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

XLIII
НАУКОВО-ТЕХНІЧНА КОНФЕРЕНЦІЯ МОЛОДИХ ВЧЕНИХ ТА СПЕЦІАЛІСТІВ ІНСТИТУТУ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ ІМ. Г.Є. ПУХОВА НАН УКРАЇНИ

ПРИСВЯЧЕНА ДНЮ НАУКИ В УКРАЇНІ

Збірник матеріалів конференції
14 травня 2025 р.

Київ – 2025

УДК 621.3 + 004 + 519.6 : 620.9

Рекомендовано до друку Вченою радою
Інституту проблем моделювання в енергетиці
ім. Г.Є. Пухова НАН України
(протокол №4 від 24 квітня 2025 р.)

Організаційний комітет:
В.В. Мохор, В.О. Артемчук, А.В. Яцишин та ін.

Програмний комітет:
В.В. Мохор, В.О. Артемчук, О.О. Попов та ін.

Відповідальний за випуск:
В.О. Артемчук

Collection of materials of the XLIII Scientific and technical conference of young scientists and specialists of G.E. Pukhov Institute for Modelling in Energy Engineering of National Academy of Sciences of Ukraine, Kyiv, May 14, 2025 / PIMEE of NAS of Ukraine. - 2025. - 144 p.

Збірник матеріалів XLIII Науково-технічної конференції молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, м. Київ, 14 травня 2025 р. / ІПМЕ ім. Г.Є. Пухова НАН України. – 2025. – 144 с.

ЗМІСТ

В.О. Мірошник

ПРОГНОЗУВАННЯ ГЕНЕРАЦІЇ ТА СПОЖИВАННЯ ЕЛЕКТРОЕНЕРГІЇ АКТИВНИМ СПОЖИВАЧЕМ

У сучасних умовах трансформації енергетичних систем у напрямку децентралізації та широкого впровадження відновлюваних джерел енергії (ВДЕ), активні споживачі (просюмери), які одночасно споживають та виробляють електроенергію, відіграють ключову роль. Це зумовлює необхідність точного прогнозування як споживання, так і генерації електроенергії для забезпечення ефективного управління енергетичними ресурсами та стабільності мережі.

Зростання кількості просюмерів, особливо в контексті мікромереж та енергетичних спільнот, створює нові виклики для прогнозування енергетичних потоків. Нестабільність генерації від ВДЕ, таких як сонячна та вітрова енергія, у поєднанні з варіативністю споживання, ускладнює процес балансування енергетичних систем.

У науковій літературі представлено різноманітні підходи до прогнозування енергетичних параметрів просюмерів. Зокрема, дослідження [1] порівнює ефективність моделей LASSO та Random Forest для прогнозування енергетичного балансу в мікромережах, виявляючи переваги Random Forest у короткострокових прогнозах. Інше дослідження [2] пропонує оптимізаційний підхід для управління енергією в розумних будинках, використовуючи комбінацію K-medoids та Elman нейронних мереж для прогнозування генерації та споживання. Також, в [3] аналізують різні методи прогнозування, включаючи SARIMA, нейронні мережі та SVM, для інтеграції просюмерів у розумні мережі.

Прогнозування енергетичних параметрів активного споживача є більш складним завданням порівняно з прогнозуванням генерації сонячної електростанції.

У випадку сонячної електростанції, прогнозування генерації базується переважно на метеорологічних даних, таких як сонячна радіація, температура та хмарність. Ці параметри мають відносно передбачуваний характер, особливо в умовах ясного неба, що дозволяє досягати високої точності прогнозів. Наприклад, дослідження показують, що при ясному небі середня абсолютна похибка прогнозу (MAPE) може становити близько 9.8%, тоді як при хмарних умовах вона зростає до 42% [4].

Споживання електроенергії залежить від поведінки користувача, часу доби, дня тижня та інших соціально-економічних факторів, що робить його менш передбачуваним. Це вимагає використання складніших моделей, які можуть враховувати взаємозв'язки між різними параметрами та адаптуватися до змінних умов. Вибір методів прогнозування повинен враховувати специфіку даних, цілі прогнозування та доступні ресурси.

Таблиця 1 – Переваги та недоліки різних методів прогнозування

Метод	Переваги	Недоліки
Статистичні (ARIMA)	Висока інтерпретованість моделей та здатність добре відображати сезонні й трендові компоненти даних	Погано враховують нелінійні залежності й мультивимірні взаємозв'язки, потребують налаштування (p,d,q)
Машинне навчання	Здатність відображати складні нелінійні залежності між генерацією та споживанням, висока точність на середніх горизонтах	Потребують великих обсягів даних для навчання та ризик перенавчання при недостатній регуляризації
Глибинне навчання	Можливість врахувати довготривалі часові залежності в поведінці споживача, адаптивність до нетипових патернів	Високі обчислювальні витрати, «чорний ящик» без прозорої інтерпретації результатів
Гібридні підходи	Поєднання переваг статистичних і ML/DL методів (наприклад, ARIMA+LSTM) дозволяє підвищити точність прогнозів енергобалансу	Ускладнена інтеграція моделей, велика обчислювальна й підтримкова складність

Це обумовлено необхідністю врахування широкого спектру змінних, включаючи поведінкові фактори, взаємодію між споживанням та генерацією, а також зовнішні економічні аспекти. Для досягнення високої точності прогнозів необхідно використовувати інтегровані моделі, які можуть адаптуватися до змінних умов та враховувати всі релевантні фактори.

