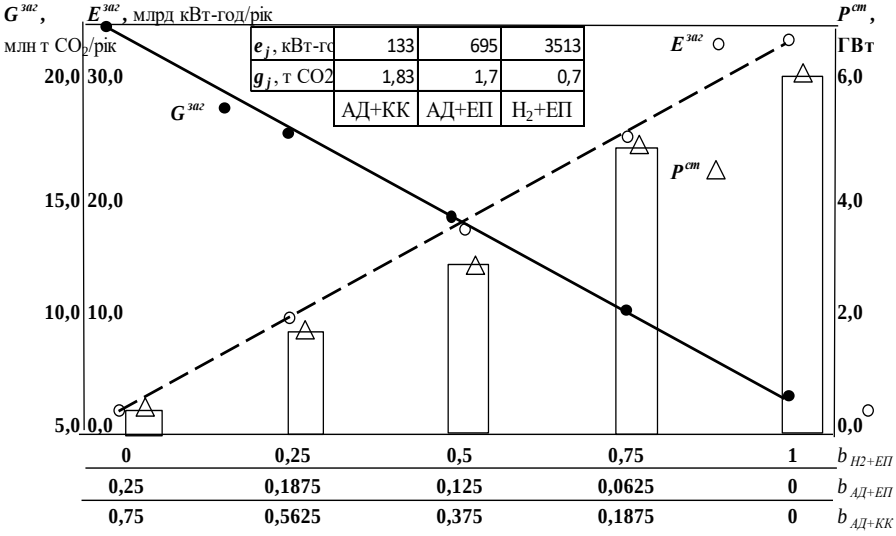


Рисунок 2 – Зміна електроспоживання, потреби в потужності електрогенерації та викидів парникових газів при декарбонізації сталеливарного виробництва (10 млн т сталі/рік)

Викиди ПГ внаслідок такої технологічної декарбонізації СВ зменшиться з 17,98 млн т CO_2-екв/рік до 7,0 млн т CO_2-екв/рік (тобто в 2,57 рази).

На рис. 3 наведена структура електрогенерації в Україні на ринку на ринку «на добу наперед» (РДН) протягом 2023 року за джерелами походження електроенергії. Як видно, вуглецевонейтральна електрогенерація (атомні електростанції та з відновлювальних джерел енергії (ВДЕ)) на поточний час в Україні складає приблизно 50…65%, з яких 25…45% є елекрогенерація з ВДЕ [4].

В перспективі можуть бути закладені припущення в моделі щодо досягнення нульових значень викидів ПГ внаслідок перманентного застосування технологій електрогенерації з ВДЕ – сонячних, вітрових та гідравлічних електростанцій. Однак зважаючи на стохастичний (мінливий) характер електрогенерації сонячними та вітровими електростанціями, забезпечення безперервного та стабільного постачання електроенергією в таких обсягах її потужності для потреб СВ в умовах українського ринку електроенергії є завданням найближчих десятиліть.

Рисунок 3 – Структура електрогенерації в Україні протягом 2023 року за джерелами походження електроенергії

1. Decarbonization Pathways for Steel and Cement Industries. URL: https://cdn.ihsmarkit.com/www/ pdf/0622/Infographic---Decarbonization-Pathways-for-Steel-and-Cement-Industries.pdf.
2. WorldSteel Sustainability Indicators 2023 report. URL: https://worldsteel.org/steel-topics/sustainability/sustainability-indicators-2023-report/.
3. Guevara Opinska, L., et Al. 2021, Moving towards Zero-Emission Steel, Publication for the committee on Industry, Research and Energy (ITRE), Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg. URL: https://www.europarl.europa.eu/committees/en/supporting-analyses/sa-highlights.
4. Інформація про обсяги та частку кожного джерела енергії, використаного для виробництва електричної енергії, проданої на ринку «на добу наперед» та/або внутрішньодобовому ринку за січень-грудень 2023 року. URL: https://www.oree.com.ua/index.php/web/55.

Н.Ю. Майстренко

ПОПИТ НА ЕЛЕКТРОЕНЕРГІЮ В ПЕРСПЕКТИВІ ПОВОЄННОЇ ВІДБУДОВИ ЕКОНОМІКИ УКРАЇНИ

При прогнозуванні попиту на електроенергію використовуються показники за групуванням за даними статистики: Населення та міграція; Макроекономічна статистика, національні рахунки; Діяльність підприємств; Послуги; Внутрішня торгівля; Капітальні інвестиції; Основні засоби; Сільське, лісове та рибне господарство; Енергетика; Промисловість; Будівництво; Транспорт; Туризм.

Основні підходи до проведення оцінок статистичних показників за відсутності даних. Відомо, що частина статистичних даних, що використовуються при розрахунку попиту на електроенергію та на паливно-енергетичні ресурси загалом відсутні, тому, залежно від методології проведення державних статистичних спостережень та здійснення розрахунків статистичних показників для проведення відповідних оцінок за відсутності даних у межах України та її регіонів застосовують такі основні підходи: компенсація даних на мікрорівні; коригування даних на макрорівні; використання наявних адміністративних даних із відкритих джерел та оцінок аналогічних показників іншими органами державної влади.

Для проведення оцінок статистичних показників за відсутності даних у межах України та її регіонів можуть використовуватися відповідні зведені дані: за попередній звітний період; за відповідний період попереднього року; за відповідний період за ряд попередніх років; за поточний звітний період у межах України та її регіонів з повним обсягом даних. Статистичні показники які потребують оцінки, аналізують у взаємозв'язку з відповідними даними в межах України та її регіонів, основні характеристики яких близькі до характеристик оцінюваного регіону.

Валовий внутрішній продукт виробничим методом та валова додана вартість за видами економічної діяльності прогнозуються з урахуванням даних рейтингових агентств: Bloomberg, Standart@Poor , Moodys; провідних фінансових установ США, Європи: МВФ, Світовий Банк, Європейський банк реконструкції та розвитку, фінансових установ України: Національний банк, Міністерство економіки, приватні фінансові організації, банки (Dragon capital) та ін., українських рейтингових агентств, опитування молодих фінансистів, що працюють в провідних банках України. Сьогодні найточніші дані надають міжнародні розвідки: MI6 (Великобританія), МОССАД (Ізраїль).

За доступними даними Державної служби статистики базовим роком дослідження вибраний 2020 р., останній, за який є відкриті дані. На наступному етапі визначаються можливі обсяги енергозбереження. Спочатку необхідно визначити технологічний потенціал енергозбереження на підприємстві, потім структурний потенціал енергозбереження – від

міжсекційних та внутрішньосекційних структурних зрушень. (Необхідно тут врахувати, що ЄБРР планує інвестувати в Україну до 10 млрд євро протягом наступних 5 років).

На черговому етапі прогнозування за прогнозом ВВП, валової доданої вартості (ВДВ) секцій економіки, енергоємності цих секцій, з врахуванням потенціалу енергозбереження проводиться розрахунок прогнозу обсягів споживання на рівні країни, секцій економіки, окремих енергоємних виробництв. Для прогнозу споживання населення використовується окрема методика. Також для прогнозу враховуються можливості експорту та імпорту електроенергії для потреб споживачів та втрати в магістральних електромережах. Розрахунок представлено в табл.1 за консервативним сценарієм з щорічним зростанням економки до 2,5% та закінченням активної фази бойових дій до кінця 2025 року.

Таблиця 1 – Прогноз попиту на електроенергію в Україні до 2030 року

Показники	2022 (факт)	2023 (факт)	2024 (очікуване)	2025	2030
Прогноз ВВП у цінах 2016 р., млрд грн	1841,9	1878,7	1925,7	1973,8	2233,2
Валове споживання електроенергії по електроємності ВВП 2022 р., млн кВт·год	106200	102507	84000 - 90560	95000 - 100800	111780 - 118600
Всього валове споживання електроенергії (брутто), млн кВт·год	127440	123000	100800 - 108670	114000 - 121000	134140 - 142320

Отже, попит на електроенергію в Україні за консервативним сценарієм розвитку економіки разом з населенням в 2030 році не перевищить 118,6 млрд кВт·год, а з урахуванням втрат в мережах – 142,3 млрд кВт·год.

1. Державна служба статистики. URL: ukrstat.gov.ua.

Д.В. Кулида

ТЕПЛОВІ НАСОСИ ТА ГІБРИДНІ PVT ПАНЕЛІ: ІННОВАЦІЙНИЙ ПІДХІД ДО ЕНЕРГОЗАБЕЗПЕЧЕННЯ ДЛЯ ПРИВАТНОГО СЕКТОРУ

Енергетична система України зазнала значних викликів внаслідок війни. Втрата частини генеруючих потужностей, руйнування електромереж та зростаючі потреби в енергоресурсах посилюють проблему енергозабезпечення. Внаслідок атак на енергетичну інфраструктуру Україна втратила значну частину своїх генеруючих потужностей. Ситуація загострюється в зимовий період через високий попит на опалення, що значно збільшує навантаження на енергосистему.

Одним із рішень цієї проблеми є підвищення енергоефективності приватних домогосподарств через впровадження сучасних технологій, таких як теплові насоси (ТН) у поєднанні з гібридними сонячними панелями. Це дозволить не лише зменшити споживання енергії, але й підвищити стійкість до енергетичних криз.

Стан приватного сектору

В Україні налічується близько **14,7 млн домогосподарств**, з яких понад **60%** використовують викопне паливо чи електроенергію для опалення. Близько **20% домогосподарств** застосовують електронагрівачі, що створює пікове навантаження на мережу в зимовий період.. Середнє споживання електроенергії для опалення становить **4000–5000 кВт·год на рік**, а викиди CO_2 від таких систем досягають **2–3 тонн на рік [1]**.

Використання теплових насосів для опалення, гарячого водопо- стачання і т.п., являє собою спосіб, альтернативний іншим способам, таким, як традиційне спалювання органічного палива, широко поширене центральне парове чи водяне опалення, електрообігрів та інше [2].

Гібридні сонячні панелі з теплообмінником: ефективне рішення

Гібридні панелі оснащені теплообмінником, який відводить надлишкове тепло від сонячних панелей, знижуючи їхню температуру. Це підвищує ефективність ФВ-панелей на **5–10%**. Зібране тепло передається до теплового насоса, який використовує його для підігріву води або опалення приміщення [3].

Що стосується фотоелектричної технології, то доведено, що охолодження робочої поверхні є ключовим експлуатаційним фактором, який необхідно враховувати для досягнення більшої ефективності. Належне охолодження може підвищити електричну ефективність і зменшити швидкість деградації фотоелементів з часом. Більше того, тепло, що відводиться системою охолодження, можна використовувати в побутових цілях.

У фотоелектричних системах лише 15-20% сонячної енергії, що падає на фотоелектричну панель, може бути перетворено в електрику, а решта перетворюється на тепло ця частина теплової енергії може бути використана для отримання теплового ефекту. Гібридна сонячна фотоелектрична і теплова енергія (PVT) - це технологія, яка об'єднує фотоелектричні панелі і компоненти відбору тепла в одному модулі [4].

Рисунок 1 – Гібридна PVT панель DUALSUN (Франція)

Можна виділити два основних типи PVT: PVT-колектори та PVT-панелі. PVT-колектори зовні дуже схожі на звичайний сонячний тепловий колектор, що складається з абсорбера, покритого фотоелектричним покриттям, в ізольованій колекторній коробці зі скляною кришкою. Така велика кількість ізоляції призводить до відносно високого теплового ККД за рахунок дещо меншого електричного ККД через додаткове віддзеркалення, яке вносить скляна кришка. З іншого боку, PVT-панелі зовні схожі на звичайні фотоелектричні панелі. Через відсутність додаткової ізоляції та скляного покриття PVT-панелі мають нижчу теплову ефективність, але вищий електричний вихід[6].

Поєднання PVT-колекторів і теплового насоса дає додаткову перевагу. Чисте електричне споживання енергії тепловим насосом може бути забезпечене за рахунок електричного виробництва PVT-модулів [6].

Висновок

Інтеграція теплових насосів із гібридними сонячними панелями є перспективним рішенням для підвищення енергоефективності приватних домогосподарств. Вона дозволяє знизити витрати на енергоресурси, скоротити викиди CO_2 та зменшити залежність від викопного палива. Для досягнення цих цілей необхідно розробити державні програми підтримки, модернізувати електромережі та забезпечити доступність технологій для населення.

1. Соціально-демографічні характеристики домогосподарств України URL:https://ukrstat.gov.ua/druk/publicat/Arhiv_u/17/Arch_cdhd_zb.htm.
2. Парокомпресійні теплонасосні установки в системах теплопостачання URL:http://ir.lib.vntu.edu.ua/bitstream/handle/123456789/3577/%d0%a2%d0%ba%d0%b0%d1%87%d0%b5%d0%bd%d0%ba%d0%be%20%d0%9e%d1%81%d1%82%d0%b0%d0%bf%d0%b5%d0%bd%d0%ba%d0%be%20%d0%bc%d0%be%d0%bd%d0%be%d0%b3%d1%80%d0%b0%d1%84%d1%96%d1%8f.PDF?sequence=1&isAllowed=y, https://dualsun.com/wp-content/uploads/dualsun-en-epd-spring4.pdf.
3. Energy analysis of a thermal system composed by a heat pump coupled with a PVT solar collector URL:https://www.sciencedirect.com/science/article/abs/pii/S0360544219303512.
4. Performance and costs of a roof-sized PV/thermal array combined with a ground coupled heat pump URL:https://www.sciencedirect.com/science/article/abs/pii/S0038092X04002853.
5. Analysis and optimization of a heat pump system coupled to an installation of PVT panels and a seasonal storage tank on an educational building URL:https://www.sciencedirect.com/science/article/abs/pii/S0378778820318788.

М.М. Середзинський, О.М. Діденко

БЕЗПЕЧНЕ ВИКОРИСТАННЯ ЛАМП ДНаТ

Освітлення відіграє велике значення у різних сферах сучасного мегаполісу. Це освітлення доріг та площ, промислових зон, великих магістралей, а також архітектурних об'єктів. У різних галузях життєдіяльності людини для освітлення застосовуються різноманітні джерела світла, різних модифікацій, форм, потужностей, різного спектрального складу.

Виходячи з дослідження параметрів багатьох сучасних джерел світла, можна відзначити їхнє раціональне застосування у всіх галузях життя. У таблиці 1 представлені основні характеристики розрядних ламп.

Таблиця 1 – Основні характеристики джерел світла

Тип джерела світла	Діапазон потужності, Вт	Світлова віддача, Лм/Вт	Термін служби, год.
Люмінесцентні лампи (ЛЛ)	18–80	70-80	6 000-15 000
Дугові ртутні лампи типу ДРЛ	50-1 000	50-55	10 000-15 000
Металогалогенні лампи типу (МГЛ)	125-3 500	65-80	300-10 000
Натрієві лампи типу ДНаТ	50-400	більше 100	6 000-12 000
Ксенонові лампи типу ДКст	10 000-55 000	30-50	300-800

Якщо розглядати основні напрями формування джерел світла, слід зазначити такі основні характеристики:

- збільшення світлової віддачі та тривалості горіння;
- компактність джерела світла;
- поліпшення та вдосконалення колірних характеристик;
- посилення екологічності при експлуатації та утилізації джерел світла.

Зараз в основному всі джерела світла високої інтенсивності, які використовуються для внутрішнього і зовнішнього освітлення, мають у своєму складі високотоксичну ртуть.

У разі руйнування колби ртуть може опинитися у навколишньому середовищі. Сама по собі ртуть у чистому вигляді має малу хімічну активність, майже не вступає в контакт з водою та солями, а також легко випаровується при кімнатній температурі, у зв'язку з цим простір руйнування такого джерела світла тривалий час буде джерелом зараження навколишнього середовища.

Тим не менш, є деякі умови розробки джерел світла високого тиску без застосування ртуті. У лампах ДНаТ світловий потік відтворюється за допомогою випромінювання парів натрію, які виходять з амальгами ртуті натрію [2].

Початок етапу виробництва натрієвих ламп розпочався з дослідження різних напрямів підвищення енергоефективності ртутних джерел світла.

Підсумком тривалих наукових досліджень була концепція, що пари будь-якого металу можна перетворити до стану світіння, складність полягала лише в тому, що лише деякі метали мають можливість перебувати в агрегатному стані. З них можна виділити ртуть, літій, калій та натрій. Натрій виявився переважно належним прикладним завданням освітлення, так як зміг відтворити світлову хвилю у жовтій зоні спектру (590 нм). На сьогоднішній момент джерела світла типу ДНаТ є досить енергоефективним джерелом, мають цілу низку переваг у порівнянні з іншими лампами. Наприклад, тривалий термін служби, високу світлову віддачу, стійкість світлотехнічних параметрів, надійність роботи тощо. У зв'язку з цим вони можуть знайти застосування у світлотехнічних системах загального призначення, а також у спеціальних опромінювальних установках різного призначення.

Сучасна концепція вуличного освітлення у всіх населених пунктах, а особливо у великих мегаполісах є досить складним завданням, не тільки з енергоефективності, а й з інженерних питань. У зв'язку з цим процеси модернізації міських світлових систем є дуже значущими і налаштованими на конкретний економічний результат [3].

Найголовнішим чинником енергоефективності у світлотехнічних установках це заміна застарілих джерел світла на сучасні, енергоекономічні лампи та освітлювальні прилади. Застосування натрієвих ламп дозволяє мати достатній ряд переваг, насамперед економічність, а також обмеження забрудненням вуглекислим газом.

В наш час відбувається загальна трансформація на використання у освітленні вулиць, магістралей та доріг, натрієвих ламп високої інтенсивності, які дозволяють відчутно знизити рівень світлового забруднення та покращити освітлення міста.

Удосконалення вуличного міського освітлення повинно включати застосування освітлювальних приладів з лампами ДНаТ з поліпшеними світлотехнічними параметрами на зміну досить застарілих світлових приладів з лампами типу ДРЛ.

Великі переваги в галузі використання ламп ДНаТ відбуваються через відмову від застосування ртуті, а також поліпшення характеру передачі кольору цих джерел світла.

1. Гуракова Л.Д., Суворова К.І., Баландаєва Л.Г. Методичні рекомендації до виконання лабораторних робіт з навчальної дисципліни «Джерела світла» (для студентів денної і заочної форм начання спеціальності 141 – Електроенергетика, електротехніка та електромеханіка. Харків : ХНУМГ, 2020. с.48.
2. Литвиненко А. С., Черкашина О.Л. Світлові прилади : навч. посіб. Харків : ХНУМГ ім. О.М. Бекетова, 2015. 125 с.
3. Електричне освітлення: навч. посіб. / О. І. Соловей, А. В. Чернявський, О. О. Ситник, В. Ф. Ткаченко. Київ, 2014 . 59 с.

Д.О. Маслов, О.М. Діденко

РОЗРОБКА СВІТЛОВОЇ РЕКЛАМИ В ЕПОХУ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Зовнішня реклама вважається одним із найдавніших видів реклами, але вона досі не втратила своєї актуальності, як досить ефективний маркетинговий інструмент.