[1] Popławski, T., Dudzik, S., & Szeląg, P. (2023). Forecasting of Energy Balance in Prosumer Micro-Installations Using Machine Learning Models. Energies, 16(18), 6726. https://doi.org/10.3390/en16186726

[2] Koltsaklis, N., Panapakidis, I. P., Pozo, D., & Christoforidis, G. C. (2021). A Prosumer Model Based on Smart Home Energy Management and Forecasting Techniques. Energies, 14(6), 1724. https://doi.org/10.3390/en14061724

[3] Petrican T. et al., "Evaluating Forecasting Techniques for Integrating Household Energy Prosumers into Smart Grids," 2018 IEEE 14th International Conference on Intelligent Computer Communication and Processing (ICCP), Cluj-Napoca, Romania, 2018, pp. 79-85, https://doi.org/10.1109/ICCP.2018.8516617.

[4] Brusco, G., Burgio, A., Menniti, D., Pinnarelli, A., Sorrentino, N., & Vizza, P. (2017). Quantification of Forecast Error Costs of Photovoltaic Prosumers in Italy. Energies, 10(11), 1754. https://doi.org/10.3390/en10111754

Т.В. Пучко

СТРАТЕГІЯ ЕВОЛЮЦІЇ З АДАПТАЦІЄЮ МАТРИЦІ КОВАРІАЦІЇ ДЛЯ ОПТИМІЗАЦІЇ СТРУКТУРИ ГЕНЕРУЮЧИХ ПОТУЖНОСТЕЙ ЕЛЕКТРОЕНЕРГЕТИЧНИХ СИСТЕМ

Забезпечення надійного електропостачання є ключовою передумовою стабільного функціонування економіки та соціальної сфери держави. Це питання набуває особливої ваги в умовах російських ракетно-дронових ударів по об'єктах енергетичної інфраструктури України. Ефективним інструментом зменшення негативного впливу таких атак виступає розвиток технологій розподіленої генерації, зокрема використання сонячних і вітрових електростанцій. Завдяки своїй розосередженості, відносно низькій вартості складових елементів та швидким термінам відновлення, такі системи є менш вразливими до одночасного знищення та значно знижують ефективність застосування високовартісних засобів ураження [1].

Водночас слід зазначити, що відновлювані джерела енергії (ВДЕ), зокрема сонячна та вітрова енергія, мають суттєво вищий рівень непередбачуваності та обмежену керованість порівняно з традиційними джерелами, такими як природний газ, вугілля або ядерне паливо. Зростання їх частки у структурі генеруючих потужностей значно ускладнює процес управління енергосистемою та створює додаткові труднощі при стратегічному плануванні її розвитку [2].

Оптимізація структури генеруючих потужностей у таких умовах, як правило, потребує формалізації у вигляді задач змішаного цілочисельного лінійного програмування (MILP). Наявність великої кількості змінних, обумовленої включенням ВДЕ, зумовлює високу обчислювальну складність таких задач і, відповідно, необхідність розробки алгоритмів, здатних ефективно працювати з використанням паралельних обчислювальних ресурсів. У зв’язку з цим, дослідження методів паралельної оптимізації структури генеруючих потужностей є надзвичайно актуальним з огляду на потреби сучасної енергетики.

Одним із ефективних підходів до розв’язання задач змішаного цілочисельного лінійного програмування великої розмірності є застосування методів декомпозиції [3]. З огляду на специфіку задачі оптимізації структури генеруючих потужностей, її доцільно розділити на підзадачу першого рівня, яка визначає кількість генеруючих блоків та вартість їх встановлення, і множину підзадач другого рівня, що враховують технологічні обмеження режимів роботи блоків та обчислюють відповідні операційні витрати. У межах такого підходу перший рівень доцільно розв’язувати за допомогою алгоритмів, які не потребують інформації про похідну цільової функції, а лише оцінюють її значення для різної кількості генеруючого обладнання. Натомість підзадачі другого рівня можуть бути розв’язані паралельно із

застосуванням наявних MILP-солверів, оскільки кількість обладнання на цьому етапі вже вважається фіксованою.

Метою даного дослідження було вивчення потенційної можливості застосування алгоритму стратегії еволюції з адаптацією матриці коваріації (CMA-ES) для розв'язання підзадачі першого рівня, з урахуванням нещодавніх удосконалень для оптимізації функцій з цілочисельними змінними [4]. У рамках роботи було проведено порівняння швидкості оптимізації структури генеруючих потужностей електроенергетичної системи при використанні лише солвера SCIP [5] та паралельного алгоритму, що поєднує CMA-ES на першому рівні зі SCIP на другому, як показано на рисунку 1. Це дозволило зробити попередні висновки щодо доцільності використання CMA-ES у задачах цього типу.

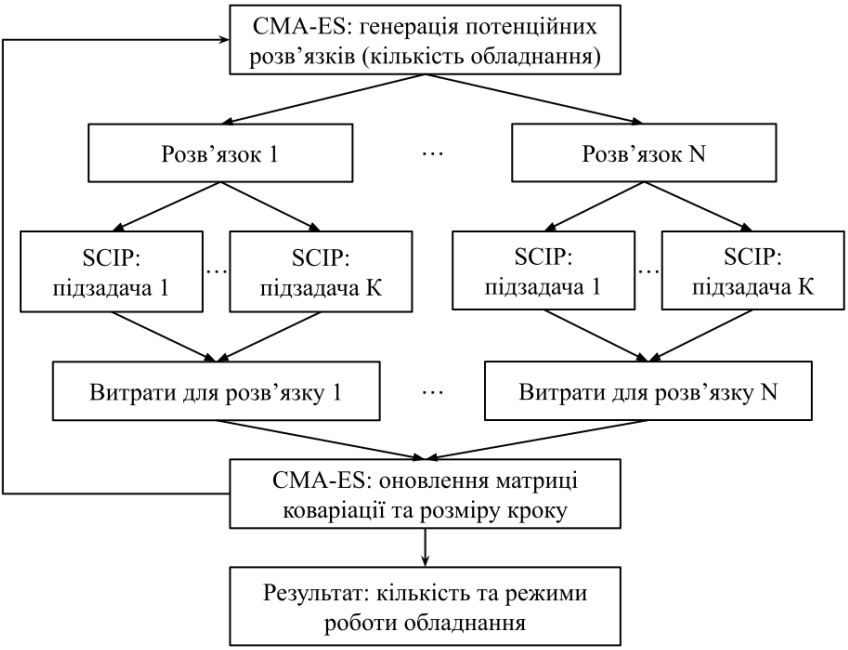


Рисунок 1 – Паралельний алгоритм оптимізації структури генеруючих потужностей електроенергетичної системи з використанням CMA-ES

Експериментальні дослідження було проведено на обчислювальній системі, оснащеній 768 ГБ оперативної пам'яті та двома процесорами AMD EPYC™ 9124 з тактовою частотою 3,0 ГГц; загальна кількість апаратних потоків процесора — 64. Програмну реалізацію алгоритмів здійснено мовою програмування Julia із використанням бібліотеки JuMP [6]. На першому етапі було визначено час розв'язання задачі виключно за допомогою солвера SCIP в однопотоковому режимі, який становив 1364,74 секунди. Далі

досліджувалася робота паралельного алгоритму за різних обмежень кількості доступних потоків центрального процесора, із застосуванням бібліотеки pycma [7]. Зважаючи на стохастичну природу CMA-ES, для кожного варіанту обмеження кількості потоків алгоритм виконувався десять разів, з ініціалізацією генератора випадкових чисел значеннями від 1 до 10. Для виконання CMA-ES застосовувалися рекомендовані параметри, за винятком розміру популяції: лише після збільшення автоматично визначеного розміру популяції на 60 % за допомогою параметра *popsize_factor* кожен запуск алгоритму забезпечував знаходження оптимального розв'язку, попередньо отриманого за допомогою лише SCIP. Узагальнені дані щодо часу виконання паралельного алгоритму наведено в таблиці 1.

Таблиця 1 – Залежність швидкості обчислень від рівня паралелізму

Кількість потоків центрального процесора	Середній час виконання (с)	Стандартне відхилення часу виконання (с)	Середній коефіцієнт прискорення
16	703,57	78,71	1,94
32	666,03	76,83	2,05
64	616,19	71,79	2,21

Як показали результати експерименту, використання паралельного алгоритму на основі CMA-ES забезпечує приблизно дворазове прискорення обчислень порівняно з використанням лише солвера SCIP. Водночас час виконання виявився слабо залежним від кількості доступних потоків центрального процесора. Це явище можна пояснити кількома чинниками.

По-перше, ефективність паралелізації на першому рівні залежить від розміру популяції CMA-ES. Однак у випадках, коли під час паралельного обчислення значень цільової функції для всієї популяції виявляється, що в окремих точках розв'язок не існує, бібліотека pycma автоматично генерує нові точки, і відповідні обчислення виконуються вже послідовно.

По-друге, паралелізм на другому рівні визначається кількістю підзадач, яка перевищує кількість доступних потоків. Однак час розв'язання окремих підзадач може істотно відрізнятися. Якщо складніші підзадачі потрапляють у кінець черги на виконання, це призводить до неефективного завантаження обчислювальних ресурсів і збільшення загального часу розв'язання, порівняно зі сценарієм, коли ресурсоємні задачі обробляються на початку.

Також на швидкість обчислень впливають робота збирача сміття в Julia та реалізація гіперпотоковості в центральному процесорі, оскільки кількість фізичних ядер удвічі менша за кількість апаратних потоків.

Проведене дослідження показало, що використання алгоритму CMA-ES у складі паралельного алгоритму дозволяє досягти приблизно дворазового прискорення обчислень у задачах оптимізації структури генеруючих

потужностей електроенергетичних систем. Це свідчить про потенційну придатність даного алгоритму для розв'язання задач першого рівня, які, попри невелику кількість змінних, характеризуються складною структурою області допустимих значень через численні обмеження, що накладаються задачами другого рівня.

Водночас результати експериментів виявили проблему неефективного завантаження обчислювальних ресурсів під час паралельного виконання, що обмежує потенційні переваги масштабування при збільшенні кількості доступних потоків. Подальші дослідження доцільно зосередити на вдосконаленні розподілу обчислювального навантаження, а також на адаптації параметрів алгоритму CMA-ES з урахуванням специфіки задачі першого рівня — зокрема, її цілочисельної природи.

[1] Саух, С. Є., & Борисенко, А. В. (2025). Моделювання електроенергетичної системи України та оцінювання її резильєнтності в умовах систематичних терористичних атак. Технічна електродинаміка, 2025(2), 57–70. https://doi.org/10.15407/techned2025.02.057

[2] 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.

[3] 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.

[4] Marty, T., Hansen, N., Auger, A., Semet, Y., & Héron, S. (2024). LB+IC-CMA-ES: Two Simple Modifications of CMA-ES to Handle Mixed-Integer Problems. In Lecture Notes in Computer Science (pp. 284–299). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-70068-2_18

[5] 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.