Ще в давнину торговці придумали розписувати стіни, щоб розповісти городянам про свої товари чи послуги. Із тих часів зовнішня реклама стала важливим атрибутом успішного бізнесу. Розміщення зовнішньої реклами займає чільне місце у рекламної структурі, що з особливостями впливу такого виду реклами на суспільство. Носії зовнішньої реклами формувалися протягом кількох століть, змінювалися технології, дизайн зовнішньої реклами, але залишалися постійними методи впливу на аудиторію.

Щоб реклама приносила користь, вона повинна мати у своїй основі самобутню ідею, яскравий, сучасний дизайн, відповідати запитам цільової споживчої аудиторії. Тому ця тема є досить актуальною в наш час.

Прикладом сучасної світлової реклами в житті міста є Таймс-сквер або яскраві вулиці в Токіо.

Максимальну яскравість можна визначити, як габаритну для гранично яскравих ділянок площею 0,2х0,2 м як у рекламних панелях, де світлодіоди розміщені всередині та закриті світлорозсіючими матеріалами, так і в рекламних щитах, освітлених зовні освітлювальними приладами.

Для того щоб обмежити сліпучу дію і світлових перешкод водіям від вивісок і плакатів, що світяться, розташованих над проїзною частиною або поперек її осі на відстані не більше 2 м від лицьової грані бардюрного каменю, необхідно вжити таких заходів:

- прямий світловий потік освітлювальних пристроїв, що висвітлює об'єкт зовні, не повинен виходити за межі його поверхні;

- рекламні панелі, що мають ділянки поверхні більше 0,04м^2 насиченого зеленого або червоного кольору яскравістю вище 150 кд/м^2, повинні розташовуватися поблизу перехресть на висоті не менш 6 м від проїзної частини.

На вулицях усіх категорій установки зовнішнього освітлення всіх видів не повинні утворювати на вікнах житлових будинків вертикальне освітлення, яке перевищує:

- 7 лк при нормі середньої горизонтальної освітленості проїзної частини 10 лк;

- 10 лк при нормі середньої горизонтальної освітленості 15 лк;

- 20 лк при нормі середньої горизонтальної освітленості 20 лк і більше.

Рекомендована та гранично допустима середня яскравість, а також максимально допустима яскравість окремих ділянок рекламних панелей та щитів залежно від їх площі та розташування зазначені в ДБН.

В роботі були зроблені розрахунки та визначені розміри лайтбоксу: висота 6м, ширина 19м, глибина 0,6м;

Для підсвітки лайтбоксу планується використовувати світлодіоди Cree 61258-A-3.5W. Загальною кількісттю 570шт (285шт на кожний бік) потужністю 3,5 Вт;

Загально висота рекламної конструкції становить 13м;

Скориставшись комп'ютерною програмою DIALux було зроблено візуалізацію розроблена рекламна установка, яка наведена на рисунку 1. Потужність рекламної установки становить 2,1 кВт.

Рисунок 1 – Візуалізація рекламної установки

Отже, при проєктуванні світлової реклами необхідно пам'ятати та звертати увагу на місце встановлення та нормативні значення щодо освітленості і яскравості яку буде створювати світлова реклама та чи відповідає вона нормативним значенням.

1. Чирчик С. В. Світлодизайн: навч. посібник. Київ : ДП Персонал, 2018. 160 с.
2. Лісна О. І. Декоративно-художнє освітлення архітектурного середовища: навч. посібник. Харків : ХНАМГ, 2010. 275 с.
3. ДБН В.2.5 – 28 – 2018. Природне і штучне освітлення. На заміну ДБН В.2.5-28-2006; Чинний від 2019-03-01. Вид. офіц. Київ : УкрНДНЦ, 2018. 76 с.

В.В. Вітер, О.М. Діденко

ЛЮМІНЕСЦЕНТНІ ЛАМПИ ТА ЗОРОВИЙ КОМФОРТ ПРАЦІВНИКІВ В ОФІСІ

Робота в житті людини відіграє важливу роль для неї. Про це нам нагадує Конституція України Стаття 43 - «Кожен має право на працю, що включає можливість заробляти собі на життя працею, яку він вільно обирає або на яку вільно погоджується. Кожна людина має право на працю» [1]. Людина працює та мешкає у тісному взаємозв'язку з навколишнім середовищем.

Світло є найважливішим з усіх видів енергії, яку люди можуть використовувати. Воно є ключовим елементом нашої здатності бачити. Допомагає оцінювати форму і колір предметів, що оточують нас у повсякденному житті. Велику частину інформації, яку ми отримуємо через наші органи чуття, надходить до нас через світло, приблизно 80%. Хотілось би звернути увагу, що душевний стан людини або ступінь втоми залежать від освітлення і кольору навколишніх предметів. Приблизно 9,5 років життя людина витрачає на роботу, це за умови 40 годинного робочого тижня але робота займає набагато більше заявлених годин, відповідно цей час ми проводимо в приміщенні де є штучне освітлення [2-4]. В офісних приміщення спостерігається тенденція, щодо недоосвітленості робочих місць, що призводить до порушення зору працівників. Може на початку експлуатації спроєктована система освітлення і відповідала нормам з освітленості, але з часом світильники постаріли і погіршилися їх світлотехнічні характеристики та все одно залишаються у використанні. Тому вони продовжують впливати на зоровий комфорт працівників.

Знаючи комплекс параметрів джерел світла можна виділити деякі технічні характеристики, які негативно впливають на зоровий комфорт працівників:

- до перенапруження очей і швидкої стомленості призводить недостатній рівень освітленості на робочому місці;
- негативний вплив на зоровий комфорт працівників, чинить коефіцієнт пульсації освітлювальних приладів;
- надмірна яскравість та наявність відблисків можуть викликати головний біль, відчуття дискомфорту та негативно позначитись на загальному стані нервової системи людини.

Сучасні офіси вже будують з розрахунком освітлюваної мережі яка базується на використанні світлодіодних освітлювальних установок, але не всі офіси нові, і не у всіх застосовуються сучасне світлотехнічне обладнання. Більшість офісів використовують для освітлення люмінесцентні лампи, які в свою чергу можуть давати недостатній рівень освітленості та створювати підвищений коефіцієнт пульсації.

Якісна робота люмінесцентних ламп пов’язана з правильно підібраним баластним опіром, засвічуючим елементом та компенсуючим елементом [6].

Тому, напрямок робот стало, дослідити, як же впливає тип баластного опору на роботу люмінесцентної лампи, на освітлення.

Було з'ясовано, що найкращі умови та рівномірний світловий потік досягається при використанні індуктивно-ємінсного баласту. Активний баласт, взагалі, не можливо було дослідити, тому що він створював стробоскопічний ефект.

Для подальшого аналізу було змодельовано офіс з люмінесцентними світильниками. За результатами моделювання було з'ясовано, що такі ЛЛ створюють освітленість від 150 до 340 лк, в порівнянні з нормами для офісу цих значень не достатньо. Тому наступним кроком стала, умовна заміна ЛЛ на світлодіодні. В результаті були отримані нові рівні освітлюваності від 400 до 555 лк, коефіцієнт засліплення 17.

Виходячи з вище сказаного, можна запропонувати рекомендації для створення зорового комфорту, а саме:

- застосовувати розсіяне рівномірне світло;

- використовувати світлодіоди високої якості, для усунення мерехтіння, саме воно створює шкідливий вплив на сітківку ока людини;

- для офісного освітлення радять використовувати “нейтральне та біле” світло, це сприяє підвищенню працездатності працівників і зменшую втому очей;

- правильно встановлювати світлові прилади, так, щоб вони не створювали засліплення і відблисків від техніки і меблів.

1. Конституція України : від 28.06.1996 р. : станом на 01 січ. 2006 р. Київ : Ін Юре, 2006. 144 с.
2. Скільки часу з життя ми витрачаємо на звичні і неминучі речі? ТурБаза. URL: https://tourbaza.com/skilki-chasu-mi-vitrachayemo-na-rechi/.
3. Сучасні тенденції облаштування офісу. Гіпермаркет Метбів. URL: https://aklas.ua/ua/article/suchasni-tendentsii-oblashtuvannya-ofisu.
4. Work – light for offices. Principles of planning and design. ERCO. URL: https://www.erco.com/en/service/light-for-flexible-office-layouts-7216.
5. echnical Committee CEN/TC 169 “Light and lighting”. (б. д.). Light and lighting. Lighting of work places - Indoor work places (BS EN 12464-1:2011). https://knowledge.bsigroup.com/products/light-and-lighting-lighting-of-work-places-indoor-work-places?version=standard.
6. Шепілко, Є. (2013). Електротехнічні пристрої світлотехнічних систем. ХНАМГ.

В.А. Герасименко, С.М. Власенко, О.В. Дорошенко

АДАПТИВНА СИСТЕМА ОСВІТЛЕННЯ ДЛЯ АВТОМОБІЛІВ

Питання оптимального освітлення простору руху залишається актуальним для автомобільної світлотехніки протягом багатьох років. З однієї сторони, дорога та навколишній простір повинні бути освітлені якомога яскравіше, щоб водій міг чітко розпізнавати об'єкти. З іншої сторони, важливо уникати засліплення інших учасників руху та самого водія. Максимально якісне балансування або навіть вирішення конфлікту між ефективним освітленням і мінімізацією засліплення є основним завданням науковців та інженерів у галузі світлотехніки.

Класичним рішенням цього питання є перемикання між дальнім та ближнім світлом. Дальнє світло фар забезпечує оптимальний розподіл світла для освітлення дороги, тоді як ближнє світло є, так би мовити, компромісним варіантом для запобігання засліпленню [1]. Проте з точки зору сучасних технологій, для забезпечення безпеки під час руху вночі це не є оптимальним варіантом [2]. Просте й очевидне рішення покращення освітлення для умов поганої погоди полягає у використанні спеціальних додаткових фар, таких як протитуманні фари, які водій може вмикати або вимикати залежно від ситуації.

Наступним кроком є інтеграція цих додаткових функцій освітлення не в окремі додаткові фари, а в основні фари автомобіля з автоматичним перемиканням між відповідними режимами розподілу світла. Це і є основною концепцією систем AFS (Advanced Frontlighting System). У системі AFS розроблена динамічна система освітлення, яка залежно від швидкості та кута повороту керма забезпечує оптимальне освітлення дорожнього полотна. Для її реалізації необхідний проекційний модуль VarioX® із обертовим валиком, розташованим між джерелом світла та лінзою (рис. 1). Завдяки кроковому двигуну валик може займати потрібне положення за кілька мілісекунд [1].

Рисунок 1 – Зовнішній вигляд поворотного модуля VarioX®

У режимі міського освітлення фар, який активується на швидкості до 50 км/год, горизонтальна світлотіньова межа запобігає засліпленню інших

учасників дорожнього руху. Крім того, розширене освітлення ближньої зони забезпечує своєчасне виявлення пішоходів на узбіччі дороги. На швидкості між 50 і 120 км/год активується шосейне освітлення, яке можна порівняти з традиційним розподілом ближнього світла. Модуль VarioX® створює асиметричний розподіл світла, що дозволяє уникнути засліплення зустрічних учасників руху. Світлотіньова межа піднімається, щоб краще освітлювати лівий край дорожнього полотна та забезпечувати більшу дальність освітлення. На швидкості понад 100 км/год активується режим освітлення для автомагістралі. Розподіл світла налаштований таким чином, щоб забезпечити оптимальну дальність освітлення для великих радіусів повороту під час руху на високій швидкості. Динамічне адаптивне освітлення також є складовою частиною системи AFS. Залежно від кута повороту керма, фари можуть повертатися на кут до 15°, забезпечуючи таким чином оптимальне освітлення поворотів. За допомогою режиму освітлення для несприятливих погодних умов забезпечується більш широке розсіювання світла, що покращує видимість під час дощу, туману або снігу. Однак, щоб зменшити засліплення для самого водія, знижується інтенсивність освітлення зони дальнього поля. Адаптація розподілу світла системи AFS (рис. 2) здійснюється в залежності від швидкості автомобіля, типу дороги та погодних умов, що є значним покращенням традиційної автомобільної світлотехніки.

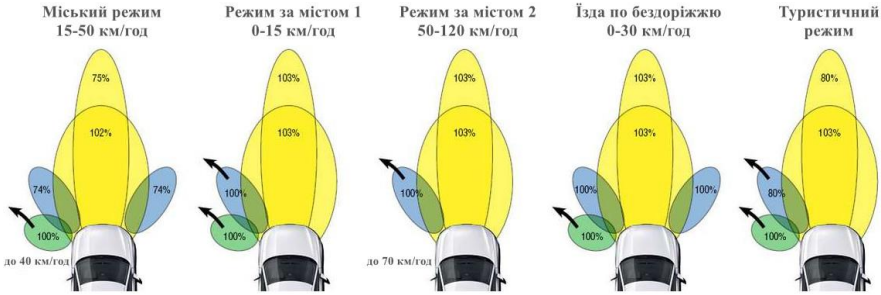


Рисунок 2 – Основні режими освітлення автомобільної системи AFS

Модернізацією системи AFS зі статичним розподілом світла є поєднання цієї системи з камерою та відповідною системою обробки зображень. Першим кроком до цього є адаптивна світлотіньова межа (aHDG) [1].

За допомогою камери на лобовому склі розпізнаються зустрічні автомобілі, або ті, що рухаються попереду, і фари регулюються таким чином, що світловий конус закінчується перед іншими автомобілями (рис. 3). Завдяки цьому дальність ближнього світла може бути збільшена з 65 метрів до 200 метрів (лінія 3 люкс). Якщо ділянка дороги вільна, система перемикається на дальнє світло, забезпечуючи водію оптимальну видимість у

будь-який час. Регулювання можливого діапазону дії фар базується на контролі рівня засліплення інших учасників дорожнього руху. Таким чином, виключається небажане засліплення, і забезпечується максимальний розподіл ближнього світла.

Рисунок 3 – Порівняння традиційної та адаптивної систем фронтального освітлення автомобільних фар

Наступною корисною інновацією є система неосліплюючого дальнього світла ADB (Adaptive Driving Beam), що базується на принципі постійно увімкненого дальнього світла, яке запобігає засліпленню інших учасників руху [3]. Система, що складається з фронтальної камери, потужного програмного забезпечення та інтелектуальної світлотехніки, автоматично затемнює ті області простору, які могли б заважати іншим учасникам руху. Це дає можливість завжди використовувати дальнє світло під час руху вночі. При виявленні камерою інших учасників руху в просторі, зона, в якій знаходиться виявлений учасник, автоматично затемнюється в розподілі дальнього світла. При цьому цей затемнений сектор може динамічно слідувати за виявленим учасником руху. Реалізація неосліплюючого дальнього світла здійснюється за допомогою спеціальної бокової поверхні обертового валика в проекційному модулі VarioX®. На основі обробки зображень та інтелектуальних налаштувань, зустрічний транспорт шляхом усунення небезпечних для засліплення ділянок виводиться з розподілу дальнього світла. Для водія зберігається розподіл дальнього світла, що порівняно з традиційними системами означає значне збільшення дальності видимості.

Завдяки стрімкому розвитку LED технологій, популярність адаптивних систем освітлення зростає, сприяючи подальшому покращенню якості та безпеки автотранспорту. Як джерело світла для будь-якої форми «активних» систем фар широке впровадження отримали світлодіодні матриці (рис. 4). Вони складаються з великої кількості (> 10) індивідуально адресованих білих

високопотужних світлодіодів. Включення світлодіодного кристалу за допомогою широтно-імпульсної модуляції забезпечує не тільки цілеспрямоване вмикання та вимикання окремих кристалів, що забезпечує модуляцію геометрії світлотіньової межі, але й модуляцію інтенсивності розподілу світла. Поряд з реалізацією функцій AFS освітлення без механічних елементів, світлодіодні матриці в поєднанні з передовою сенсорною технологією також пропонують можливість реалізації «активних» варіантів розподілу світла, наприклад, неосліплюючого дальнього світла [1] (рис. 4).

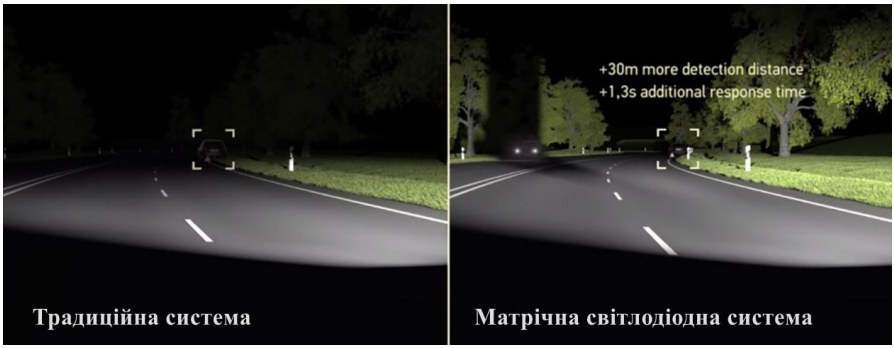


Рисунок 4 – Порівняння традиційної та матричної світлодіодної системи фронтального освітлення автомобільних фар

Вже зараз застосування світлодіодних матричних фар дає можливість цілеспрямованого освітлення об'єктів, наприклад, дітей, які грають на узбіччі дороги. Таким чином, увага водія своєчасно привертається до цих джерел небезпеки, що дозволяє забезпечити більш ранню реакцію на них.

У процесі розвитку інтелектуальних систем освітлення автомобільні фари перестають бути продуктом, який виконує лише базові функції відповідно до інженерних налаштувань. Вони мають адаптуватися до мінливих дорожніх та погодних умов і різноманітних сценаріїв водіння. В епоху штучного інтелекту можливим стане також інтегрування збережених даних про водіння для більш точного визначення кутів налаштування фар. Такий підхід забезпечить більш високу точність і контрольованість, що дозволить ще більше покращити безпеку дорожнього руху.

1. Hella Automotive Lighting. URL: https://www.hella.com/techworld/us/Technical/Automotive-lighting-209/ (дата звернення: 15.11.2024).
2. The Dangers of Overly Bright Headlights at Night. URL: https://ndakotalaw.com/the-dangers-of-overly-bright-headlights-at-night (дата звернення: 15.11.2024).
3. Snehal G. Magar, "Adaptive Front Light Systems of Vehicle for Road Safety" 2015 International Conference on Computing Communication Control and Automation, pp. 551-554 (IEEE 2015).

В.А. Герасименко, В.В. Сухов

УДОСКОНАЛЕННЯ СВІТЛОТЕХНІЧНИХ РІШЕНЬ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ ДОРОЖНЬОГО РУХУ В НІЧНИЙ ЧАС

У багатьох містах України рівень освітлення доріг значно нижчий за нормативний через використання застарілих світильників, обладнаних низькоефективними лампами розжарювання (світловіддача 15 лм/Вт) та ртутними лампами (світловіддача 60 лм/Вт) [1]. До того ж існуючі схеми електропостачання не забезпечують необхідного рівня надійності для систем зовнішнього освітлення.

Підвищення надійності мереж зовнішнього освітлення відкриває можливості для енергозбереження, безперебійного електропостачання та підвищення безпеки на дорогах. Адже якісне освітлення міських територій суттєво зменшує кількість дорожньо-транспортних пригод і протиправних дій. На сьогоднішній день мережі зовнішнього освітлення є одними з найбільших споживачів електроенергії. Тому їх модернізація виступає одним із найефективніших і необхідних заходів з енергозбереження [2].