[6] Lubin, M., Dowson, O., Garcia, J. D., Huchette, J., Legat, B., & Vielma, J. P. (2023). JuMP 1.0: recent improvements to a modeling language for mathematical optimization. Mathematical Programming Computation. https://doi.org/10.1007/s12532-023-00239-3

[7] Nikolaus Hansen, yoshihikoueno, ARF1, Sait Cakmak, Gabi Kadlecová, Guillermo Abad López, Kento Nozawa, Luca Rolshoven, Youhei Akimoto, brieglhostis, & Dimo Brockhoff. (2024, September 3). CMA-ES/pycma: r4.0.0. https://doi.org/10.5281/ZENODO.2559634

Ye.P. Kholiavka, Yu.V. Parfenenko

SIMULATION-BASED FORECASTING OF BATTERY STATE OF CHARGE FOR ASSESSING THE ENERGY MICROGRID FUNCTIONAL STATE

Modern microgrids operating as part of distributed energy systems with high integration of renewable energy sources (RES) are characterized by a complex structure of energy flows, high sensitivity to weather conditions and seasonal fluctuations, as well as limited predictability of energy output. Under such conditions, ensuring reliable, economically efficient, and uninterrupted operation of the microgrid requires the application of tools for rapid assessment of its functional state, taking into account forecast parameters.

One of the key indicators reflecting a microgrid's ability to maintain energy balance in the short- and medium-term horizons is the forecasted state of charge (SoC) of the battery. This parameter serves as an indicator of the current and future autonomy of the system and determines its capacity to compensate for energy deficits under conditions of reduced generation or increased demand. In contrast to load and generation forecasting, which are widely supported by machine learning algorithms, SoC forecasting cannot be directly implemented using neural network models due to the lack of representative, structured, and labeled datasets. This complicates the creation of training samples that would account for both internal battery characteristics (temperature dependence, degradation, current limitations) and external operating conditions (load profiles, generation fluctuations).

Due to these limitations, the use of physics-based simulation models becomes particularly relevant. These models perform charge calculations based on an energy balance approach—comparing incoming energy from generation sources with load consumption, while accounting for efficiency coefficients [1, 2]. Such models allow the incorporation of physical constraints (charge limits, losses, capacity) and are distinguished by high computational efficiency, result predictability, and ease of integration into larger information-analytical microgrid management systems [3, 4].

The object of the study is the process of predictive assessment the technical condition of an autonomous microgrid energy system under conditions of variable energy load and renewable energy generation.

The aim of the study is to develop a mathematical model for forecasting the state of charge (SoC) of a battery based on a simulation of the generation-load balance, with subsequent integration of the result into a decision support system for microgrid management.

To ensure an accurate assessment of the forecasted state of the microgrid using battery energy storage systems, this study substantiates the feasibility of applying a simulation-based approach for calculating the state of charge. After analyzing scientific approaches and technological constraints, it was proposed to adopt a model based on the computation of the energy balance between forecasted

electricity generation and microgrid load. This approach enables a formalized description of the dynamics of stored energy over time by incorporating the physical parameters of the battery into the model.

The study employs a model based on the energy balance between generation power and load. The calculation is performed at each time step, taking into account the efficiency of the charging process. The formula is adapted for forecasting conditions:

$$SoC_{t+1} = min(1, max(0, SoC_t + \frac{\eta_c \times (P_{gen,t} - P_{load,t})}{C_{bat}} \times \Delta t)) \quad (1)$$

where

— SoC_t : the battery state of charge at time t ,

— $P_{gen,t}$: total forecasted power generation (W),

— $P_{load,t}$: forecasted power consumption (W),

— η_c : charging efficiency coefficient,

— C_{bat} : nominal battery capacity,

— Δt : simulation time step (1 hour).

A distinguishing feature of this model is that it accounts only for the surplus balance between generation and consumption, allowing for the modeling of charge accumulation during daylight hours and its decline at night without the need for detailed representation of discharge processes. In addition, thanks to the limiting operators min and max, the model prevents unrealistic SoC values, maintaining them within the physically permissible interval [0;1].

This approach has gained considerable traction in the scientific literature, particularly in [5], which highlights the effectiveness of physics-based models for energy storage management tasks. Reference [6] also emphasizes that even with the availability of advanced artificial intelligence methods, models incorporating the internal logic of energy balancing demonstrate greater stability and interpretability under scenarios of high generation uncertainty.

To validate the model, simulation-based forecasting of SoC was carried out using a 24-hour load and generation profile. The input data included forecasted generation (ppv1), load (pLoad), and charging power (pCharge), obtained from a monitoring system. The initial SoC was set to 75%, battery capacity to 10 kWh, and charging efficiency to 95%.

To validate the proposed approach, simulation-based forecasting of SoC was carried out using a 24-hour profile of load and generation. The predictive models for electricity generation and consumption used in this study were developed and tested in [7], where a comprehensive forecasting framework was presented for microgrid energy management. The input data included forecasted photovoltaic generation (ppv1), electrical load (pLoad), and charging power (pCharge), all obtained from a monitoring system. The initial SoC was set to 75%, battery capacity to 10 kWh, and charging efficiency to 95%.