Більшість аварій у нічний час відбуваються через погану видимість на дорозі, а також через відсутність належного освітлення пішохідних переходів. Для ефективного забезпечення безпеки важливо використовувати сучасні світлотехнічні рішення, такі як LED-освітлення, яке забезпечує яскраве, рівномірне світло при значно менших енергетичних витратах.

Ще однією важливою складовою є правильно підібране розташування освітлювальних приладів. Нерівномірне або надмірне освітлення може призвести до засліплення водіїв, що також підвищує ризик аварій. Згідно з сучасними дослідженнями [3], оптимальне освітлення повинно бути адаптоване до конкретних умов дороги, враховуючи її ширину, інтенсивність руху та вид транспортних засобів.

Одним із важливих аспектів є також освітлення пішохідних переходів. В умовах нічного часу, коли видимість значно знижується, пішоходи часто не можуть швидко оцінити наближення транспортного засобу. Тому необхідно забезпечити чітке та яскраве освітлення на перехрестях і переходах задля підвищення видимості пішоходів для водіїв.

Для досягнення високої ефективності світлотехнічних рішень рекомендується застосовувати наступні підходи:

1. Використання сучасних світлодіодних технологій. LED-освітлення є однією з найкращих альтернатив традиційним лампам через свої низькі енергетичні витрати та довговічність. Світлодіоди дають яскраве та якісне світло, яке рівномірно розподіляється по поверхні дороги, зменшуючи темні ділянки та мінімізуючи ризик аварій.

2. Розумні системи управління освітленням. Сучасні технології дозволяють створювати автоматизовані системи, які можуть регулювати інтенсивність освітлення у реальному часі, в залежності від інтенсивності руху або погодних умов [4]. Такі системи можуть включати датчики руху або навіть використовувати штучний інтелект для прогнозування змін в умовах освітлення та автоматичного налаштування освітлення відповідно до ситуації на дорозі.

3. Інтеграція освітлення з іншими системами безпеки. Освітлення може бути інтегроване з сигналізаціями або камерами спостереження, що дозволяє отримати більш точну картину ситуації на дорозі та оперативно реагувати на виникаючі небезпеки. Цей захід також дозволяє автоматично включати підсвітку пішохідних переходів або інших небезпечних ділянок, коли це необхідно.

4. Ергономіка та дизайн освітлення. Дизайн освітлення, розташування ліхтарів, їх висота та кут нахилу повинні бути розраховані таким чином, щоб мінімізувати засліплення водіїв та забезпечити максимальну видимість для пішоходів.

5. Покращення освітлення пішохідних переходів та зупинок. Оскільки пішоходи є найбільш вразливою групою учасників дорожнього руху, освітлення пішохідних переходів має особливу важливість. Крім того, на зупинках громадського транспорту слід забезпечити комфортне освітлення, щоб люди могли чітко бачити наближення транспорту та пішохідні переходи.

Використання сучасних технологій, таких як LED-освітлення, адаптивні системи управління освітленням та інтеграція з іншими системами безпеки, здатні значно покращити умови для водіїв та пішоходів, знижуючи ризики, пов'язані з недостатнім освітленням на дорогах. Сьогодні необхідно враховувати різноманітність умов і потреб, оптимізуючи рішення для конкретних типів доріг та конкретних ситуацій, щоб забезпечити максимальний рівень безпеки. Впровадження таких технологій дозволить не тільки покращити безпеку, але й досягти економії енергії, що є важливим аспектом у контексті сталого розвитку та охорони навколишнього середовища.

1. ДБН В.2.5-28:2018 Інженерне обладнання споруд. Природне та штучне освітлення.
2. Салтиков В.О. Освітлення міст: Навч. пос. – Харків: ХНАМГ, 2009. – 221 с.
3. Пилипчук Р.В. Зовнішнє освітлення міста / Р.В. Пилипчук, Р.Ю. Яремук, В.В. Щиренко // Світло-люкс. – 2006. – №6. – С. 75–79.
4. Іванова М.С. Інтелектуальна система управління в освітленні пішохідних переходів для підвищення енергоефективності [Текст] / М.С. Іванова, І.В. Олейнікова // Технології та інжиніринг. – 2021. – №3. – С. 9-17.

O. Korchenko, A. Herasymenko

FORM A DATABASE OF PRIMARY SOURCES FOR REQUIREMENTS DEVELOPMENT FOR A SYSTEM THAT COMBINES SEMANTIC ANALYSIS AND ANALYSIS OF USER BEHAVIOUR IN ORDER TO DETECT AND PREDICT ANOMALIES IN THE CRYPTOCURRENCY MARKET

Recently, methods of semantic analysis and behaviour analysis users are increasingly being used to forecast market trends. These methods allow researchers and analysts to understand psychological aspects influencing market movements. However, their potential in the context of cybersecurity has not yet been fully disclosed. This work aims to form a database of primary sources for requirements development for a system that combines semantic analysis and analysis of user behaviour to detect and predict anomalies in the cryptocurrency market. An innovative approach to studying cryptocurrency markets from a cybersecurity perspective may provide investor protection and promote stability and trust in this new segment of the economy. In conclusion, this study aims to create a strong foundation for developing tools and strategies that will provide a more secure and transparent environment for cryptocurrency market participants [1,2,3,4].

Development of the system that combines semantic analysis and analysis of user behaviour requires the use of a number of methods:

General scientific methods:

1. Analysis and synthesis: Used to break down the test subject object into parts and generalise the obtained data.

2. Induction and deduction: Used to form general inferences based on individual observations and logical inference conclusions.

Special Methods:

1. Methods of Semantic Analysis: These methods analyse textual information obtained from news, forums, and social networks to identify possible anomalies [5,6,7].

2. User Behavior Analysis Techniques: These methods will focus on learning patterns and user interaction in cryptocurrency markets [8,9,10].

Research tools:

1. Machine Learning: Using Deep Learning Algorithms and neural networks for detecting anomalies based on big data.

2. Statistical Analysis: Using statistical methods to test hypotheses and identify data patterns [10,11].

Thus, having analysed the methods necessary for development, the authors formed a base of primary sources for determining the requirements for the system.

1. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Режим доступу: https://bitcoin.org/bitcoin.pdf.
2. Milutinović, Monia (2018). "Cryptocurrency". Ekonomika. 64 (1): 105– 122. doi:10.5937/ekonomika1801105M. ISSN 0350-137X.
3. Pernice, IngolfG. A. ; Scott, Brett (20 May 2021). "Cryptocurrency" . InternetPolicy Review. 10 (2). doi:10.14763/2021.2.1561. ISSN 2197-6775.
4. Liu , Jinan ; Rahman , Sajjadur ; Serletis , Apostolos (2020). " Cryptocurrency Shocks" . SSRN Electronic Journal. doi: 10.2139/ssrn.3744260. ISSN 1556-5068. S2CID 233751995.
5. Turney, Peter (2002). "Thumbs Up or Thumbs Down? Semantic Orientation Applied to Unsupervised Classification of Reviews". Proceedings of the Association for Computational Linguistics. pp. 417–424.
6. 6. Pang, Bo; Lee, Lillian; Vaithyanathan, Shivakumar (2002). "Thumbs up? Sentiment Classificationusing Machine Learning Techniques". Proceedings of the Conference on Empirical Methods in Natural Language Processing (EMNLP). pp. 79–86.
7. Shahzad Qaiser, Ramsha Ali - Text Mining: Use of TF-IDF to Examine the Relevance of Words to Documents - International Journal of Computer Applications – No.1, July 2018 - https://www.researchgate.net/ publication/326425709_Text_Mining_Use_of_TF-IDF_to_Examine_the_Relevance_of_Words_to_Documents.
8. Daniel Jurafsky & James H. Martin - Speech and Language Processing - https://web.stanford.edu/~jurafsky/slp3/3.pdf.
9. Xinying Song, Alex Salcianu, Yang Song, Dave Dopson, Denny Zhou - Fast WordPiece Tokenization - Proceedings of the 2021 Conference on Empirical Methods in Natural Language Processing - November 7–11, 2021 - https://aclanthology.org/2021.emnlp-main.160.pdf.
10. The Pros and Cons of Using Natural Language Processing Tools - https://www.wesuggestsoftware.com/the-pros-and-cons-of-using-natural-language-processing-tools.
11. Adhikari R. An Introductory Study on Time Series Modeling and Forecasting / Adhikari R. – Riga: LAP Lambert Academic Publishing, 2013. – 76 p.

I.O. Dubovkina

DISCRETE-PULSED INPUT OF ENERGY FOR TREATMENT OF LIQUID NUTRIENT SOLUTION

Today innovative technologies have been improved by the application of modern scientific knowledge.The method of the alternating impulses of pressure may be appropriate for technology of the associated liquid aqueous systems and solutions processing for nutrient solution and semi-finished products.

The method of discrete-pulsed input of energy can power structural transformations in difficult liquid systems on micro- and nanolevel and gives possibility to initiate physical and chemical transformations in these complex systems[1].

The main effects of the discrete-pulsed input of energy are effects which connected with:

- increase of velocity of association of a continuous phase;
- power of pressure of shift;
- cavitations;
- the effect of explosive boiling;
- collective effects in assembly of vials;
- crossness of an interphase surface in gas-liquid bubbly medium;
- action of hydrodynamic oscillations;
- alternating impulses of pressure [2].

To optimize the process of hydrodynamic treatment it is necessary to define the level of power influence on the liquid medium and solutions for indispensable transformations which can provide predictable physical chemical characteristics and parameters.

The analytical chemistry and chemical methods were used for the researches physical and chemical parameters of the aquatic solutions.There are different types of hydroponic systems[3].

It is passive hydroponic systems without any powered equipment and apparatus and active hydroponic systems, which include automatic controllers, timers, measuring systems, mechanical pumps, engines etc.

The development of different microliquid devices for some last decades has caused growth of interest to microscale streams. Rotary pulse apparatus is characterised by small enough sizes of width of channels which gives the possibility to consider them as microchannels with effects of slippage a watercourse on walls and surfaces.

The aim of this studies it to treat water in hydroponics system by discrete-pulsed input of energy such as alternating impulses of pressure for changing the pH of the hydroponics.

A number of heat and mass technological processes (structuring, crushing, dispersion, emulsification, homogenization, mixing) are spend in rotary pulse

apparatus of cylindrical type which realise principles of alternating impulses of pressure.

Among other agricultural systems, the opportunities soilness systems present are becoming more evident. Because of this the alternative agricultural technologies, techniques and equipment as an innovative food production technology accommodates increased productivity with limited resources and improved carbon footprint.

There are many kinds of hydroponic systems. Some of them are: a wick system (passive system); a water culture (active system), a flood and drain (active system), the drip systems (active system), a nutrient film technique (active system), an aeroponic (active system).

The hydroponic system from recirculation technological mode of greenhouse in the technological processes of the growing crops is exceptionally multiple constituent elements complex organic organization which includes many types of biotic organisms [4].

This study was carried out at the pilot unit designed and created at the IET HASU, the main part of the unit is a rotary pulsed apparatus in which realized alternating impulses of pressure.

During the volume three-dimensional parametric imitation it was established that speeds of shift of a stream should be equal to $2{,}0 \cdot 10^5 s^{-1}$ for the first rotor and $2{,}5 \cdot 10^5 s^{-1}$ for the second rotor.

Through researches increases pH of the pure water on 15% have been established, thus the hydrogen potential of the water prepared on technology for hydroponic system has raised on 15-16.5%.

Investigational studies have shown that the method of the alternating impulses of pressure may be suitable for technology of water treatment in hydroponics system.

As a result of research, it was found that the discrete-pulsed input of energy for water treatment such as alternating impulses of pressure can greatly reduce energy, power and resource consumption, increase efficiency of the growing crops. It can be appropriate for processing in existing technologies without high economic costs.

1. Dubovkina Iryna (2017), Change of physical and chemical parameters of the liquid binary systems by alternating impulses of pressure, Ukrainian Food Journal, 6(1), pp. 142–154, DOI: 10.24263/2304-974X-2017-6-1-16.
2. Dolinskij A.A., Basok B.I. (2005), Nanoscale effects by discrete-pulsed transformation of energy, IFZH, 78(1), pp. 15–23.
3. Edited by Kenneth I.Ozomwna (2007), Recent Advances in Analitycal Electrochemistry, *Transword Research Network*, 300 p. Available at: Network.http://www.ressign.com/UserBookDetail.aspx?bkid=605&catid=160.
4. Mamta D. Sardare, Shraddha V. Admane (2013), A Review on Plant without Soil – Hydroponics. International Journal of Research in Engineering and Technology Volume 2, Issure 3, 299-304 https://www.ijret.org.

Г.Є. Дубинський, В.Ю. Зубок

РЕЗИЛЬЄНТНІСТЬ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ЕНЕРГЕТИЧНОЇ КРИЗИ

В технологічних системах та операційних технологіях дедалі більше використовуються дистанційне керування, віддалений доступ, а отже – глобальні електронні комунікації та кіберпростір. Впродовж російсько-української війни російські війська активно застосовують атаки на цивільну енергетичну інфраструктуру в якості фактору військового впливу. Спровоковані таким чином перебої в роботі енергосистеми держави впливають на усі галузі, зокрема і на кіберстійкість об'єктів критичної інфраструктури. Основним чинником впливу є втрата зв'язку. У зв'язку з цим актуальною є проблема **резильєнтності об'єктів критичної інформаційної інфраструктури (ОКІІ) у зв'язку із вразливостями його зовнішніх зв'язків у кіберпросторі.** Розглянемо декілька основних напрямів підвищення кіберстійкості ОКІІ, які пов'язані з топологією, або можуть вплинути на топологію його зовнішніх зв'язки з кіберпростором.

Стале та безпечне функціонування компонентів критичного інформаційного активу. Критичний інформаційний актив (КІА) – компонент ОКІІ, порушення цілісності якого або незабезпечення (авторизованого) доступу до якого безпосередньо вплине на стале функціонування ОКІ. Одним з найважливіших чинників, що впливає на топологію ОКІІ, є вибір базового архітектурного рішення – розгортання системи або на власному програмно-апаратному обладнанні підприємства, або в орендованій «хмарі». Багато підприємств переглянули ставлення до конфіденційності чутливих даних в рамках завдань забезпечення безперервності бізнес-процесів на користь їх доступності, оскільки таким чином вони більше відповідають завданням безперервності бізнесу. Втім, хмарне рішення означає фактично передавання логічного доступу до даних ще одному учасникові ланцюжка постачання. Альтернативою рішенню on-premises та орендованої хмари є послуга *colocation* - розгортання КІА в спеціалізованому приміщенні центру обробки даних (ЦОД), але на обладнанні власника КІА. Розміщення власних апаратних серверів в ЦОД усуває загрози, пов'язані з конфіденційністю в хмарній інфраструктурі [1].

Сучасним підходом також є використання гібридної хмарної інфраструктури - комбінації приватного середовища (on-premises, приватна хмара або colocation), з публічною хмарою. Гібридна інфраструктура дозволяє зберігати конфіденційні дані локально в приватному середовищі, тоді як програмні засоби та віртуальні машини можна розгорнути в публічній хмарі, серед переваг якої – швидке масштабування. Сучасні автоматизовані системи керування процесами (АСКТП) мають гібридну архітектуру, в якій задіяні on-premises активи сумісно із приватними чи публічними хмарами, що є невід'ємними частинами певної платформи (це

типово для промислового інтернету речей). Організаційні та технічні ризики, пов'язані з хмарними обчисленнями, детально викладено в рекомендаціях ENISA [2].

Резильєнтність ОКІІ в умовах масштабних відключень електроенергії. Через російські атаки на критичну інфраструктуру забезпечення доступу до КІА потребує використання найбільш витривалих комунікаційних технологій в умовах переривань електропостачання. Критерієм витривалості може служити кількість активних точок ретрансляції, що потребують електроживлення. Обрання певного рішення з підвищення доступності залежить від пріоритетів власника системи. Три критерії є вхідними даними для оцінювання:

– мінімально прийнятна функціональність системи;
– доступна вартість відновлення;
– цільовий час відновлення.

В [3] розглянуто та порівняно комунікаційні технології так званої «останньої милі», що типово використовуються для підключення кінцевих споживачів: Ethernet, DOCSIS, ADSL, FTTB або FTTH, PON, різні супутникові системи широкосмугового доступу (VSAT, Starlink, OneWeb). Технологія побудови широкосмугових мереж доступу PON вважається найбільш стійкою до дефіциту електроенергії за умови забезпечення автономного живлення лише кінцевих точок. Таким чином, ця технологія забезпечить високу доступність даних при обміні між КІА та суб'єктів доступу в разі масштабних відключень електроенергії. Це має високу цінність, оскільки для ОКІ безперервність роботи (тобто швидше відновлення) є найвищим пріоритетом. Важливим фактором є принципова можливість використання певних рішень для підвищення доступності доступу до мережі в конкретному приміщенні або на конкретній території.

Отже, ефективне обрання комбінацій варіантів впливає на резильєнтність ОКІІ. Процес вибору продемонстрований на рис.1.

Рисунок 1 – Складові резильєнтності ОКІІ

Прийняття рішень може потребувати ще більшої деталізації, яка має привести до розуміння переваги того чи іншого рішення по сукупності метрик: можливість впровадження*; швидкість впровадження; низька вартість впровадження; результативність впровадження*. Результативність впровадження може бути відображена або в зменшенні часу на відновлення, або в зменшенні вартості відновлення в межах визначеного часу (recovery point objective, RPO).

1. Cloud Computing. Benefits, risks and recommendations for information security. URL: http://www.enisa.europa.eu/media/news-items/cloud-computing-speech (accessed: 11.11.2024).
2. В.В. Зубок, Р.С. Драгунцов, В.Ю. Зубок. Резильєнтність ERP-систем в умовах енергетичної кризи. 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. – с. 13-16.
3. Zubok, V. Assessment and improvement of digital resilience in the energy crisis caused by missile strikes. IOP Conf. Ser.: Earth Environ. Sci. 1254 012039. DOI: 10.1088/1755-1315/1254/1/012039.

Yu. Tkach, I. Diuba

ANALYSIS OF THE CURRENT STATE BIOMETRICS ACCESS CONTROL SYSTEMS

Access control systems are an integral part of modern information systems. Access control mechanisms have yet to be developed and varied, but by their nature, they are associated with users of knowledge, property or properties whose are the basis of identification and authentication procedures. Biometrics [1] is a science that studies human property in order to build mechanisms and identifiers of access control based on them. While there are many types of biometric authentication, some of the most widely used solutions include [2]:

- Fingerprint door locks or a fingerprint entry system.
- Vein recognition.
- Facial recognition door locks or entry system.
- Eye scan door locks or entry system.
- Retinal scan door locks or entry system.
- Iris scan door locks or entry system.

A significant reduction in the cost of such devices has recently made them the main contender when choosing an access control mechanism. Therefore, we will outline ways to analyze them.

There are two types of biometrics [3]:

1. Physiological measurements. They can be either morphological or biological.

– Morphological identifiers mainly consist of fingerprints, the hand's shape, the finger vein pattern, the eye (iris and retina), and the face's shape.