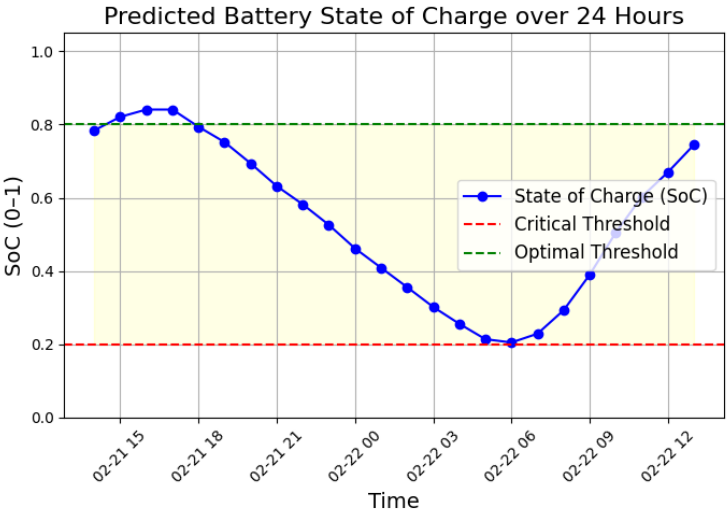


Figure 1 – Forecasted Battery State of Charge over a 24-Hour Period

The obtained SoC values can serve as input for fuzzy logic systems to assess the functional state of a microgrid. This enables a linguistic interpretation of the technical condition (“critical”, “risky”, “stable”) based on forecasted parameters and supports automated decision-making. These results are planned to be integrated into a fuzzy classification model that evaluates the microgrid's condition using forecasted load, generation, and battery charge level.

[1] Chen, M.; Wang, Z.; Mi, C.C. State of charge estimation of lithium-ion batteries in electric drive vehicles using a hybrid method. Energies, 2010, 3, 1202–1219.

[2] Liu, K.; Li, K.; Peng, Q.; Zhang, C. A brief review on key technologies in the battery management system of electric vehicles. Frontiers in Mechanical Engineering, 2021, 6, 590674.

[3] Khosravi, A.; Nahavandi, S.; Creighton, D.; Atiya, A.F. Comprehensive review of battery modeling and state estimation approaches. Renewable Energy, 2021, 159, 806–830.

[4] Zhou, F.; Liu, L.; Wang, X.; Wang, H. Predictive control for battery management in hybrid renewable systems. Journal of Energy Storage, 2022, 49, 04170.

[5] Wang, Y.; Gu, W. Dynamic battery model-based optimization for microgrid dispatch. Applied Energy, 2020, 264, 114726.

[6] Zhang, C.; Li, K.; Deng, J.; Yuan, C. A comparative study of state of charge estimation methods for lithium-ion batteries. IEEE Transactions on Industrial Informatics, 2021, 17(3), 1585–1594.

[7] Parfenenko, Y.; Shendryk, V.; Kholiavka, E.; Miroshnichenko, O. Electricity Demand Forecasting Software for Microgrid Energy Management System. In: Proceedings of the 2024 International Conference on Computer Modeling and Intelligent Systems (CMIS), 2024, pp. 413–423.

О.І. Клюзко

МЕТОД МАШИННОГО НАВЧАННЯ «ВИПАДКОВИЙ ЛІС» В ЗАДАЧАХ ПРОГНОЗУВАННЯ ОБСЯГІВ СПОЖИВАННЯ ЕЛЕКТРОЕНЕРГІЇ

При укладанні договорів постачання компанія-постачальник забезпечує постачання всього обсягу фактичного споживання електричної енергії споживачами протягом розрахункового місяця. Для здійснення закупівлі електричної енергії споживач надає постачальнику загальний плановий обсяг споживання на весь розрахунковий місяць. Відповідно до вимог Правил ринку електричної енергії, компанія-постачальник, як сторона, відповідальна за балансування, формує погодинні баланси постачання, купівлі та споживання електроенергії на кожну годину t місяця постачання T:

$$V_{купівля-продаж} = V_{постачання} = V_{споживання} \quad (1)$$

Відповідно перед постачальником постає необхідність у використанні математичних моделей прогнозу погодинного графіку заявлених споживачами обсягів споживання.

Методи машинного навчання демонструють високу ефективність у задачах прогнозування споживання електричної енергії. Існуючі моделі базуються на різних підходах до обробки вхідних даних, що зумовлено специфікою поставлених задач. Для побудови адекватної прогнозної моделі, яка враховує особливості обмеженого доступу до даних в українських умовах, було застосовано метод Random Forest для оцінювання погодинного коефіцієнта споживання протягом розрахункового періоду.

Для навчання моделі використовується історичний набір даних, що містить часові, метеорологічні та календарні ознаки.

Основна ідея застосування Random Forest полягає у побудові ансамблю незалежних дерев рішень, передбачення яких агрегуються для підвищення точності прогнозу погодинного споживання. У контексті короткострокового прогнозування кожне дерево тренується на випадковій підмножині історичних даних, які включають такі ознаки, як дата, час доби, температура повітря та інформація про святкові/вихідні дні. Така стратегія сприяє зниженню кореляції між окремими деревами, покращуючи здатність моделі до узагальнення та зменшуючи дисперсію прогнозів.

Метод Random Forest реалізується шляхом послідовного виконання низки етапів, адаптованих для вирішення задачі прогнозування обсягів споживання електроенергії. На початковому етапі з навчального набору даних D, що містить історичні записи обсягів споживання електроенергії Y_i та відповідні вектори ознак X_i (година доби, день тижня, температура повітря, вихідний чи святковий день), формується множина бутстреп-вибірок:

$$D = \{(X_1, Y_1), (X_2, Y_2), \dots, (X_N, Y_N)\}, \quad (2)$$

де: $X_i \in \mathbb{R}^p$– вектори ознак (наприклад, година доби, день тижня, температура повітря); Y_i – обсяг споживання у момент часу i; N – кількість спостережень; p – кількість ознак.