– For biological analyses, DNA, blood, saliva, or urine may be used by medical teams and police forensics.

2. Behavioral measurements. The most common are:

– voice recognition,

– signature dynamics (speed of movement of pen, accelerations, pressure exerted, inclination),

– keystroke dynamics,

– the way we use objects,

– gait, the sound of steps,

– gestures, etc.

So biometric authentication is based upon biometric recognition which is an advanced method [4] of recognizing biological and behavioral characteristics of an user.

– Universality means that every person using a system should possess the trait.

– Uniqueness means the trait should be sufficiently different for individuals in the relevant population such that they can be distinguished from one another.

– Permanence relates to the manner in which a trait varies over time. More specifically, a trait with good permanence will be reasonably invariant over time with respect to the specific matching algorithm.

– Measurability (collectability) relates to the ease of acquisition or measurement of the trait. In addition, acquired data should be in a form that permits subsequent processing and extraction of the relevant feature sets.

– Performance relates to the accuracy, speed, and robustness of technology used (see performance section for more details).

– Acceptability relates to how well individuals in the relevant population accept the technology such that they are willing to have their biometric trait captured and assessed.

– Circumvention relates to the ease with which a trait might be imitated using an artifact or substitute.

Quickly review the most typical use cases of biometric technologies includes [3]: Law enforcement and public security (criminal/suspect identification); Military (enemy/ally identification); Border, travel, and migration control(traveler/migrant/passenger identification); Civil identification (citizen/resident/voter identification); Healthcare and subsidies (patient/beneficiary/healthcare professional identification); Physical and logical access (owner/user/employee/ contractor/partner identification); Commercial applications (consumer/customer identification).

Summing up, we should note - a brief overview of biometric approaches to tent access control shows us a taxonomy of future research.

1. Biometric Access Control Systems: Complete Guide https://getsafeandsound.com/blog/biometric-access-control/.
2. An Introduction to Biometric Access Control | Gallagher Security https://security.gallagher.com/en-US/Blog/An-Introduction-to-Biometric-Access-Control#:~:text=A%20biometric%20access%20control%20system%20uses%20unique%20physical,grant%20them%20access%20to%20restricted%20areas%20of%20buildings.
3. Biometrics (facts, use cases, biometric security) https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics.
4. Biometrics - Wikipedia https://en.wikipedia.org/wiki/Biometric.

О.А. Хоменко, М.М. Худинцев

АВТОМАТИЗАЦІЯ ПРОЦЕСІВ КІБЕРСТРАХУВАННЯ В РАМКАХ ISO / IEC 27102: 2019 (E) УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ – ВКАЗІВКИ ЩОДО КІБЕРСТРАХУВАННЯ

Актуальність кіберстрахування пов'язана із збільшенням залежності користувачів від цифрових послуг, що призвело до розробки нормативних документів з кіберстрахування [1], формалізації та алгоритмізації підходів до пом'якшення ризиків [2] Типові атаки призвели до критичних наслідків і вплинули на тисячі компаній у багатьох регіонах і галузях [3,4].

Перший нормативний документ з кіберстрахування ISO / IEC 27102: 2019 [1] описує застосування відповідних практик у бізнес-діяльності. Стандарт містить термінологію та нові визначення, огляд кіберстрахування та його політик, опис принципів і структури кіберстрахового полісу, визначення кіберризиків та страхового покриття, опис процесів управління ризиками та кіберстрахування, ідентифікацію кіберінцидентів, вплив на бізнес і збитки, що підлягають страхуванню, ризики постачальників, визначення тихого або нетвердого покриття в інших страхових полісах, процеси взаємодії з постачальниками та користувачами щодо реагування на інциденти, винятки полісу кіберстрахування з урахуванням обмеження сум покриття, оцінку ризиків, яку підтримує андеррайтинг кіберстрахування, опис внутрішніх процесів кіберстрахування (огляд, збір інформації, оцінка кіберризиків страхувальника, зв'язок з СУІБ у підтримці кіберстрахування, джерела інформації, обмін інформацією про ризики та засоби контролю, зобов'язання за полісами кіберстрахування).

Основна стратегія страхування полягає у розподіленні ризику 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.

Автоматизація процесів, передбачених [1], починається з визначення бізнес-процесів, доступних для алгоритмізації. Існуючі технології застосовуються, у першу чергу, для процесів збору інформації та оцінювання ризиків.

В якості можливого підходу для оцінювання кіберризиків пропонується використання кількісних моделей зрілості кібербезпеки для інформаційних

(інформаційно-комунікаційних) систем і процесів у секторах критичної інфраструктури, в національній системі кібербезпеки з використанням індикаторів та індексів стану мережевої та інформаційної безпеки.

Існуючі світові та національні практики дозволяють досліджувати рівень зрілості кібербезпеки, але впровадження практик, фреймворків, стандартів оцінювання інформаційної безпеки, кібербезпеки, їх зрілості стикається з низкою організаційно-технічних проблем, серед яких невідповідність матеріально-технічної бази необхідному рівню кіберзахисту, відсутність або недосконалість механізмів практичного оцінювання рівня загроз та планування адекватних заходів захисту, недостатність або невідповідність даних для побудови прогностичних моделей захисту та розвитку.

Ієрархія моделей оцінювання зрілості кібербезпеки в національній екосистемі кібербезпеки (національній системі кібербезпеки, критичній інфраструктурі, зокрема, паливно-енергетичному секторі) дозволяє розробити та впровадити автоматизовану процедуру кількісного оцінювання ризиків з одночасним накопиченням статистичних даних щодо кіберінцидентів, кібератак, заходів протидії для подальшого використання цих даних у прогностичному аналізі та моделюванні, використанні цих даних у задачах та процесах кіберстрахування.

Метою дослідження є визначення даних та технологій їх обробки, які у подальшому використовуються в процесах кіберстрахування, передбачених ISO / IEC 27102: 2019 [1], опис та оцінювання готовності застосування до повного виробничого циклу кіберстрахування запропонованих методів збору та обробки даних про кіберінциденти та кіберризики.

Також розглянуто застосування Методики оцінювання стану кібербезпеки електричних мереж та практик кібербезпеки електричних мереж [5] у паливно-енергетичному секторі для реалізації основних положень [1] з метою подальшого страхування об’єктів критичної інфраструктури різних рівнів зрілості.

1. ISO / IEC 27102: 2019 (E) International standard. Information security management - Guidelines for cyber-insurance. First edition 2019-08. Copy of International Cybersecurity University (2019).
2. Franke U.: The cyber insurance market in Sweden. Comput. Secur. 68, 130–144 (2017).
3. Survey, H. Cyber Insurance: A Hard Reset, Howden Broking, https://www.howdengroup.com (2022).
4. Gallagher Cyber Insurance Market Conditions Report: Guidance as the cyber insurance market continues to harden. https://www.ajg.com/us/news-and-insights/ (2023).
5. Про затвердження Методики оцінювання стану кібербезпеки електричних мереж та практик кібербезпеки електричних мереж, наказ Міністерства енергетики України від 5.08.2024 № 285, https://zakon.rada.gov.ua/laws/show/z1278-24#Text (2024).

М.М. Худинцев, І.Л. Палажченко

ПОКАЗНИКИ ВІДНОВЛЕННЯ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Аналіз рекомендацій з захисту (кіберзахисту) критичної інформаційної інфраструктури [1] свідчить про суттєвий вплив показників відновлення інфраструктури, які можна виділити (відокремити) від інших показників захисту (див. Таблицю 1).

Таблиця 1 – Показники відновлення критичної інформаційної інфраструктури

Функція захисту	Категорія заходу	Показники відновлення (підкатегорія заходу)	Умовна вага
Ідентифікація (ID)	Управління активами (ID.AM)	ID.AM-0: Перелік та категоризації об'єктів критичної інфраструктури затверджени	1
		ID.AM-1: Інвентаризуються фізичні пристрої та системи в організації	2
		ID.AM-2: Інвентаризуються програмні платформи та додатки в організації	2
		ID.AM-3: Інвентаризуються відокремлені/віддалені підрозділи, організації в сфері управління, персонал	2
	Ділове середовище (ID.BE)	ID.BE-2: Місце організації в критичній інфраструктурі та її галузевому секторі визначається та повідомляється	1
		ID.BE-4: Встановлено залежності та критичні функції для надання критичних послуг	3
		ID.BE-5: Вимоги до відмовостійкості для підтримки надання критично важливих послуг встановлені для всіх робочих станів	3
	Стратегія	ID.RM-3: Визначення організацією	3

	управління ризиками (ID.RM)	стійкості до ризику базується на її ролі в критичній інфраструктурі та аналізі ризиків у певному секторі	
	Управління ризиками ланцюга поставок (ID.SC)	ID.SC-5: Планування реагування та відновлення, а також тестування проводяться разом із постачальниками та сторонніми постачальниками	3
Захист (PR)	Обізнаність і навчання (PR.AT)	PR.AT-1: Усі користувачі проінформовані та навчені	2
		PR.AT-4: Старші керівники розуміють ролі та відповідальність	1
		PR.AT-5: Персонал із фізичної та інформаційної безпеки розуміє ролі та обов'язки	1
	Безпека даних (PR.DS)	PR.DS-7: Середовища розробки та тестування відокремлені від середовища виробництва	1
	Процеси та процедури захисту інформації (PR.IP)]	PR.IP-4: Резервне копіювання інформації виконується, підтримується та тестується	2
		PR.IP-9: Плани реагування (на інциденти та забезпечення безперервності роботи) і плани відновлення (аварійного відновлення) існують і ними керуються	8
		PR.IP-10: Плани реагування та відновлення перевіряються	4
	Технології захисту (PR.PT)	PR.PT-5: Механізми відмовостійкісті реалізовані для досягнення вимог стійкості в нормальних і несприятливих ситуаціях	1
Реагування (RS)	Планування реагування (RS.RP)	RS.RP-1: План реагування виконується під час або після події	8
	Зв'язки (RS.CO)	RS.CO-1: Персонал знає свої ролі та порядок дій, коли потрібна реакція	4

		RS.CO-3:Інформація передається відповідно до планів реагування	4
		RS.CO-4: Координація із зацікавленими сторонами відбувається відповідно до планів реагування	4
Відновлення (RC)	Планування відновлення (RC.RP)	RC.RP-1: План відновлення виконується під час або після інциденту	8
	Покращення (RC.IM)	RC.IM-1: Плани відновлення включають отримані висновки	8
		RC.IM-2: Оновлено стратегії відновлення	8
	Комунікації (RC.CO)	RC.CO-2: Репутація після події відновлюється	8
		RC.CO-3: Діяльність з відновлення повідомляється внутрішнім і зовнішнім зацікавленим сторонам, виконавчим і управлінським командам	8

Зв'язок показників відновлювання критичної інформаційної інфраструктури з стійкістю (резильєнтністю) такої інфраструктури описується в рамках моделі локального індексу кібербезпеки [2], показниками якого виступатимуть показники відновлювання критичної інформаційної інфраструктури.

Вимірювання показників індексу здійснюється шляхом експертного оцінювання. У найпростіших моделях індексу використовується дво- або багатобальна система дискретної експертної оцінки з ваговими коефіцієнтами, які дорівнюють 1. Більш складні моделі використовують системи безперервної оцінки та/або змінні (самоузгоджені) вагові коефіцієнти (можливий варіант значень вагових коефіцієнтів наведено у Таблиці 1).

1. Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України 06 жовтня 2021 року № 601 https://cip.gov.ua/services/cm/api/attachment/download?id=42914.
2. Худинцев М.М., Жилін А.В., Давидюк А.В. Світові індекси кібербезпеки: огляд та методики формування (Глобальний звіт / Каталог). Міжнародний університет кібербезпеки, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. К.: 2021. 240 с.

Ю.І. Дзюбан

ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ НА БЕЗПЕКУ ЕНЕРГЕТИЧНИХ СИСТЕМ

В умовах швидкого розвитку систем штучного інтелекту оцінка їх впливу на енергетичні системи має величезне значення для безпеки та безперебійної роботи енергетичних систем. Розглянемо позитивні та негативні впливи, потенційні ризики та виклики впливу штучного інтелекту (надалі «ШІ» - автор) на енергетичні системи

Позитивний вплив ШІ на безпеку енергетичних систем:

- *активне виявлення аномалій*. ШІ може аналізувати великі обсяги даних з різних джерел (сенсори, мережевий трафік) для виявлення відхилень від нормального функціонування системи, що можуть свідчити про потенційні загрози;

- *прогнозування та попередження аварій*. За допомогою алгоритмів машинного навчання ШІ може прогнозувати можливі збої в роботі обладнання, що дозволяє вжити профілактичних заходів;

- *оптимізація режимів роботи.* ШІ може оптимізувати режими роботи енергетичних систем, знижуючи ризик перевантажень та аварій;

- *посилення кібербезпеки*. ШІ може використовуватися для виявлення кібератак, аналізу шкідливого коду та розробки нових методів захисту інформації.

- *автоматизація рутинних операцій*. ШІ може автоматизувати багато рутинних операцій, зменшуючи людський фактор та підвищуючи надійність системи;

Потенційні ризики та виклики:

- *вразливість моделей ШІ*. Моделі ШІ можуть бути обмануті або атаковані, що може призвести до помилкових рішень та компрометації системи;

- *залежність від даних.* Якість роботи ШІ безпосередньо залежить від якості та повноти даних, які використовуються для навчання моделей;

- *висока вартість впровадження*. Впровадження ШІ в енергетичні системи вимагає значних інвестицій у обладнання, програмне забезпечення та навчання персоналу;

- *етичні питання*. Використання ШІ в енергетиці пов'язане з рядом етичних питань, таких як відповідальність за прийняття рішень, захист даних та приватність.

Стратегії впровадження ШІ для підвищення безпеки:

- *комплексний підхід.* Поєднання ШІ з традиційними методами забезпечення безпеки;

- *поступове впровадження.* Початок з простих завдань та поступове розширення сфер застосування ШІ;

- *безпека даних.* Забезпечення надійного захисту даних, що використовуються для навчання моделей ШІ;

- *регулярна перевірка та оновлення.* Регулярна перевірка моделей ШІ на наявність уразливостей та їх оновлення;

- *співпраця з експертами.* Залучення експертів у галузі енергетики, кібербезпеки та штучного інтелекту.

Специфічні напрямки застосування ШІ в енергетиці:

- *прогнозування попиту на електроенергію.* ШІ може прогнозувати попит на електроенергію з високою точністю, що дозволяє оптимізувати виробництво та розподіл.

- *оптимізація роботи енергомереж.* ШІ може аналізувати дані про стан енергомережі та оптимізувати її роботу для підвищення ефективності та надійності.

- в*иявлення аномалій в роботі обладнання.* ШІ може виявляти відхилення від нормального функціонування обладнання на ранніх стадіях, що дозволяє запобігти аваріям.

- *кібербезпека.* ШІ може використовуватися для виявлення кібератак, аналізу шкідливого коду та розробки нових методів захисту інформації.

- *управління розподіленими джерелами енергії.* ШІ може оптимізувати роботу розподілених джерел енергії (сонячні батареї, вітряні турбіни) та забезпечити їх інтеграцію в енергосистему.

Висновок.

Штучний інтелект має великий потенціал для підвищення безпеки енергетичних систем. Однак, для досягнення цієї мети необхідно враховувати як переваги, так і ризики, пов'язані з використанням ШІ. Комплексний підхід, постійний розвиток технологій та співпраця між різними галузями знань є ключовими факторами успіху.

1. «Штучний інтелект в енергетиці», національний інститут стратегічних досліджень, 2022 р., https://niss.gov.ua/sites/default/files/2022-07/dopovid-ai-v-energetici-red_01-pogodzheno-sukhodolya_02-1.pdf.
2. «Перспективи застосування штучного інтелекту для покращення енергозбереження в умовах україни», 2024 р., http://inneco.org/index.php/innecoua/article/view/1246/1349.

В.Я. Тищенко

ПОКАЗНИКИ НЕСИНУСОЇДАЛЬНОСТІ НАПРУГИ У НАЦІОНАЛЬНИХ СТАНДАРТАХ І СТАНДАРТІ IEEE

У нормативних документах [1, 2] перелік показників якості електричної енергії включає коливання напруги, відхилення частоти, просадки та імпульси напруги, тимчасові перенапруги та інші. Водночас для напівпровідникових перетворювачів одним з основних показників якості електричної енергії є несинусоїдальність напруги [1].

В Україні для оцінки несинусоїдальності напруги використовують так званий коефіцієнт гармонік напруги [3]:

$$К_{Г_U} = \frac{1}{n.}\sqrt{\sum_{k=2}^{\infty} U_k^2}, \quad (1)$$

де U_k – діюче значення k-ої гармоніки напруги; U_1 – діюче значення першої гармоніки напруги.

Крім терміну «коефіцієнт гармонік», також вживаються такі назви як «коефіцієнт несинусоїдальності» [4], «коефіцієнт спотворення» [5], «сумарний коефіцієнт гармонічних спотворень напруги» [6], тощо.

Як зазначено у п. 11.4.12 нормативного документу [2], «сумарний коефіцієнт гармонічних спотворень напруги електропостачання, ураховуючи всі гармоніки до 40-ї включно, для мереж низької напруги має бути меншим чи рівним 8 %».

Національні стандарти [1] та [2] також регламентують допустимі середньоквадратичні значення напруги для кожної гармоніки. Їх наведено в таблиці 1.

В стандарті IEEE 519-2022 [7] визначення коефіцієнта THD (Total Harmonic Distortion) звучить як відношення середньоквадратичного значення гармонік, враховуючи гармонійні компоненти до 50-го порядку до основної гармоніки:

$$THD = \frac{\sqrt{U_2^2+U_3^2+U_4^2+\cdots}}{n.}, \quad (2)$$

Граничні значення коефіцієнта THD приведені в таблиці 2.

Таким чином, можна зробити висновок, що коефіцієнт THD, який визначено в нормативному документі [7] та який широко використовується в іноземних публікаціях, наприклад, [8], є ніщо інше як коефіцієнт гармонік або сумарний коефіцієнт гармонічних спотворень. Більш того, їхні допустимі значення співпадають згідно національних стандартів та стандарту IEEE. Водночас таблиці 1 і 2 показують, що допустимі середньоквадратичні значення напруги окремих гармонік в зазначених стандартах різняться.

Таблиця 1 – 95 % середньоквадратичних значення напруги кожної гармоніки, усереднених на 10-хвилинному проміжку

Непарні гармоніки				Парні гармоніки	
не кратні 3		кратні 3			
порядок	відносна амплітуда	порядок	відносна амплітуда	порядок	відносна амплітуда
5	6,0 %	3	5,0 %	2	2,0 %
7	5,0 %	9	1,5 %	4	1,0 %
11	3,5 %	15	0,5 %	6…24	0,5 %
13	3,0 %	21	0,5 %		
17	2,0 %				
19	1,5 %				
23	1,5 %				
25	1,5 %				

Таблиця 2 – Граничні значення коефіцієнта THD згідно з IEEE 519-2022

Bus voltage Vat PCC	Individual harmonic (%) h ≤ 50	Total harmonic distortion THD (%)
V ≤ 1.0 kV	5.0	8.0

Для опису якості електроенергії також використовується термін «коефіцієнт нелінійних спотворень»:

$$К_{Н.С.,,} = \frac{1}{,,}\sqrt{\sum_{k=2}^{\infty} U_k^2}, \quad (3)$$

де U – діюче значення напруги.

Слід зазначити, що в діапазоні 0 < Кг < 0,1 (0 < Кн.с. < 0,1) різниця між цими коефіцієнтами є настільки незначною, що в багатьох випадках у технічній літературі та навіть у нормативних документах їх часто вважають рівнозначними [9]. Проте при значеннях Кг > 0,1 різниця між ними постає суттєвою. Вони визначаються один через одного таким чином:

$$К_Г(THD) = \frac{К_{н.с}}{\sqrt{1-К_{н.с}^2}}, \; К_{н.с.} = \frac{К_г}{\sqrt{1+К_г^2}}. \quad (4)$$

У документації на аналізатори якості електроенергії закордонного виробництва, як правило, наводяться два коефіцієнти гармонічних спотворень [10], а саме THD Fund, який є аналогом коефіцієнта гармонік, та THD Rms, який є аналогом коефіцієнта нелінійних спотворень.

1. Электрическая энергия. Совместимость технических средств электромагнитная. Нормы качества электрической энергии в системах электроснабжения общего назначения: ГОСТ 13109-97 — [Чинний від 01.01.2000-М]. (Міждержавний стандарт).
2. Кодекс систем розподілу. Постанова НКРЕКП 14.03.2018 № 310— Офіц. вид. — К. : Урядовий кур'єр від 18.04.2018— № 75.
3. Електричні й магнітні кола та пристрої. Терміни та визначення: ДСТУ 2815-94 — [Чинний від 01.01.1996] — К.: Держстандарт України, 1996. — (Державний Стандарт України).
4. Жемеров Г. Г. Коэффициент несинусоидальности напряжения сети в точке подключения активного выпрямителя / Г. Г. Жемеров, О. И. Ковальчук // Технічна електродинаміка. – 2011. – Ч. 2. Тематичний вип. – С. 33–40.
5. Перетворювачі електроенергії напівпровідникові. Терміни та визначення ДСТУ 2847-94 — [Чинний від 01.01.1996] — К.: Держстандарт України, 1996. — (Державний Стандарт України).
6. Характеристики напруги електропостачання в електричних мережах загальної призначеності (EN 50160:2022, IDT) ДСТУ EN 50160:2023— [Чинний від 08.12.2023] — К.: Державне підприємство «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості, 2023. — (Державний Стандарт України).
7. Harmonic Control in Electric Power Systems IEEE 519-2022. PE/T&D - Transmission and Distribution: IEEE Standard — [Чинний від 05.08.2022].
8. Saeed Sepasi1, Member, IEEE, Celia Talichet1, Student, IEEE, Abrar S. Pramanik1, Student, IEEE. 1 Hawai'i Natural Energy Institute, University of Hawaii at Manoa, Honolulu, HI 96822, USA / Power Quality in Microgrids: A Critical Review of Fundamentals, Standards, and Case Studies // IEEE Access 2022.
9. Качество электрической энергии. Термины и определения. ГОСТ 23875-88 — [Не діючий від 01.01.2019] — М.: Міністерство енергетики і електрифікації СРСР, 1988. — (Міждержавний стандарт).
10. Прилад для вимірювання показників якості та обліку електричної енергії SATEC PM180. Керівництво по експлуатації. 2018 SATEC Ltd.

Г.П. Костенко, А.О. Запорожець

ІНТЕГРАЦІЯ ПРИНЦИПІВ ЦИРКУЛЯРНОЇ ЕКОНОМІКИ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ ЕНЕРГЕТИКИ: ПОВТОРНЕ ВИКОРИСТАННЯ БАТАРЕЙ ЕЛЕКТРОТРАНСПОРТУ В СИСТЕМАХ ЗБЕРІГАННЯ ЕНЕРГІЇ

В умовах глобального переходу до екологічно чистої енергії та циркулярної економіки, все більшої актуальності набуває питання ефективного використання ресурсів. Одним із перспективних напрямків, що є логічним продовженням масового впровадження електротранспорту [1-2], є повторне використання літій-іонних батарей (ЛІБ) від електротранспорту в системах зберігання енергії. Після завершення свого первинного життєвого циклу у транспортних засобах, ці батареї все ще мають значний потенціал для зберігання енергії, що робить їх цінним ресурсом для енергетичних систем [3]. Схема життєвого циклу ЛІБ представлена на Рис.1. Вторинне застосування дозволяє зменшити витрати на виробництво нових батарей та знизити екологічне навантаження за рахунок зменшення відходів.

Рисунок 1 – Життєвий цикл ЛІБ електротранспорту [4]

Використання вторинних ЛІБ є важливим аспектом циркулярної економіки, яка спрямована на максимальне використання ресурсів та мінімізацію відходів [5]. Це включає повторне використання, переробку та відновлення матеріалів, що дозволяє зменшити потребу у видобутку нових ресурсів. Застосування таких ЛІБ в системах зберігання енергії сприяє зменшенню викидів парникових газів та підвищенню енергоефективності.

Розвиток методів та моделей для оптимального використання вторинних ЛІБ є ключовим завданням для підвищення стійкості та ефективності енергетичних систем [6-7]. Це включає розробку технологій для оцінки залишкової ємності ЛІБ, прогнозування їхнього залишкового терміну служби та визначення оптимальних параметрів для їх інтеграції в енергетичні системи.

Потенціал вторинних літій-іонних батарей

Вторинні ЛІБ можуть бути ефективно інтегровані в системи, що працюють на ВДЕ, таких як СЕС та ВЕС. Оскільки ВДЕ часто характеризуються нерівномірним виробництвом електроенергії, системи зберігання енергії на основі вторинних ЛІБ можуть відігравати ключову роль у забезпеченні стабільності енергопостачання. Наприклад, СЕС виробляють енергію переважно вдень, тоді як потреби в електроенергії можуть бути вищими ввечері. Використання ЛІБ для зберігання надлишкової енергії, виробленої вдень, дозволяє забезпечити її постачання під час пікових навантажень. Це зменшує навантаження на енергетичну мережу та підвищує її стабільність.

Повторне використання ЛІБ сприяє зменшенню витрат на зберігання енергії. Виготовлення нових батарей є дорогим і ресурсозатратним процесом, що включає видобуток та переробку цінних матеріалів. Використання вже існуючих батарей дозволяє зменшити потребу в нових ресурсах, що позитивно впливає на економічну ефективність енергетичних проектів.

Деградація батарей та оцінка залишкової ємності

Для ефективного використання вторинних ЛІБ необхідно розробити надійні методи оцінки їх залишкової ємності та ефективності. Першим кроком у цьому процесі є проведення детального аналізу характеристик батарей, включаючи вимірювання ємності, внутрішнього опору та ефективності заряду/розряду. Ці показники надають важливу інформацію про поточний стан ЛІБ та дозволяють оцінити її потенціал для подальшого використання для зберігання енергії [8-9].

Визначення ступеня деградації ЛІБ є наступним важливим етапом у процесі оцінки. Деградація ЛІБ може відбуватися через різні механізми, такі як втрати активного матеріалу, зростання внутрішнього опору або пошкодження електроліту.

Прогнозування залишкового терміну служби ЛІБ є критично важливим для планування їх повторного використання. Розробляються моделі, які прогнозують залишковий термін служби ЛІБ на основі їх поточних характеристик та історії експлуатації. Ці моделі можуть враховувати різні фактори, представлені на Рис.2, такі як температура експлуатації, кількість циклів заряду/розряду та умови зберігання, що дозволяє забезпечити точність прогнозів та планування заміни батарей.

Рисунок 2 – Діагностичні та прогностичні моделі вторинного використання ЛІБ електротранспорту [10]

Використання надійних методів оцінки залишкової ємності дозволяє оптимізувати процес інтеграції вторинних батарей у енергетичні системи.

Аспекти ефективного використання

Вторинні батареї електротранспорту є перспективним рішенням для забезпечення надійного резервного джерела енергії, особливо для критично важливих об'єктів. Вони дозволяють накопичувати відновлювану енергію та забезпечувати її безперервне постачання, знижуючи залежність від традиційних джерел енергії. Застосування таких батарей стає особливо важливим для лікарень, диспетчерських центрів та інших об'єктів, де навіть короткочасні перебої електропостачання можуть мати серйозні наслідки. Завдяки оптимізації споживання накопиченої енергії вторинні батареї забезпечують тривалу підтримку важливих функцій у періоди перебоїв в електропостачанні.

Крім того, вторинні батареї сприяють балансуванню енергомережі, допомагаючи управляти піковими навантаженнями. Вони ефективно згладжують піки споживання, забезпечуючи збережену енергію в мережу у години максимального попиту. Це дозволяє знижувати навантаження на основні електростанції, зменшуючи витрати на виробництво енергії під час пікових періодів. Завдяки швидкому реагуванню на зміни навантаження, такі батареї можуть підтримувати стабільність і якість електроенергії у мережі, регулюючи частоту та підвищуючи загальну ефективність системи.

В умовах аварійних відключень вторинні батареї забезпечують резервну підтримку, автоматично підключаючись для підтримання електропостачання. Це сприяє енергетичній незалежності, особливо в місцевих мережах, де інтеграція таких батарей забезпечує більшу гнучкість та знижує залежність

від централізованих енергосистем. Наявність автономного джерела живлення підвищує стійкість енергетичних систем до природних катастроф та інших кризових ситуацій. Відомим прикладом є досвід автомобільних компаній, таких як Nissan, Mitsubishi та Toyota, які впроваджували технології Vehicle-to-Grid та вторинні батареї в Японії для забезпечення резервного живлення після стихійних лих.

Запровадження стратегій циркулярної економіки для літій-іонних батарей електротранспорту може значно знизити викиди CO_2, скоротити експлуатаційні витрати та забезпечити стабільне функціонування енергосистеми. Вторинні батареї не лише продовжують життєвий цикл ресурсів, але й сприяють сталому розвитку енергетики, інтегруючись у сучасні енергетичні стратегії.

Висновки

Використання вторинних літій-іонних батарей від електротранспорту в установках зберігання енергії є одним із ключових напрямів розвитку циркулярної економіки в сучасній енергетиці. Це рішення дозволяє ефективно використовувати ресурси, зменшуючи потребу у виробництві нових батарей і водночас знижуючи витрати на впровадження енергетичних систем. Вторинні батареї сприяють зменшенню викидів CO_2 завдяки повторному використанню матеріалів, а також мінімізують обсяг відходів, що відповідає глобальним цілям сталого розвитку.

Розробка методів та моделей для оцінки залишкової ємності та оптимального використання вторинних батарей є критично важливою для підвищення ефективності енергетичних систем. Інтегральний показник деградації, що враховує календарне та циклічне старіння, а також вплив зовнішніх факторів, дозволяє здійснювати точне прогнозування залишкової продуктивності батарей. Використання таких підходів сприяє оптимальному розподілу ресурсів, що забезпечує економічну доцільність і високий рівень надійності енергетичних рішень. Світовий досвід свідчить про життєздатність і ефективність використання вторинних батарей у критично важливих інфраструктурах, таких як лікарні, диспетчерські центри та інші об’єкти, де надійність електропостачання є пріоритетом.

1. Denysov, V. et al. (2024). Energy System Optimization Potential with Consideration of Technological Limitations. In: Zagorodny, A., Bogdanov, V., Zaporozhets, A. (eds) Nexus of Sustainability. Studies in Systems, Decision and Control, vol 559. Springer, Cham. https://doi.org/10.1007/978-3-031-66764-0_5.
2. Kostenko, G. (2023). Situation analysis of electric transport development prospects and its integration into Ukrainian power system. Power Engineering: Economics, Technique, Ecology, 1(71), 117–124. https://doi.org/10.20535/1813-5420.1.2023.276185.
3. Second Life Battery Capacity – Globally 2030. (2019). [WWW Document]. Statista. URL: https://www.statista.com/statistics/876624/global-second-life-battery-capacity/ (accessed: 08.08.2024).

4. Elis, S. (2023). Second Life Applications for Degraded EV Batteries: Evaluating Benefits Based on Remaining Useful Life and Battery Configurations [Thesis]. URL: https://urn.kb.se/resolve?urn=urn:nbn:se:liu:diva-196013 (accessed: 08.08.2024).
5. 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.
6. Pagliaro, M., & Meneguzzo, F. (2019). Lithium Battery Reusing and Recycling: A Circular Economy Insight. Heliyon, 5(6), e01866. https://doi.org/10.1016/j.heliyon.2019.e01866.
7. Lluc Canals Casals, B. Amante García, Camille Canal, Second life batteries lifespan: Rest of useful life and environmental analysis, Journal of Environmental Management, Volume 232, 2019, Pages 354-363, https://doi.org/10.1016/j.jenvman.2018.11.046.
8. Kostenko, G., & Zaporozhets, A. (2024). Transition from Electric Vehicles to Energy Storage: Review on Targeted Lithium-Ion Battery Diagnostics. *Energies*, *17*(20), 5132. https://doi.org/10.3390/en17205132.
9. Kostenko, G. (2024). Accounting Calendar And Cyclic Ageing Factors In Diagnostic And Prognostic Models Of Second-Life EV Batteries Application In Energy Storage Systems. System Research in Energy, (3 (79), 21-34. https://doi.org/10.15407/srenergy2024.03.021.

П.С. Шпилюр

ЕФЕКТИВНІСТЬ І БЕЗПЕКА ВИКОРИСТАННЯ СОНЯЧНИХ КОЛЕКТОРІВ У ДЕЦЕНТРАЛІЗОВАНІЙ ЕНЕРГЕТИЦІ

Сонячні колектори є одним із найперспективніших джерел енергії у децентралізованих енергосистемах, що сприяють сталому розвитку, енергетичній незалежності та зниженню вуглецевого сліду. Їх інтеграція у сучасну енергетику відповідає глобальним тенденціям переходу до відновлюваних джерел енергії та розвитку цифрових технологій.

У той же час впровадження сонячних колекторів у децентралізовані системи супроводжується низкою викликів. З одного боку, цифровізація відкриває нові можливості для підвищення ефективності управління та моніторингу енергосистем за допомогою Інтернету речей (IoT), штучного інтелекту (AI) та розумних мереж (Smart Grids). З іншого боку, ці технології вимагають вирішення питань кібербезпеки, захисту даних і стійкості до потенційних загроз.

Фізична безпека сонячних колекторів також є критично важливою, оскільки вони можуть бути піддані впливу екстремальних погодних умов, вандалізму чи інших ризиків. Усі ці фактори вимагають комплексного підходу до забезпечення ефективності та безпеки їх використання.

Таким чином, дослідження ефективності та безпеки сонячних колекторів у децентралізованій енергетиці є актуальним і важливим кроком до створення автономних, стійких та екологічно чистих енергосистем.

Інтелектуальна електроенергетична система – це енергосистема, оснащена адаптованою автоматичною системою оптимального управління процесами генерації, передавання, розподілу й споживання електроенергії. При цьому під інтелектуальністю варто розуміти здатність до самоорганізації та самонастроювання енергосистеми відповідно до заздалегідь визначених режимів функціонування без активної участі людини в процесі експлуатації в нормальних, аварійних і післяаварійних режимах. Інтелектуальні мережі включають комплекс технічних засобів, що дають можливість забезпечувати високу надійність електропостачання і якість електроенергії.[1]

Основні рішення для ефективності та безпеки сонячних колекторів у децентралізованій енергетиці Ефективність використання сонячних колекторів.

Сонячні колектори демонструють високу ефективність у виробництві енергії, особливо у децентралізованих енергосистемах:

- інтеграція з розумними мережами: Завдяки цифровим технологіям, таким як IoT і штучний інтелект, сонячні системи можуть забезпечувати 1

оптимальний розподіл енергії між споживачами, а також автоматизувати процеси управління.

- Прогнозування та оптимізація: Використання великих даних і алгоритмів машинного навчання дозволяє передбачати зміни погодних умов, визначати потреби споживачів і адаптувати роботу системи для максимізації продуктивності.

- Енергетична автономність: Встановлення сонячних колекторів дає змогу створювати автономні енергетичні системи, які зменшують залежність від традиційних централізованих мереж.

Кібербезпека в децентралізованих системах. Із поширенням цифрових технологій у децентралізованій енергетиці виникають ризики, пов'язані з кібербезпекою.

- Ризики кібератак: Автоматизовані системи, підключені до інтернету, є вразливими до кібератак, які можуть призводити до збоїв у роботі чи втрати даних.

- Захист даних: Важливим є впровадження шифрування даних, систем автентифікації користувачів і багаторівневого захисту.

- Системи раннього виявлення загроз: Використання штучного інтелекту для моніторингу мереж та ідентифікації аномальної активності дозволяє швидко реагувати на потенційні загрози.

- Децентралізовані рішення: Використання блокчейн-технологій може посилити безпеку передачі даних і забезпечити прозорість енергетичних транзакцій.

Фізична безпека сонячних колекторів. Фізична безпека сонячних колекторів є критично важливим аспектом їх ефективної та довготривалої експлуатації. Вона охоплює заходи, спрямовані на захист від природних катаклізмів, пошкоджень через людський фактор, технічні несправності та інші зовнішні впливи. Нижче детально розглянуто ключові аспекти фізичної безпеки.

- Стійкість до екстремальних умов: Сонячні колектори повинні витримувати сильний вітер, град, високі температури чи сильні морози. Для цього використовуються міцні матеріали та інноваційні конструкції.

- Оскільки сонячні колектори можуть бути об'єктами вандалізму або крадіжок, особливо у віддалених або незахищених місцях, необхідно впроваджувати комплексні заходи захисту такі як огородження території, встановлення охоронних огорож або шлагбаумів обмежують доступ до колекторів, камери спостереження зі здатністю фіксувати підозрілу активність та використання спеціальних болтів або систем захисту, що ускладнюють демонтаж панелей без спеціальних інструментів.

Збереження енергії. Інтеграція з акумуляторами: Використання акумуляторних систем дозволяє громадам накопичувати надлишкову енергію,

вироблену вдень, для її подальшого використання вночі або в похмуру погоду, коли виробництво енергії зменшується.

- Стабільність енергопостачання: Накопичена енергія гарантує безперебійне постачання електрики навіть за непередбачуваних змін погодних умов.

- Рівномірний розподіл енергії: Зберігання енергії допомагає уникнути пікових навантажень і забезпечити рівномірний розподіл електрики протягом доби.

Перешкоди впровадження сонячних колекторів у децентралізовану енергетику. Попри численні переваги сонячних колекторів, їх впровадження в децентралізовану енергетику стикається з низкою перешкод. Вони можуть бути технічними, економічними, соціальними та регуляторними.

Економічні перешкоди. Це, високі початкові витрати, недостатня фінансова підтримка та довгий період окупності. Необхідність та відсутність початкових інвестицій може стримувати впровадження, що вимагає державної підтримки.

Регуляторні та законодавчі перешкоди. Це невідповідність нормативної бази, обмеження на продаж надлишкової енергії та інші бюрократичні бар'єри.