Для кожного дерева рішень застосовується випадкове підпросторове семплювання. У кожному вузлі дерева випадково обирається підмножина з $m < p$ ознак, серед яких вибирається та, що мінімізує функцію втрат.

Критерій розщеплення даних полягає у виборі ознаки j та порогу розщеплення s, які мінімізують функцію втрат $L(j, s)$:

$$L(j,s) = \sum_{i \in D_{left}} (Y_i - \bar{Y}_{left})^2 + \sum_{i \in D_{right}} (Y_i - \bar{Y}_{right})^2 \qquad (3)$$

де:

$D_{left}\{i \mid X_{ij} \le s\}$ – підмножина зразків, що потрапляють у ліве піддерево після розщеплення;

$D_{right}\{i \mid X_{ij} \le s\}$ – підмножина зразків, що потрапляють у праве піддерево після розщеплення;

$X_{i,j}$ – значення ознаки j для зразка i;

$\bar{Y}_{left}, \bar{Y}_{right}$ – середні значення обсягів споживання електроенергії в лівому та правому піддеревах відповідно.

Розщеплення триває рекурсивно до досягнення зупиняючих критеріїв (максимальна глибина, мінімальна кількість спостережень тощо).

Після побудови ансамблю з B дерев прогноз для нового зразка X обчислюється як середнє передбачень дерев:

$$\hat{Y} = \frac{1}{B} \sum_{b=1}^{B} T_b\,(X) \qquad (4)$$

де:

$\hat{Y}$ – прогнозоване значення обсягу споживання електроенергії;

B – кількість дерев у ансамблі**;**

$T_b(X)$ – прогноз, згенерований b-им деревом.

Окрім прогнозування, метод дозволяє оцінити важливість ознак. Вона визначається як середнє зменшення функції втрат у вузлах, де використовувалась відповідна ознака:

$$VI(j) = \frac{1}{B} \sum_{b=1}^{B} \sum_{t \in T_b} \delta_j(t) \Delta L_t \qquad (5)$$

де:

$VI(j)$ – важливість ознаки j;

T_b – множина вузлів у b-му дереві;

$\delta_j(t)$– індикаторна функція, яка дорівнює 1, якщо у вузлі t використовується ознака j, і 0 в іншому випадку;

ΔL_t – зменшення функції втрат L при розщепленні у вузлі t.

Цей механізм дозволяє проаналізувати вплив окремих ознак на результати моделі та виділити ключові фактори електроспоживання (наприклад, температуру або святкові дні).

Для практичного впровадження прогнозної моделі розроблено програмний комплекс Energy AI на мові Python. Він автоматизує ключові етапи: очищення даних, нормалізацію, генерацію календарних ознак і blackout-фактора, підбір гіперпараметрів Random Forest за допомогою Optuna, тренування моделі, логування та збереження у форматі .pkl. Прогнози експортуються у форматі .xlsx для використання у бізнес-процесах енергетичних компаній.

Проведене дослідження підтвердило високу точність RF-моделі для короткострокового прогнозування погодинного електроспоживання. Модель, навчена на даних за жовтень 2021 – липень 2024 року, досягла середньоквадратичної похибки 0, MAE у межах 0–0.00001 і коефіцієнта детермінації $R^2 = 1$. Відносна похибка не перевищила 0.0004 %, а точність залишалась 100 % в усіх заданих інтервалах відхилення.

Аналіз важливості ознак показав, що найбільший вплив має година доби, а також ознаки робочого часу, температура повітря, календарні та сезонні чинники. Такий розподіл підтверджує релевантність обраного підходу та якість ознак.

Отримані результати засвідчують придатність моделі для практичного використання у балансуванні та плануванні споживання. Рекомендовано регулярне оновлення на основі нових даних та розгляд альтернативних моделей для адаптації до динаміки ринку.

[1] Закон України №2019-VIII вид 13.04.2017 «Про ринок електричної енергії»: https://zakon.rada.gov.ua/laws/show/2019-19#Text

[2] І.В. Блінов, Є.В. Парус Оптовий та роздрібний ринок електричної енергії: розрахункова робота [Електронний ресурс] : навч. посіб. для студ. які навчаються за спеціальністю 141 «Електроенергетика, електротехніка та електромеханіка» / КПІ ім. Ігоря Сікорського; уклад.: Електронні текстові дані (1 файл: 1,1 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2022. – 44 с.

[3] Саух С. Є., Борисенко А. В. Математичне моделювання електроенергетичних систем в ринкових умовах: монографія. К.: «Три К». 2020. 340 с

А.В. Ковилін, С.Я. Гільгурт

ПОРІВНЯЛЬНИЙ АНАЛІЗ ТАБЛИЧНИХ І ГРАФОВИХ МОДЕЛЕЙ ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ У МЕРЕЖАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Системи забезпечення кібербезпеки на об'єктах критичної інфраструктури (ОКІ) стикаються зі складними загрозами, серед яких: цілеспрямовані атаки, багатовекторні впливи та zero-day [1] атаки, які важко виявити за допомогою сигнатурних методів. Одним із ключових завдань у такому контексті є вчасне виявлення аномалій у мережевому трафіку, що може свідчити про початок чи підготовку до вторгнення або підозрілу активність.