Екологічні та геополітичні перешкоди. На це впливає залежність від імпорту обладнання та енергетичної політики.

Висновки Сонячні колектори відіграють ключову роль у децентралізованій енергетиці, сприяючи підвищенню енергоефективності та безпеки енергопостачання.

Оптимізація управління за допомогою цифрових технологій дозволяє підвищити ефективність роботи сонячних колекторів. Інтелектуальні системи управління можуть автоматично регулювати роботу колекторів залежно від погодних умов, споживання енергії та інших факторів, забезпечуючи максимальну продуктивність і економію ресурсів.

Для України використання переваг розумних енергетичних мереж є особливо актуальним, оскільки енергетична інфраструктура та системи сильно зношені як фізично, так і морально. Можливість оперативного та гнучкого управління інфраструктурою має вирішальне значення для балансування енергетичних потоків.[2]

1. «Системи режимно-технологічного управління електромережами та практика регулювання навантажень у енергосистемах зарубіжних країн з урахуванням розвитку поновлюваної енергетики», Відділ інформаційно-аналітичного забезпечення НТЦЕ НЕК «Укренерго», 2011р. https://ua.energy/wp-content/uploads/2018/01/3.-Systemy-rezhymnotehnologichnogo-upravlinnya.pdf.
2. Стан впровадження та розвитку Smart Grid та Smart Metering в енергетиці у європейських країнах, травень 2024 р., https://visnyk.fem.sumdu.edu.ua/issues/1_2021/36.pdf.

В.Р. Герасимов, В.В. Душеба

СУЧАСНІ ПІДХОДИ ДО ОПТИМІЗАЦІЇ БАЗ ДАНИХ ЗА ДОПОМОГОЮ ІНДЕКСІВ

Ключові слова: оптимізація баз даних, індекси, B-дерева, хеш-індекси, бітові карти, геопросторові індекси, машинне навчання, адаптивна індексація, NoSQL, реляційні СУБД, продуктивність, обробка даних, цифрова трансформація.

У сучасному світі бази даних відіграють ключову роль у функціонуванні інформаційних систем, забезпечуючи зберігання та обробку великих обсягів даних. В умовах зростання складності структур даних і збільшення запитів, оптимізація роботи баз даних стає критично важливим завданням для різних сфер, включаючи промисловість, фінанси, телекомунікації та енергетику. Одним із найефективніших інструментів для підвищення продуктивності є індекси, які дозволяють зменшити час виконання запитів і забезпечити швидкий доступ до інформації.

Це дослідження спрямоване на аналіз сучасних підходів до створення та налаштування індексів у базах даних, включаючи реляційні СУБД і NoSQL-системи. Розглянуто ефективність різних типів індексів та їх адаптацію до сучасних умов обробки даних.

Індекси є спеціалізованими структурами, що дозволяють значно скоротити час пошуку та обробки запитів, завдяки чому їх використання стає важливим для різноманітних задач, пов'язаних із великими обсягами даних. Серед основних типів індексів варто виділити B-дерева, хеш-індекси, бітові карти та геопросторові структури. Кожен із цих типів має свої переваги та обмеження.

B-дерева є універсальними та використовуються в більшості реляційних і NoSQL баз даних, таких як MongoDB [1]. Вони забезпечують баланс між швидкістю пошуку та операціями запису, хоча останні можуть бути дещо повільнішими при великій кількості індексів. Хеш-індекси забезпечують високу швидкість доступу за точним ключем, але не підтримують діапазонних запитів, що обмежує їх застосування. Бітові карти ефективні для колонкових баз даних і полів із невеликою кількістю унікальних значень, що робить їх ідеальними для агрегатних операцій. Геопросторові індекси, такі як R-дерева, широко використовуються для роботи з просторовими даними, але мають свої обмеження при динамічних змінах великих обсягів даних.

Сучасні підходи до оптимізації індексів включають використання алгоритмів машинного навчання, які дозволяють автоматично аналізувати робоче навантаження та адаптувати структури індексів. Наприклад, моделі, що базуються на глибокому навчанні з підкріпленням, можуть визначати оптимальну конфігурацію індексів для конкретних сценаріїв використання,

що дозволяє скоротити час виконання запитів на 15–30% [2]. Інший перспективний напрямок — адаптивні алгоритми, такі як Kaizen, які використовують історичні дані для налаштування індексів залежно від змін у характері запитів [3].

Крім того, розподілені NoSQL системи активно впроваджують механізми автоматичної індексації, які здатні ефективно працювати в умовах динамічних запитів і високого навантаження. Наприклад, проект HindEx демонструє значні переваги у масштабованих середовищах завдяки адаптивній оптимізації складних запитів [4].

Висновки

Оптимізація баз даних за допомогою індексів є важливим напрямом підвищення продуктивності інформаційних систем у різних галузях, включаючи промисловість, телекомунікації, фінансовий сектор і цифрову енергетику. Використання сучасних алгоритмів налаштування індексів, таких як машинне навчання та адаптивні моделі, дозволяє скоротити час виконання запитів, оптимізувати використання ресурсів і забезпечити гнучкість системи до змін у характері даних.

У сфері енергетики ефективне управління даними є критично важливим для прогнозування навантажень, аналізу роботи мереж і підтримки стабільності енергосистем. Впровадження адаптивних індексаційних механізмів і гібридних підходів може суттєво покращити продуктивність баз даних, що використовується для цих завдань, сприяючи загальному розвитку галузі в умовах цифрової трансформації.

1. Ankur S., Felix M. S., Jens D. The Case for Automatic Database Administration using Deep Reinforcement Learning. — URL: https://www.researchgate.net/publication/322568144_The_Case_for_Automatic_Database_Administration_using_Deep_Reinforcement_Learning (дата звернення 18.11.2024).
2. Dash D., Polyzotis N., Ailamaki A. CoPhy: A Scalable, Portable, and Interactive Index Advisor for Large Workloads // Proc. VLDB Endow. — 2011. — Vol. 4, no. 6. — Pp. 362–372.
3. Kaizen: A Semi-Automatic Index Advisor / I. Jimenez, H. Sanchez, Q.T. Tran, N. Polyzotis // Proceedings of the 2012 ACM SIGMOD International Conference on Management of Data. — SIGMOD ’12. — 2012. — Pp. 685–688.
4. Chopade R., Pachghare V. MongoDB Indexing for Performance Improvement // ICT Systems and Sustainability. Advances in Intelligent Systems and Computing / Ed. by M. Tuba, S. Akashe, A. Joshi. — Singapore: Springer, 2020. — Vol. 1077. — Pp. 338–347.

В.В. Оранський

ЦИФРОВІ ТЕХНОЛОГІЇ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЕНЕРГЕТИЧНОЇ БЕЗПЕКИ ТЕПЛИЦЬ: ВИКЛИКИ ТА МОЖЛИВОСТІ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ АГРОПРОМИСЛОВИХ СИСТЕМ

Теплиці є важливою частиною агропромислового комплексу України, забезпечуючи вирощування культур протягом всього року і підвищення врожайності. Однак, для забезпечення стабільної та ефективної роботи теплиць необхідно враховувати не лише оптимальні агротехнічні практики, але й енергетичні потреби. Теплиці потребують значних енергетичних ресурсів для підтримки температурного режиму, освітлення та вентиляції, що ставить перед ними завдання зменшення енергетичних витрат і забезпечення енергетичної безпеки.

Сільське господарство — один із найдавніших видів людської діяльності, який водночас є чудовим ґрунтом для впровадження новітніх технологій. Так, уже подейкують про Другу зелену революцію: інвестиційна компанія Goldman Sachs прогнозує, що продуктивність світового агробізнесу до 2050 року зросте на 70%. Такий прогноз частково базується на активному розвитку технології Internet of Things. Так з'явилася концепція smart farming, «розумних» ферм, коли до фермерського господарства підключають комунікаційні та інформаційні технології: за стадами стежать дрони, рослини садять після аналізу ґрунту, а в теплицях підтримують штучний мікроклімат [1].

Однією з ключових технологій, що сприяють розвитку «розумного» сільського господарства, є ефективне використання енергії, зокрема в теплицях, де цифрові рішення відіграють важливу роль у забезпеченні стабільної та економічної роботи.

Цифрові технології для оптимізації енергетичного споживання в теплицях.

Інтелектуальні енергетичні мережі (Smart Grids)

Інтелектуальні енергетичні мережі є важливим елементом для управління енергоспоживанням теплиць. Вони дозволяють здійснювати автоматичне регулювання енергетичних потоків, інтегруючи різні джерела енергії, включаючи відновлювальні (сонячні панелі, біогазові установки). Завдяки Smart Grids можна:

- Оптимізувати енергоспоживання теплиць, зменшуючи витрати на електроенергію та інші енергоресурси.
- Забезпечити стабільність енергопостачання, навіть в умовах нестабільності енергосистем, завдяки використанню відновлювальних джерел енергії.
- Моделювати енергетичні потреби теплиць в реальному часі та коригувати енергоспоживання в залежності від температури, вологості та

інших умов. Завдяки цифровим технологіям Smart Grids енергоспоживання може знижуватися до 15-20% завдяки інтеграції відновлювальних джерел енергії, автоматизації процесів і оптимальному розподілу енергетичних потоків.

Інтернет речей (IoT) для моніторингу енергоспоживання в теплицях. Розумні теплиці нині з'являються по всьому світу. У них застосовують такі технології, як світлодіодні ліхтарі, системи фільтрації повітря та зрошення. Серцем розумних теплиць є системи, що працюють від IoT (Internet of Things) «Інтернету речей», концепції мережі, що складається із взаємозв'язаних фізичних пристроїв, які мають вбудовані датчики, а також програмне забезпечення, що дозволяє здійснювати передавання і обмін даними між фізичним світом і комп'ютерними системами в автоматичному режимі за допомогою використання стандартних протоколів зв'язку. Датчики IoT надають інформацію про рівень освітленості, температуру та вологість. Інформація, зібрана цими датчиками, дає змогу операторові зробити середовище всередині теплиці якомога придатнішим для ефективного виробництва агропродукції. У розумних теплицях з'являється можливість вирощувати більшу кількість їжі завдяки точному налаштуванню усіх параметрів регулювання клімату за допомогою комп'ютерного інтелекту.

Витрати на виробництво продукції у таких розумних системах значно менші, ніж у разі застосування традиційних методів тепличного господарства [2].

Дослідження показують, що використання IoT у теплицях може знижувати енергоспоживання на 10-20% завдяки точному моніторингу і автоматизованому управлінню енергетичними системами.

Великі дані для оптимізації енергоспоживання та прогнозування

Застосування Big Data в агропромислових системах дозволяє збирати та аналізувати величезні обсяги даних про температуру, вологість, освітлення, а також енергетичні показники теплиць. Використання таких технологій допомагає:

- Прогнозувати енергетичні потреби теплиць на основі аналізу даних за певний період часу.
- Оптимізувати використання енергетичних ресурсів, забезпечуючи економічну ефективність і знижуючи витрати на енергію.
- Виявляти тенденції в енергоспоживанні та розробляти стратегії для зменшення витрат енергії.

Використання аналітики великих даних дозволяє досягти зниження енергоспоживання на 15% завдяки точному прогнозуванню потреб та оптимізації використання енергетичних ресурсів. У результаті зменшуються надмірні витрати енергії, що дозволяє знизити витрати на енергію та підвищити ефективність теплиць.

Використання відновлювальних джерел енергії для енергозабезпечення теплиць. Інтеграція відновлювальних джерел енергії в енергетичні системи

теплиць дозволяє зменшити залежність від традиційних джерел енергії та знижує витрати на електроенергію. Сонячні панелі, вітрові турбіни та біогазові установки можуть стати основними джерелами енергії для теплиць, забезпечуючи:

- Енергетичну незалежність теплиць та зниження витрат на енергію.
- Зниження екологічного сліду завдяки використанню чистих джерел енергії.
- Оптимізацію енергоспоживання через інтеграцію таких джерел в єдину енергетичну систему теплиць.

Завдяки використанню сонячних панелей, встановлених на дахах теплиць, можна покрити до 30% енергетичних потреб, що знижує витрати на енергію. Сонячні батареї інноваційне рішення для теплиць, яке дозволяє використовувати сонячну енергію як джерело живлення. На відміну від інших видів енергії, сонячна енергія нескінченна, екологічно чиста та доступна у більшості регіонів світу. Використання сонячних батарей для теплиці має безліч переваг, серед яких економія на електриці, збільшення продуктивності та покращення якості врожаю [3].

Висновки. Цифрові технології можуть значно підвищити ефективність енергозабезпечення теплиць в Україні, зменшуючи витрати на енергію та підвищуючи енергетичну безпеку агропромислових підприємств. Впровадження інтелектуальних енергетичних мереж, IoT, великих даних та відновлювальних джерел енергії є важливими кроками на шляху до забезпечення стійкого та економічно ефективного виробництва в агропромисловому секторі. За рахунок цифровізації можна знизити енергоспоживання теплиць на 15-30%, що має величезне значення для сталого розвитку агропідприємств.

1. IoT у сільському господарстві: https://hub.kyivstar.ua/articles/internet-rechej-u-silisikomu-gospodarstvi-8-porad.
2. Смартрішення в агросвіті (07.01.2022) https://ifarming.ua/itehnologii/selektsiya/smartrishennya-krokuyut-agrosvitom.
3. Теплиця на сонячних батареях https://energoseti.com.ua/uk/teplytsia-na-soniachnykh-batareiakh-innovatsijni-rishennia-dlia-efektyvnoho-vyroshchuvannia-roslyn/.

П.І. Щур, В.Ю. Зубок

РЕЗЕРВНЕ КОПІЮВАННЯ ЯК ІНСТРУМЕНТ ПІДВИЩЕННЯ КІБЕРСТІЙКОСТІ ЕНЕРГЕТИЧНИХ ОБ'ЄКТІВ

Кіберстійкість (Cyber Resilience, кіберрезилєнтність) — це здатність організації передбачати, виявляти, реагувати на інциденти інформаційної безпеки та готуватися до них, забезпечуючи швидке відновлення як під час інцидентів, так і після їх завершення [1]. Згідно затвердженого рішення Ради національної безпеки і оборони України "Про Стратегію кібербезпеки України" від 14 травня 2021 кіберстійкість визначається як набуття здатності швидко адаптуватися до внутрішніх і зовнішніх загроз у кіберпросторі, підтримувати та відновлювати стале функціонування національної інформаційної інфраструктури, насамперед об'єктів критичної інформаційної інфраструктури. А набуття кіберстійкості є невідємною складовою процесу створення максимально відкритого, вільного, стабільного і безпечного кіберпростору в інтересах забезпечення прав і свобод людини, соціального, політичного і економічного розвитку держави [2].

Рисунок 1 – Піраміда кіберстійкості: кібербезпека, управління ризиками, безперервність бізнесу, аварійне відновлення

Кіберрезильєнтність у контексті безпеки енергетичної інфраструктури вимагає створення надійної та адаптивної системи, яка здатна ефективно протистояти кіберзагрозам та забезпечувати безперервну роботу критичних енергетичних процесів. Це охоплює захист інформаційних систем енергетичних компаній, управління ризиками, які можуть призвести до перебоїв у роботі як окремих обєктів так і системи вцілому, забезпечення безперервності енергетичних операцій та розробку планів аварійного відновлення для швидкого реагування на інциденти. Основними елементами, що підтримують цілісну стратегію кіберстійкості є: кіберзахист (Cybersecurity), управління ризиками (Risk management), безперервність бізнесу (Business continuity), аварійне відновлення (Disaster recovery).

Резервне копіювання — це процес створення копій критичних даних інформаційних систем для їх відновлення у разі втрати або пошкодження. Цей процес забезпечує безперебійність енергетичних операцій при технічних збоях, атаках чи фізичних пошкодженнях. Резервні копії включають дані операційних систем, баз даних, конфігурацій та образи віртуальних машин, конфігурацію мережевих пристроїв тощо. В даних системах використовуються три основні типи резервних копій: снепшоти, бекапи та реплікація.

Снепшоти створюють знімки системи на конкретний момент часу, зберігаючи тільки зміни після останнього знімка. Вони дозволяють швидко відновлювати дані, але більше підходять для короткострокових збережень, а не для повного відновлення в разі серйозних збоїв. Бекапи можуть бути повними або інкрементними. Повний бекап зберігає всі файли, тоді як інкрементний — лише зміни від останнього збереження. Інкрементні бекапи займають менше місця, але для відновлення з них потрібно більше часу через залежність від кількох версій. Також недоліком таких копій є їх залежність один від одного та чутливість до пошкоджень. Реплікація — це процес постійного дублювання даних в реальному часі на інші сховища або сервери. Цей метод забезпечує високу доступність і надійність, хоча потребує значних ресурсів для ефективного виконання.

Для зберігання резервних копій використовуються різні типи сховищ. NAS (Network-Attached Storage) забезпечує централізоване зберігання даних для кількох серверів, а DAS (Direct-Attached Storage) дозволяє підключати сховище безпосередньо до одного сервера, забезпечуючи високу швидкість доступу, але з обмеженою масштабованістю. Storage Area Network (SAN) [3] — це мережа зберігання даних яка дозволяє зберігати резервні копії через мережу. Це дає змогу кільком користувачам або серверам доступатися до сховища, забезпечуючи гнучкість і масштабованість. SAN є більш ефективним для спільного доступу до резервних копій та зручним для великих організацій, де потрібно централізовано зберігати і керувати даними.

Один із важливих етапів реалізації системи резервного копіювання — визначення ключових параметрів для оцінки її ефективності, надійності та внеску в кіберстійкість організації. Основні часові метрики включають RTO (Recovery Time Objective), що вказує на цільовий час відновлення після аварії, який залежить від апаратних параметрів та швидкості реакції персоналу, і RPO (Recovery Point Objective), що визначає максимальний час, протягом якого можуть бути втрачені дані без критичних наслідків для системи. Ці показники мають відмінності: RTO оцінює доступність сервісів, а RPO — частоту резервного копіювання та допустимі втрати даних.

Інші важливі метрики включають період зберігання резервних копій (BRP - Backup Retention Period), який варіюється залежно від типу копії та вимог законодавства, а також вікно резервного копіювання, що визначає час, протягом якого створення копій не впливає на продуктивність системи.

Коефіцієнт успішності резервного копіювання вимірює відсоток успішних копій від загальної кількості спроб. Масштабованість резервного копіювання відображає здатність системи адаптуватися до зростання обсягів даних, а вартість резервного копіювання охоплює всі витрати на впровадження, підтримку та масштабування системи.

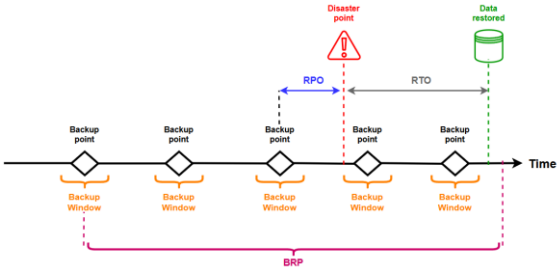


Рисунок 2 – Метрики оцінювання ефективності резервного копіювання

У результаті розгляду концепції кіберстійкості можна зробити висновки, що резервне копіювання є невід'ємною частиною стратегії кіберстійкості об'єктів енергетики. Правильне налаштування стратегії резервного копіювання включає вибір найбільш підходящих типів сховищ (NAS, DAS, SAN) і резервних копій (снепшоти, бекапи, реплікація), що дозволяє оптимізувати основні метрики, такі як RTO (Recovery Time Objective) та RPO (Recovery Point Objective), що визначають максимально допустимі часові межі відновлення після інцидентів і можливі втрати даних. Крім того, стратегія резервного копіювання повинна включати належне управління зберіганням копій, визначення періодів зберігання, а також оцінку ефективності системи через коефіцієнт успішності резервного копіювання та здатність до масштабування, що забезпечує її стійкість до зростання обсягів даних. Тільки в такому разі організації можуть забезпечити надійний захист інформаційної інфраструктури, гарантувати безперебійність енергетичних процесів і підтримувати стабільність функціонування навіть у випадку технічних збоїв або кіберінцидентів.

1. Swanson, M., Bowen, P., Wohl Phillips, A., Gallup, D., & Lynes, D. (2010, травень). *Contingency Planning Guide for Federal Information Systems*. nvlpubs.nist.gov. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf.
2. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України", Указ Президента України № 447/2021 (2021) (Україна). https://zakon.rada.gov.ua/laws/show/447/2021#Text.
3. *What is Storage Area Network (SAN)? | VMware Glossary*. (б. д.). VMware by Broadcom - Cloud Computing for the Enterprise. https://www.vmware.com/topics/storage-area-network-san.

С.В. Матвєєв, І.В. Івченко

ВПЛИВ ВИСОКОГО ЕНЕРГОСПОЖИВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ НА БЕЗПЕКУ ЕНЕРГЕТИКИ В ЕПОХУ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Анотація: Стаття аналізує вплив високого енергоспоживання систем штучного інтелекту (ШІ) на безпеку енергетичної інфраструктури в умовах цифрової трансформації. Швидке впровадження ШІ у промисловість, фінанси, охорону здоров'я та інші галузі значно підвищує навантаження на енергетичні системи, створюючи нові виклики для їх стабільності та стійкості. Окрему увагу приділено ризикам, пов'язаним із нестабільністю енергозабезпечення.

Цифрова трансформація стимулює широке впровадження ШІ у різні сектори, однак високі енергетичні потреби обчислювальних моделей ставлять під загрозу надійність енергетичних систем. Для обчислень ШІ, таких як тренування великих мовних моделей, використовується величезна кількість енергії, що дорівнює енергоспоживанню великих промислових об'єктів.

Енергоспоживання ШІ-систем варіюється залежно від типу алгоритму, його структури та інфраструктури, на якій він працює. Основними споживачами енергії є процеси навчання нейронних мереж та їх використання для інференсу (виведення результатів).

Навчання складних нейронних мереж, таких як GPT-3 або AlphaGo, може тривати кілька тижнів і потребує використання великих обчислювальних кластерів. Навчання однієї такої моделі може призвести до споживання тисяч мегават-годин енергії . Наприклад, дослідження показують, що тренування моделей із сотнями мільйонів або мільярдамі параметрів вимагає використання десятків тисяч графічних процесорів (GPU) на великих дата-центрах, що значно збільшує витрати електроенергії. Ось дані щодо енергоспоживання для забезпечення процесу навчання деяких моделей ШІ [1]:

- GPT-3 (175Г параметрів) – 1287 МВт·год;
- AlphaGo від DeepMind – біля 1000 МВт·год;
- BLOOM (176Г параметрів) від Hugging Face – близько 433 МВт·год;
- BERT (Google) – близько 1440 кВт·год.

Великі мовні моделі (LLM), такі як GPT-4 від OpenAI та BERT від Google, потребують ще більш значної кількості обчислювальних ресурсів, а значить і енергії.

Ці цифри підкреслюють важливість аналізу впливу ШІ на енергетику та впровадження енергоефективних рішень.

Інтенсивне енергоспоживання великих дата-центрів, які забезпечують роботу ШІ, створює значний попит на електричну енергію, що призводить до перевантаження регіональних енергетичних мереж. У 2023 році Google і Microsoft звітували про збільшення споживання електроенергії дата-центрами на 30% порівняно з попереднім роком. Розташування центрів обробки даних у густонаселених регіонах, таких як Каліфорнія, збільшує ризик перевантаження локальних енергетичних систем, що вже відчувають тиск через часті посухи та зміни клімату [2].

Існує кілька підходів до зниження енергоспоживання ШІ-систем, які вже застосовуються або розробляються.

Одним із рішень є зменшення кількості параметрів моделі або використання компресії даних. Компанії Google та OpenAI активно працюють над оптимізацією моделей, що дозволяє значно знизити споживання енергії без суттєвої втрати точності прогнозів або результатів. Методи прунінгу та квантизації дозволяють зменшити енергоспоживання, знижуючи складність обчислень. Наприклад, впровадження прунінгу у BERT дозволяє знизити енергоспоживання на 30% без втрати точності [3].

Використання спеціалізованих процесорів для глибокого навчання, таких як Tensor Processing Units (TPU) від Google або Graphcore IPUs, дозволяє значно знизити енергоспоживання завдяки більш ефективному використанню ресурсів. Ці чіпи спеціально розроблені для обробки нейронних мереж і споживають менше енергії, ніж традиційні графічні процесори .

Децентралізація енергосистеми та використання відновлюваних джерел енергії також сприяє зменшенню негативного впливу високого енергоспоживання ШІ на енергетику та екологію. Великий інтерес викликає перехід дата-центрів на відновлювані джерела енергії. Компанії Microsoft, Google та Amazon активно інвестують у проєкти, спрямовані на використання сонячної та вітряної енергії для живлення своїх дата-центрів. Хоча відновлювані джерела енергії можуть мінімізувати вплив на довкілля, їх нестабільність (наприклад, залежність від погодних умов) може створити ризики для підтримки сталого енергопостачання великих ШІ-систем. Тому великі компанії, такі як Microsoft, Google і Amazon, використовують можливості партнерства з компаніями, що працюють у сфері ядерного синтезу, щоб забезпечити доступ до енергії майбутнього. Загальний обсяг фінансування приватного сектору в галузі ядерного синтезу перевищив 7,1 мільярдів доларів у світі. Основними гравцями в цій галузі є Commonwealth Fusion Systems, яка залучила понад 2 мільярди доларів, та TAE Technologies

із загальним фінансуванням понад 1 мільярд. Інші помітні компанії, такі як Helion, SHINE, і General Fusion, також отримали суттєві інвестиції. Наприклад, Helion отримала 65 мільйонів доларів для розвитку своєї технології імпульсного синтезу[4].

Швидке зростання енергоспоживання систем ШІ створює нові виклики для енергетичної безпеки, що вимагає впровадження енергоефективних технологій та підвищення стійкості енергетичних систем. Поєднання інновацій у сфері ШІ, відновлюваної енергії та ядерного синтезу сприятиме адаптації до цифрової епохи.

1. Alexandra Sasha Luccioni, Sylvain Viguier, Anne-Laure Ligozat (3 November, 2022) Carbon Footprint of BLOOM *arXiv:* https://arxiv.org/pdf/2211.02001v1.
2. Alex de Vries (October 18, 2023) The growing energy footprint of artificial intelligence *Cell Journal: Joule* https://www.cell.com/joule/fulltext/S2542-4351(23)00365-3.
3. Andy Stone (host), Dion Harris, Benjamin Lee. (September 24, 2024). Why AI Consumes So Much Energy and What Might Be Done About It. *Penn's Kleinman Center for Energy Policy* .https://kleinmanenergy.upenn.edu/commentary/podcast/why-ai-consumes-so-much-energy-and-what-might-be-done-about-it/.
4. Nuclear Engineering International (October 9, 2024) *Fusion's growth trajectory* https://www.neimagazine.com/analysis/fusions-growth-trajectory/.

О.С. Потенко

ОЦІНКА ТА ОПТИМІЗАЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АВТОМАТИЗОВАНИХ СИСТЕМ ЗА МУЛЬТИКРИТЕРІАЛЬНИМ ПІДХОДОМ, ЩО ОХОПЛЮЄ «РИЗИК БЕЗПЕКИ – ГАРАНТІЯ БЕЗПЕКИ – ТИП ІД – ВАРТІСТЬ»

Розробка критеріїв оцінки інформаційної безпеки є важливим елементом забезпечення захисту даних та інформаційних систем в умовах сучасних загроз і викликів. Необхідність розробки таких критеріїв зумовлена низкою факторів, зокрема потребою в системному підході до виявлення вразливостей і загроз, оцінки ризиків та ефективного розподілу ресурсів для мінімізації можливих втрат. Правильна оцінка стану безпеки дозволяє визначити слабкі місця в інфраструктурі, обрати найкращі засоби захисту та своєчасно реагувати на потенційні інциденти.

Запропонований мультикритеріальний підхід (Рис.1) базується на чотирьох взаємопов'язаних факторах, що дозволяє ефективно обрати необхідний рівень захисту інформації. Спочатку проводиться оцінка ризику безпеки, яка дозволяє визначити ймовірність загроз і їх можливі наслідки для інформаційних ресурсів. Це допомагає зрозуміти, які загрози є найбільш серйозними і потребують підвищеної уваги.

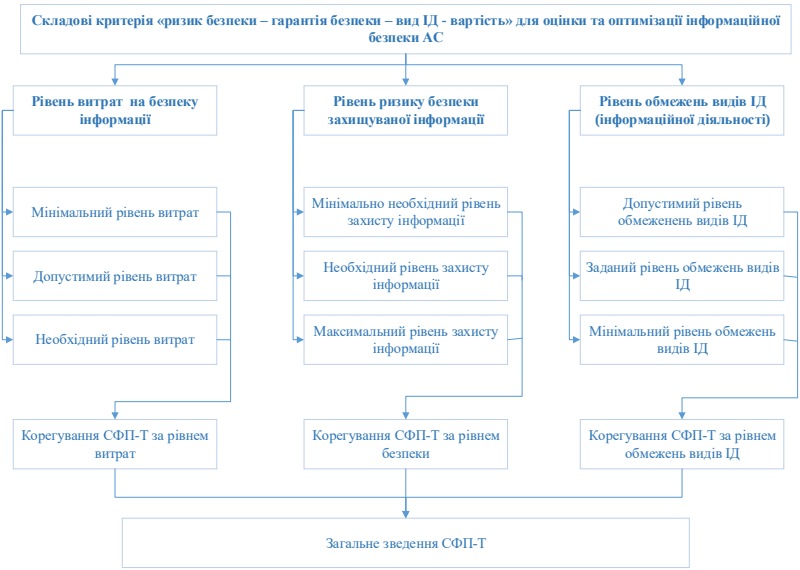


Рисунок 1 - Графічне відображення мультикритерія «ризик безпеки – гарантія безпеки – вид ІД - вартість»

Далі оцінюється гарантія безпеки, що відображає рівень захисту, який необхідно забезпечити для зменшення ймовірності реалізації цих загроз.

Також важливим є врахування виду інформаційної діяльності, оскільки різні типи інформації потребують різного рівня захисту. Наприклад, фінансова інформація або персональні дані мають бути захищені більш жорстко, ніж звичайні комерційні дані. Врахування цього аспекту дозволяє оптимізувати заходи безпеки, орієнтуючись на специфіку інформації.

Останнім критерієм є вартість заходів безпеки. Оцінка витрат дозволяє знайти баланс між необхідним рівнем захисту та фінансовими можливостями організації. У результаті такого підходу можна сформувати комплексну стратегію, яка забезпечить ефективний захист при мінімальних витратах, враховуючи всі ризики, вимоги до інформаційної діяльності та специфіку необхідного захисту.

Враховуючи вищесказане, розробимо метод оцінки та оптимізації інформаційної безпеки автоматизованих систем за мультикритеріальним підходом, що охоплює «ризик безпеки – гарантія безпеки – тип ІД – вартість»

Першим кроком є вибір профілю захищеності залежно від призначення автоматизованих систем [1].

На вимоги НД ТЗІ 2.5-005-99[1] необхідно накласти вектор виду інформаційної діяльності який включає в себе (1)

$$ВидІД = \begin{Bmatrix} ОІ \\ ВІ \\ ПІ \\ ЗІ \end{Bmatrix} \quad (2)$$

де ОІ – одержання інформації, ВІ – використання інформації, ПІ – поширення інформації, ЗІ – зберігання інформації.

На *другому* кроці методу здійснюється визначення класу АС та підкласів АС:

- Визначаємо клас АС.
- Визначаються підкласи відповідно до вимоги то тріади КЦД і в залежності від їх важливості.
- Вибирається діапазон можливих рівнів профілю для даної системи, відповідно до підкласу у відповідності з НД ТЗІ 2.5-005-99.

На *третьому* кроці методу починається оцінка складових критерію «ризик безпеки – гарантія безпеки – вид ІД – вартість» для оцінки та оптимізації інформаційної безпеки автоматизованої системи. Зокрема, на основі даних, отриманих на першому етапі, визначається рівень обмежень для видів інформаційної діяльності. Складова рівня ризику безпеки інформації, що підлягає захисту, отримує початкові дані і починає

обчислюватися на подальших етапах методу. Рівень витрат на забезпечення безпеки інформації буде визначений і скоригований на останньому етапі.

На *четвертому* кроці здійснюється обчислення цільової функції (1)[2, 3].

$$\Psi_i(xi) = [1-(1-\gamma i)]^{xi-ai} \qquad (1)$$

На *п'ятому* кроці здійснюється обчислення максимального значення математичного очікування втрат на об'єктах АС при оптимальному використанні функціонального профілю безпеки (ФПБ).

На *шостому* кроці в залежності від мети визначається чи досягнуті умови оптимізації і відповідно, якщо умови оптимізації не досягнуто, переходимо до нового обчислення цільової функції з новими умовами. Якщо умови оптимізації досягнуто, переходимо до наступного кроку методу.

На *сьомому* кроці перевіряється розподіл ФПБ по складовим автоматизованої системи (АС).

На *восьмому* кроці проводиться оцінка фінансових витрат на реалізацію заходів захисту та перевірка їх відповідності наявному бюджету. Якщо бюджет значно перевищує витрати, виникає можливість підвищити рівень захисту, що призводить до зміни умов оптимізації та повторення кроків методу.

На *дев'ятому* кроці відбувається загальне зведення ФПБ.

Запропонований мультикритерій «ризик безпеки – гарантія безпеки – вид ІД – вартість» дозволяє шляхом послідовної виваженої оцінки кожного з елементів, таких як гарантія безпеки, вид інформаційної діяльності та вартість, ефективно сформувати необхідний набір послуг безпеки. Цей підхід дає змогу в формальному вигляді визначити найбільш підходящий рівень захисту, враховуючи різні фактори, що впливають на інформаційну безпеку автоматизованої системи.

1. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
2. Richard E. Bellman. Dynamic Programming. - Princeton University Press, 2010. – 392 p.
3. Шорошев В.В, Давиденко А.Н. Потенко А.С. Оценка профилей противодействия угрозам на основе динамического программирования с использованием принципа Р. Беллмана // Моделювання та інформаційні технології: Зб.наук.праць ІПМЕ НАН України. – Київ, 2010. – Вип. 55 – С.82-87.

В.В. Шкарупило, В.В. Душеба, О.А. Чемерис

ЩОДО ТРИВИМІРНОЇ КОНЦЕПЦІЇ ОПРАЦЮВАННЯ РЕЗИЛІЄНТНОСТІ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ

Актуальні ризики, що постають перед об'єднаною енергосистемою України (ОЕС-У), у визначальній мірі обумовлені неспровокованим повномасштабним вторгненням країни-агресора зі Сходу, початок якого мав місце 24 лютого 2022 р. Зазначена подія є комплексною і багатовимірною. Підтвердженням тому слугують, у тому числі, і різноманітні події, що передували вказаній. Серед найбільш показових – масштабна кібератака на енергетичну інфраструктуру України у грудні 2015 р. Результатом стало відключення від ОЕС-У близько 225 тисяч споживачів [1]. Вказана подія є підтвердженням значимості ґрунтовного опрацювання ризиків, що постають у кібернетичній площині.

Ризики площини фізичної, у свою чергу, є не менш критичними. Показовими представниками у даному контексті є, наприклад, наступні: серії ракетних обстрілів від лютого по листопад 2022 р., результатом яких стало пошкодження близько 40% генеруючих і передавальних можливостей ОЕС-У [2]; подія, що відбулась 16-17 листопада 2024 р. – масштабна ракетна атака на енергосистему, у результаті якої було виведено з ладу значну кількість електричних підстанцій, означених Міжнародним агентством з атомної енергії як критичні [3].

Охоплені приклади, а також подібні, є обґрунтуванням доцільності оперування поняттям «резилієнтності» [4], і застосування при цьому комплексного підходу [5]. Вказаний підхід, у свою чергу, засновується на розробленій концепції, згідно якої опрацюванню підлягають три виокремлені концептуальні площини (виміри) [6] (рис. 1).

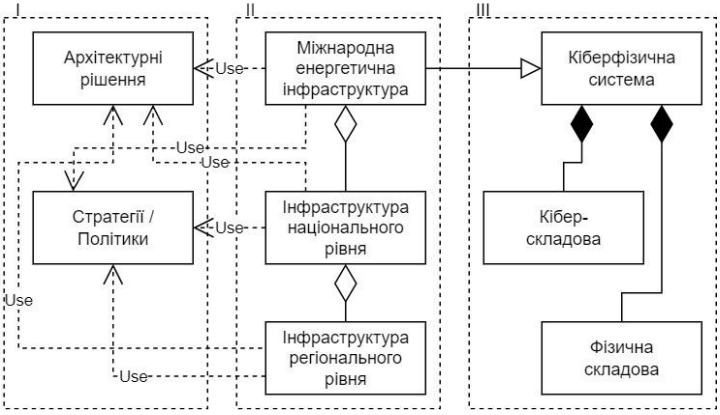


Рисунок 1 – Графічне подання розробленої тривимірної концепції

На рисунку 1 зведено три виокремлені концептуальні площини, представлені і сполучені із залученням засобів UML (Unified Modeling Language) [7].

Дослідження проведено в рамках вирішення задач наступних науково-дослідних робіт, виконуваних в Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України: «Кіберризики та кіберзахищеність топології розподілених інформаційних систем в глобальному кіберпросторі», за договором з МОН України № РН/15 - 2023 від 24.05.2023; W911NF-22-2-0153 research work, funded by the US Army Engineer Research and Development Center (ERDC); науково-дослідної роботи № 0120U102683 «Розроблення спеціалізованих комп'ютерних технологій моделювання та опрацювання оперативної інформації в задачах енергетики».