Окрім сигнатурних методів на практиці цю задачу намагаються вирішити за допомогою традиційних моделей машинного навчання, які працюють з табличними ознаками (features) [2]. Проте ці підходи мають низку обмежень:

1. *Ігнорування топології мережі*. Більшість моделей ML аналізують кожен мережевий запис незалежно, не враховуючи взаємозв'язки між джерелами та одержувачами трафіку, що є критичним для виявлення DDoS, ботнетів та інших координованих атак.
2. *Обмежена здатність виявляти приховані патерни*. Багато атак формуються у вигляді послідовностей зв'язків між вузлами (наприклад, порт-сканування, повторні з'єднання, зміна маршрутів), які важко ідентифікувати без урахування структури мережі.
3. *Нестійкість до нових типів атак*. При виникненні нових атак, що не входили до тренувального набору, традиційні моделі часто демонструють слабку здатність до узагальнення.
4. *Дисбаланс класів*. У реальних даних частка аномальних подій може становити менше 1%, що ускладнює навчання та призводить до зниження ефективності.
5. *Затримки в реагуванні*. Методи післяобробки та фільтрації з високими порогами можуть затримувати виявлення атак, що є неприйнятним для реального часу (або в разі необхідності швидкого реагування).

Вказані обмеження особливо критичні для енергетики, транспорту, охорони здоров'я та оборонної сфери, де кожен день зволікання може мати катастрофічні наслідки.

Тому виникає потреба у застосуванні моделей, які враховують не лише індивідуальні характеристики даних, а й топологію взаємодій у мережі. Одним із таких підходів є графові нейронні мережі (Graph Neural Networks, GNN)[3], які дозволяють будувати узагальнені уявлення (embedding) про вузли на основі їхнього оточення, що значно підвищує якість виявлення аномалій у складних мережах критичної інфраструктури.

Саме тому метою нашого дослідження стала розробка та порівняльна оцінка ефективності традиційних алгоритмів машинного навчання, глибокого навчання, а також графових моделей (зокрема Graph Neural Networks (GNN)) для виявлення аномалій у мережевому трафіку критичної інфраструктури. Особливий акцент було зроблено на виявлення DDoS-атак, підозрілих з'єднань та zero-day загроз.

Для досягнення цієї мети було реалізовано кілька етапів:

1. *Побудова графа взаємодій*. На основі логів мережевого трафіку побудовано неорієнтований граф, де вузлами виступали унікальні IP-адреси, а ребрами - з'єднання між ними. Це дозволило врахувати топологію зв'язків і контекст трафіку.
2. *Генерація ознак та методи векторизації*. Були протестовані підходи до ідентифікації вузлів:

- Табличні ознаки (наприклад, Packet Length, Protocol, Ports), та інші числові характеристики, що використовуються в класичних ML-моделях.
- Графові нейронні мережі (GNN). Архітектура на основі GCNConv [4], що враховує як локальні, так і глобальні властивості графа та дозволяє здійснювати агрегування інформації з оточення вузла.

3. *Навчання моделей.* Для кожного з підходів було реалізовано і протестовано такі моделі:

- Наглядові ML-моделі: MLP, Label Propagation, Ensemble, KMeans, LOF, Isolation Forest.
- Глибоке навчання: Keras-мережа на табличних ознаках.
- Графова модель: GCN як реалізація GNN.

4. *Оцінка ефективності.* Оцінка проводилась на тестовому датасеті DDoS-атак, що знаходиться у відкритому доступі і який було попередньо очищено та збалансовано. У випадку GNN-моделі враховано вплив оточення вузла (neighbor aggregation) та перевірено якість класифікації при малому обсязі даних (few-shot learning).

Таблиця 1 – Використані метрики оцінки ефективності

Метрики	Опис
Класифікаційні метрики	Precision, Recall, F1-Score, Accuracy
Додаткові метрики	AUC, Cohen Kappa, Specificity, FPR, FNR
Крос-валідація	Stratified K-Fold (k=5)

Для оцінки ефективності алгоритмів було використано датасет DDoS-атак (850 тисяч рядків) [5] з мітками класів. У процесі експерименту було протестовано як табличні, так і графові підходи. Серед табличних моделей розглядалися алгоритми unsupervised (Isolation Forest, DBSCAN, LOF, KMeans) та supervised (MLP, Label Propagation, Voting Ensemble, глибока

нейронна мережа на Keras). Графові методи включали Graph Neural Networks (GNN) з агрегуванням сусідів. Для кожної моделі було проведено 5-кратну стратифіковану крос-валідацію та виміряно ключові метрики.

Таблиця 2 – Результати дослідження (метрики)

Model	Precision	Recall	F1-Score	Accuracy	Specificity	FPR	FNR	Cohen Kappa	AUC
Isolation Forest	0.862	0.07	0.13	0.659	0.993	0.006	0.929	0.079	0.532
KMeans	0.001	0.001	0.001	0.061	0.094	0.905	0.998	0.08	0.0482
DBSCAN	0.631	0.001	0.003	0.638	0.999	0.001	0.998	0.001	0.5
LOF	0.012	0.001	0.001	0.61	0.956	0.043	0.999	0.053	0.478
MLP Classifier	0.995	0.998	0.997	0.998	0.997	0.002	0	0.995	0.999
Label Propagation	0.858	0.998	0.923	0.939	0.906	0.093	0.001	0.874	0.997
Deep Learning Model	0.862	0.995	0.924	0.939	0.905	0.094	0	0.873	0.996
Ensemble Model	0.995	0.998	0.997	0.997	0.997	0.002	0.001	0.995	0.999
GNN	0.993	0.998	0.998	0.999	0.997	0.002	0.001	0.998	0.998

Висновок. Проведене дослідження підтвердило доцільність використання графових моделей, зокрема Graph Neural Networks (GNN), для виявлення аномалій у мережевому трафіку критичних інформаційних систем. Порівняльний аналіз показав, що графові моделі здатні ефективно враховувати топологічні зв'язки між вузлами мережі, що є особливо важливим для виявлення розподілених атак типу DDoS та zero-day загроз. У порівнянні з класичними алгоритмами машинного навчання (Isolation Forest, LOF, DBSCAN тощо), GNN-моделі продемонстрували високу точність, стабільність та здатність до узагальнення при аналізі великих обсягів даних. Завдяки використанню генерації векторних подань вузлів та побудові орієнтованих графів, забезпечується гнучка інтеграція просторової інформації, яка недоступна при традиційному табличному підході.