1. Pricop, A.-I., Gavrilaş, M., Sălceanu, A., & Neagu, B.-C. (2023). Power systems resilience against cyber-attacks. A systematic analysis. *2023 10th International Conference on Modern Power Systems, MPS 2023*, Cluj-Napoca, Romania. https://doi.org/10.1109/MPS58874.2023.10187420.
2. Nikolaieva, I., & Zwijnenburg, W. (2022, December). Risks and impacts from attacks on energy infrastructure in Ukraine. PAX report. https://paxforpeace.nl/wp-content/uploads/sites/2/import/2023-01/PAX_Ukraine_energy_infrastructure_FIN.pdf.
3. International Atomic Energy Agency. (2024, November 21). *Update 261 – IAEA Director General Statement on Situation in Ukraine*. https://www.iaea.org/newscenter/pressreleases/update-261-iaea-director-general-statement-on-situation-in-ukraine.
4. Linkov, I. et al. (2014). Changing the resilience paradigm. *Nature Climate Change*, 4, 407–409. https://doi.org/10.1038/nclimate2227.
5. Шкарупило, В.В., Душеба, В.В., & Тіменко, А.В. (2023). Огляд рівнів забезпечення резилієнтності у галузі енергетики. Survivability & Resilience – 2023: collection of materials of the international scientific and practical conference, Kyiv, October 19, 2023, PIMEE of NAS of Ukraine, 33–34. https://ipme.kiev.ua/konferencii/zhivuchist-ta-rezilyentnist-2023/.
6. Шкарупило, В.В., Чемерис, О.А., & Душеба, В.В. (2024). Стратифікований підхід до опрацювання резилієнтності у галузі енергетики. *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., 54-55. https://ipme.kiev.ua/konferencii/konferenciya-molodix-vchenix-2024/.
7. Shkarupylo, V., Chemerys, O., Artemchuk, V., Alsayaydeh, J., Kudermetov, R., & Polska, O. (2024). Comprehensive stratified approach to energy resilience solutions taxonomy: a Ukraine scenario. Proc. *14th International Conference on Dependable Systems, Services and Technologies*, Greece, Athens, October 11-13, 2024. (in press).

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

ПОВЕРХНЯ АТАКИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Поверхнею атаки соціальної інженерії визначаються варіанти впливання зловмисників на працівників організації [1]. Це дозволяє їм отримувати доступ до інформації [2] і, як наслідок, впливати на її діяльність [3]. Під кожним з варіантів здебільшого розуміються методи здійснення атак соціальної інженерії. Таке тлумачення до того ж доповнюється урахуванням каналів і даних [2], потреба в яких обумовлюються відповідним методом. Наприклад, у процесі фішингу одним із каналів впливання соціального інженера на працівника організації може бути електронна пошта. Тоді як дані про нього можуть отримуватися за результатами розвідки на основі відкритих джерел (англ. Open source intelligence, OSINT) [4]. Тож поверхнею атаки соціальної інженерії відображається сукупність уразливостей працівників організації. Кожна з них вважається потенційною точкою доступу зловмисника до інформації.

Перш за все уразливості працівників організації і, як наслідок, поверхня атаки визначаються направленістю використання соціальної інженерії [5, 6]. Об'єктом такого впливання є свідомість (підсвідомість) людини. Воно характеризується цілеспрямованістю, «проти волі працівника організації, але за його згодою». Наприклад, поверхня атаки соціальної інженерії може визначатися у межах урахування таких аспектів [7]:

1. *Пізнання та знання*. Визначаються здобутим досвідом або готовністю до отримання нових знань працівниками організації. Це проявляється у їх здатності обирати практичні рішення при виконанні або покладених на них обов'язків, або поставлених завдань. До того залежить від типовості/нетиповості навколишнього середовища і може ускладнюватися у випадках появи, змінення обставин. Результативність даної діяльності обумовлюється інерційністю мислення працівника організації, а також рівнями його конформності і потреби в пізнанні. Наприклад, з огляду на необізнаність можуть завантажуватися і відкриватися сумнівні вкладення електронної пошти [6–8].

2. *Поведінка та звички*. Визначаються шаблонною поведінкою працівників організації. Здебільшого вона формується як серія інстинктивних дій в типових умовах діяльності працівника. Такі дії характеризуються автоматичністю, мимовільністю і добровільністю. Вони можуть проявлятися з огляду на неуважність, недостатність або залишеність поза увагою забезпечення інформаційної безпеки. В даному випадку шаблонність поведінки обумовлюється звичками працівників організації і може проявлятися через неуважність, легковажність, лінь. Наприклад, через легковажність працівник організації переходить за сумнівним посиланням попри заборону такої діяльності [6–8].

3. *Емоції та почуття*. Визначаються ставлення працівників організації до виконання завдань або дотримання настанов зі забезпечення інформаційної безпеки. Це обумовлюється впливанням людських факторів. Серед них виокремлюються, по-перше, страх, цікавість, хвилювання, гнів. По-друге,

смуток, провина. Першим різновидом визначаються емоції працівників організації. Тоді як другим – їхні почуття. І емоції, і почуття впливають на діяльність працівників організації і насамперед в нетипових ситуації можуть призводити до порушень інформаційної безпеки. Наприклад, соціальний інженер може спонукати працівника організації до страху перед покаранням за використання неліцензійного програмного забезпечення [6–8].

4. *Психологічний фактор*. Визначається людською природою, індивідуальними характеристиками працівників організації. Ними встановлюються моделі їхньої поведінки. Вони різні в кожного працівника організації і, як наслідок, впливають на дії як в типових, так і нетипових ситуаціях забезпечення інформаційної безпеки. Характерною особливістю використання соціальними інженерами індивідуальних характеристик є мова. Її застосування може дозволяти маніпулювати або обманювати жертву. Наприклад, соціальний інженер може телефонувати та представлятися службовою підтримки банку та намагатися спонукати працівника до повідомленням отриманого коду для доступу до гаманця [6–8].

Отже, поверхня атаки соціальної інженерії відображає уразливості працівників організації з погляду забезпечення інформаційної безпеки. Об'єктом такого впливання є їхня свідомість (підсвідомість). Це дозволяє соціальному інженеру цілеспрямовано впливати на працівника «проти волі, але за його згодою». Тоді як результативність такої діяльності передбачає урахування відповідних психологічних факторів. Загалом ними формується поведінка працівників організації у типових і нетипових ситуаціях.

1. International Organization for Standardization. (2023). *Cybersecurity. Guidelines for Internet security* (ISO/IEC Standard No. 27032:2023). https://www.iso.org/standard/76070.html.
2. Theisen C., Munaiah N., Al-Zyoud M., Carverc J., Meneely A, Williamsa L. (2024). Attack surface definitions: A systematic literature review. *Information and Software Technology*. 104. 94–103. https://doi.org/10.1016/j.infsof.2018.07.008.
3. Cuchta T., Blackwood B., Devine T. R., Niichel R. J. (2023). View Affiliations. Human risk factors in cybersecurity. Experimental assessment of an academic human attack surface. Interaction Studies. 24 (3). 437–463. https://doi.org/10.1075/is.22053.cuc.
4. Gray J. (2022). Practical Social Engineering : A Primer for the Ethical Hacker. No Starch Press.
5. Attack Surface Analysis Cheat Sheet. OWASP. https://cheatsheetseries.owasp.org/cheatsheets/Attack_Surface_Analysis_Cheat_Sheet.html.
6. 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*. Vol. 2067. (p. 92–98). CEUR Workshop Proceedings. http://ceur-ws.org/Vol-2067/paper13.pdf.
7. Wang Z., Zhu H., Sun L. (2021). Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods. *IEEE Access*. 9. 11895–11910. https://doi.org/10.1109/access.2021.3051633.
8. Burda P., Allodi L., Zannone N. (2024). Cognition in Social Engineering Empirical Research: A Systematic Literature Review. *ACM Transactions on Computer-Human Interaction*. 31 (2). 1–55. https://doi.org/10.1145/3635149.

Я.Ю. Дорогий, В.В. Цуркан, О.О. Дорога-Іванюк

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ПРИ ЗАХИСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УСТАНОВ ЕНЕРГЕТИЧНОЇ ГАЛУЗІ

Анотація. У статті розглянуто використання штучного інтелекту (ШІ) для захисту критичної інфраструктури енергетичних установ. Розкрито можливості ШІ у протидії кібератакам та забезпеченні стабільного функціонування систем енергозабезпечення. Особливу увагу приділено ризикам, спричиненим агресією російської федерації, а також обговорено потенційні рішення на основі технологій ШІ, що допомагають посилити захист від зовнішніх та внутрішніх загроз.

Вступ. Критична інфраструктура енергетичної галузі є фундаментальною для забезпечення національної безпеки України, оскільки від її стабільного функціонування залежить робота більшості інших секторів, зокрема військового, транспортного, медичного. Енергетичні установи України вже тривалий час стикаються з численними викликами, пов'язаними з агресією рф, яка застосовує широкий спектр методів для порушення роботи об'єктів енергетичної інфраструктури. Основні загрози включають кібератаки, фізичне пошкодження об'єктів, внутрішні інсайдерські загрози та обмеженість ресурсів для реагування на інциденти. В умовах таких викликів технології штучного інтелекту стають важливим інструментом, що допомагає вчасно виявляти та реагувати на загрози, а також оптимізувати процеси захисту.

Проблематика захисту енергетичної інфраструктури в умовах агресії рф. Енергетичні установки, зокрема електричні станції, лінії передачі, об'єкти зберігання та розподілу енергії, є пріоритетними цілями для кібератак та фізичних нападів. В останні роки рф активізувала свої дії, спрямовані на дестабілізацію української енергетичної галузі. Основні напрямки атак включають:

1. *Кібератаки на енергосистеми*. З початку військової агресії російські хакери неодноразово здійснювали складні атаки на системи керування енергопостачанням. Зокрема, кібератаки BlackEnergy та Industroyer (2015 та 2016 роки) призвели до масштабних відключень електропостачання в Україні [1]. Такі атаки спрямовані на виведення з ладу систем SCADA (Supervisory Control and Data Acquisition), які є критичними для моніторингу та управління енергетичними мережами. Штучний інтелект може допомогти у виявленні цих загроз шляхом аналізу мережевої активності в режимі реального часу та виявлення аномалій, які можуть свідчити про зловмисну активність.

2. *Фізичні атаки на об'єкти енергетики*. Пошкодження трансформаторів, підстанцій та іншого обладнання, спричинені ракетними ударами та обстрілами, стають частими подіями в умовах військової агресії.

ШІ може допомогти у моніторингу стану фізичних компонентів енергосистем за допомогою безпілотних літальних апаратів, обладнаних сенсорами. Це дозволить проводити швидке виявлення пошкоджень та планувати оперативні ремонтні роботи.

3. *Внутрішні загрози та інсайдерська діяльність*. Окрім зовнішніх загроз, існують також інсайдерські ризики, коли співробітники або особи, які мають доступ до систем, можуть сприяти порушенню функціонування об'єктів енергетичної інфраструктури. ШІ може застосовуватися для автоматизованого аналізу поведінки користувачів у системах, щоб виявляти підозрілі дії, які можуть вказувати на потенційну інсайдерську загрозу.

Використання штучного інтелекту для забезпечення кібербезпеки енергетичних установ. Сучасні технології ШІ можуть виконувати численні завдання, пов'язані із забезпеченням кібербезпеки. Серед них:

1. *Аналіз загроз і раннє виявлення аномалій*. Алгоритми ШІ, що використовуються для аналізу великих обсягів даних, допомагають виявляти аномальні патерни активності, що можуть бути ознакою кібератак. Наприклад, методи машинного навчання можуть знаходити підозрілі операції, які вказують на можливе втручання у функціонування мережевих систем.

2. *Розширений моніторинг системи*. Використання ШІ дозволяє безперервно аналізувати трафік та активність в інформаційних мережах енергетичних об’єктів. Такі системи можуть розпізнавати новітні типи шкідливого ПЗ та інші кіберзагрози, що робить можливим оперативне реагування на загрози, що з’являються.

3. *Автоматизація процесів реагування*. За допомогою ШІ стає можливим автоматизувати процеси реагування на кіберзагрози, що дозволяє знизити навантаження на персонал та зменшити час між виявленням та нейтралізацією загрози. Зокрема, алгоритми ШІ можуть автоматично ізолювати підозрілі пристрої від мережі для зменшення шкоди від потенційної атаки.

Використання ШІ для фізичного моніторингу об’єктів енергетичної інфраструктури. Фізичний захист об'єктів критичної інфраструктури є важливим елементом забезпечення їх стійкості. Використання ШІ в поєднанні з сенсорами та безпілотними апаратами може значно покращити здатність до моніторингу та управління об'єктами енергетичної інфраструктури. Основні напрямки використання:

1. *Дрони для виявлення фізичних пошкоджень*. Застосування безпілотників з ШІ-аналізом зображень дозволяє автоматизувати процес моніторингу об’єктів. За допомогою візуального аналізу та тепловізійних камер такі дрони можуть виявляти пошкодження інфраструктури, спричинені фізичними атаками, та передавати дані для швидкого ремонту.

2. *Сенсорні мережі для раннього виявлення аварій*. Установки, обладнані мережами сенсорів, можуть передавати дані в реальному часі для

аналізу ШІ. Це дозволяє швидко ідентифікувати несправності або критичні зміни у роботі обладнання, що мінімізує ризик масштабних аварій.

Прогнозування та оцінка ризиків з використанням ШІ. Однією з найбільш перспективних можливостей використання ШІ в енергетичній галузі є прогнозування ймовірних загроз та оцінка ризиків для критичної інфраструктури. ШІ дозволяє здійснювати детальний аналіз минулих інцидентів, а також поточного стану систем, що дозволяє створити точні прогнози щодо майбутніх атак і сприяє покращенню стратегії захисту енергетичних об'єктів. Такі системи можуть стати важливим інструментом у боротьбі з кіберзагрозами, дозволяючи енергетичним компаніям вчасно реагувати на потенційні загрози.

Основними напрямками застосування ШІ можуть бути:

1. *Прогнозування інцидентів на основі даних про атаки*. Використовуючи великі обсяги історичних даних про попередні кібератаки, ШІ може ефективно прогнозувати ймовірність нових атак на енергетичну інфраструктуру. За допомогою алгоритмів машинного навчання та аналізу патернів у даних про атаки, ШІ здатний ідентифікувати тренди і повторювані моделі, що можуть свідчити про підготовку до нових інцидентів. Ці алгоритми здатні враховувати різноманітні фактори, такі як тип атак, методи проникнення, вразливості в системах та особливості хакерських угруповань, що здійснюють напади.

Наприклад, якщо система спостерігає підвищену активність певних кіберзагроз у інших секторах або регіонах, ШІ може передбачити ймовірність того, що ці загрози також можуть поширитись на енергетичну інфраструктуру. Така обізнаність дозволяє заздалегідь вжити заходів, таких як оновлення безпеки або зміна тактик захисту.

2. *Аналіз вразливостей системи та оцінка ризиків*. Оцінка ризиків є важливим аспектом для виявлення слабких місць у критичних енергетичних інфраструктурах. Завдяки використанню ШІ, можна створити моделі, які прогнозують, де саме система має найбільшу вразливість до потенційних атак. ШІ здійснює постійний моніторинг і виявляє нетипові аномалії в роботі систем, які можуть свідчити про спроби проникнення чи інші шкідливі дії. В результаті цієї роботи, алгоритми здатні оцінити ступінь ризику для кожного з об'єктів енергетичної інфраструктури і, на основі цих даних, надавати конкретні рекомендації для зниження цього ризику.

3. *Автоматичне оновлення заходів безпеки*. ШІ може допомогти в автоматичному оновленні заходів безпеки на основі прогнозів і оцінки ризиків. Наприклад, алгоритми машинного навчання здатні адаптуватися до нових загроз і атак, змінюючи налаштування системи безпеки в реальному часі. Якщо ШІ виявить нові вразливості або зростання ймовірності атак у певній частині енергетичної інфраструктури, система може автоматично вжити відповідних заходів для зміцнення захисту, включаючи оновлення антивірусного програмного забезпечення, зміни в параметрах мережевого захисту або впровадження додаткових бар'єрів безпеки.

4. *Інтеграція з іншими системами безпеки*. Важливою перевагою використання ШІ є можливість інтеграції з іншими системами безпеки, що дозволяє створювати комплексні системи моніторингу та захисту. ШІ може працювати в тандемі з існуючими технологіями захисту, такими як фаєрволи, системи виявлення вторгнень (IDS) [2] та системи управління інцидентами (SIEM) [3]. Такий подхід дозволяє отримати більш точну картину загроз і забезпечує більш ефективне реагування на інциденти. Таким чином, прогнозування і оцінка ризиків за допомогою ШІ не лише підвищує рівень безпеки енергетичних об'єктів, але й інтегрує різні технології для комплексного захисту.

5. *Динамічне оновлення прогнозів з урахуванням поточних умов*. Однією з ключових переваг ШІ є можливість динамічного оновлення прогнозів у реальному часі. Коли змінюються умови, такі як зростання активності хакерських угруповань або зміна зовнішніх факторів, ШІ може швидко адаптувати свої прогнози, забезпечуючи постійне оновлення стратегій захисту. В умовах сучасного агресивного середовища здатність оперативно адаптувати прогнози та стратегічні рішення буде важливою перевагою для енергетичних компаній.

Підсумовуючи вищенаведене, використання таких можливостей дозволить енергетичним компаніям бути готовими до ймовірних атак і ефективно розподіляти ресурси для захисту своїх критичних інфраструктур. Завдяки прогностичним можливостям ШІ, енергетична галузь здатна значно покращити свої системи безпеки, знижуючи ризик кібератак і мінімізуючи потенційні збитки від інцидентів.

Висновки. Агресія рф створює численні виклики для захисту критичної інфраструктури енергетичної галузі України. У цих умовах використання штучного інтелекту стає невід'ємною частиною забезпечення надійності та безпеки енергетичних систем. ШІ не лише дозволяє автоматизувати моніторинг і виявлення загроз, але й надає можливості для прогнозування інцидентів, що значно підвищує ефективність захисту. Застосування технологій ШІ у кібербезпеці та фізичному захисті енергетичних об'єктів сприятиме зменшенню ризиків, забезпечуючи стабільне функціонування енергетичної інфраструктури в умовах агресії.

1. Повернення Industroyer: нові кібератаки на енергетичний сектор в Україні / Softico. URL: https://softico.ua/uk/news/povernennya-industroyer-novi-kiberataki-na-energetichnij-sektor-v-ukrayini/ (дата звернення: 02 листопада 2024).
2. Захист критичної інфраструктури: як зберегти безпеку в умовах нових кіберзагроз / Wezom. URL: https://wezom.com.ua/ua/blog/zahist-kritichnoyi-infrastrukturi (дата звернення: 12 листопада 2024).
3. Захист критичної інфраструктури: аналіз сучасних підходів / Науково-інформаційний журнал «Науковий вісник» НУОУ. DOI: 10.28925/295272. URL: https://sit.nuou.org.ua/article/download/295272/295497/700877 (дата звернення: 13 листопада 2024).

ЗМІСТ

МАТЕРІАЛИ
VI НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«БЕЗПЕКА ЕНЕРГЕТИКИ В ЕПОХУ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ»

13 грудня 2024 року
м. Київ

Формат 60×90/16. Тираж 100.
Підписано до друку 30.11.2023. Заказ № 10

Інститут проблем моделювання в енергетиці
ім. Г.Є. Пухова Національної академії наук України,
Україна, 03164, Київ, вул. Генерала Наумова, 15,
тел.: +38 044 424 10 63
https://ipme.kiev.ua/, ipme@ipme.kiev.ua