Таким чином, графові моделі машинного навчання відкривають нові можливості для побудови інтелектуальних, адаптивних та безпечних систем кіберзахисту в енергетиці, транспорті, телекомунікаціях та інших критичних

галузях. Та відкривають перспективи для подальших досліджень у вигляді використання динамічних графових нейромереж (Dynamic GNNs) для аналізу змін у топології мережі з плином часу; використання нових типів графів (зокрема Heterogeneous Graphs із семантичними типами вузлів та ребер) та потенційної інтеграції GNN у тестові системи реального часу для моніторингу мереж критичної інфраструктури в майбутньому.

[1] Danita Samuel Prakash (2023). Zero-day Vulnerabilities: An In-depth analysis. https://doi.org/10.13140/RG.2.2.12775.01445

[2] Vladimir Nasteski. An overview of the supervised machine learning methods (2017) https://www.researchgate.net/publication/328146111_An_overview_of_the_supervised_machine_learning_methods

[3] Khemani, B., Patil, S., Kotecha, K. et al. A review of graph neural networks: concepts, architectures, techniques, challenges, datasets, applications, and future directions. J Big Data 11, 18 (2024). https://doi.org/10.1186/s40537-023-00876-4

[4] Zhang, S., Tong, H., Xu, J. et al. Graph convolutional networks: a comprehensive review. Comput Soc Netw 6, 11 (2019). https://doi.org/10.1186/s40649-019-0069-y

[5] https://www.kaggle.com/code/akritiupadhyayks/cyber-attack-detection-with-random-forest/input?select=UNSW_NB15_training-set.csv

О.В. Гольонко, О.М. Дибач

ТЕХНОЛОГІЇ ШТУЧНОГО ІНТЕЛЕКТУ ТА ЇХ ПРАКТИЧНЕ ЗАСТОСУВАННЯ В ЯДЕРНІЙ ЕНЕРГЕТИЦІ: ПРОГНОЗНЕ ТЕХНІЧНЕ ОБСЛУГОВУВАННЯ

Штучний інтелект (ШІ) є однією з найактуальніших та найперспективніших технологій сучасності, здатною корінним чином трансформувати складні технологічні процеси шляхом обробки великих обсягів даних у реальному часі та виявлення прихованих закономірностей у динамічних системах.

Атомна електростанція є складним та багатовимірним виробничо-технічним комплексом з експлуатації реакторної установки для вироблення електроенергії. АЕС характеризуються великим масивом даних щодо стану технологічних параметрів енергоблоку, стану конструкцій, систем та елементів, даних досвіду експлуатації, експлуатаційної та протиаварійної документації.

З огляду на великі масиві даних, накопичений досвід експлуатації, технологічну зрілість технології та ін., ШІ відкриває нові можливості для підвищення ефективності та безпеки експлуатації АЕС.

За результатами аналізу наукових публікацій у наукометричній базі даних SCOPUS в Таблиця 1 наведено визначення та застосування окремих технологій ШІ в ядерній енергетиці (перелік не є вичерпним)

Таблиця 1. Технології штучного інтелекту: визначення та перспективне застосування в ядерній енергетиці

Галузь/технологія ШІ	**Визначення/сутність технології**	**Застосування**
Машинне навчання	Галузь ШІ, що навчається приймати рішення, налаштовуючи параметри математичних моделей відповідно до даних спостереження. Є ключовою концепцією в інтелектуальних обчисленнях, що зосереджується на розробці алгоритмів, які дозволяють машинам навчатися на основі даних та покращувати свою продуктивність через досвід.	▪ Прогнозне технічне обслуговування; ▪ Вібраційна та акустична діагностика; ▪ Інтелектуальний моніторинг; ▪ Виявлення кібератак і аномалій; ▪ Прогнозування відмов обладнання.

Галузь/технологія ШІ	Визначення/сутність технології	Застосування
Глибинне навчання	Галузь машинного навчання, яка присвячена тренуванню моделей, таких як нейронні мережі, що складаються з багатьох шарів	▪ Діагностика несправностей; ▪ Прогноз аварійних сценаріїв; ▪ Класифікація типів аварій; ▪ Автономне керування реактором; ▪ Аналіз дій оператора. ▪ Управління магнітним полем для утримання плазми в термоядерному реакторі.
Штучна нейронна мережа (нейронна мережа, нейромережа)	Модель, яка складається з одного або кількох шарів штучних нейронів, з'єднаних зваженими зв'язками з ваговими коефіцієнтами. Клас обчислювальних моделей, натхненних структурою та функціонуванням біологічних нейронних мереж у людському мозку. Нейронна мережа перетворює вхідні дані, пропускаючи їх через себе, при цьому кожен нейрон виконує прості обчислення.	▪ Прогнозування стану реактора. ▪ Діагностика дефектів; ▪ Оптимізація завантаження палива в реакторі; ▪ Автоматичний моніторинг; ▪ Прогноз аварійних ситуацій.
Обробка природньої мови	Напрям ШІ, який зосереджується на обробці, аналізі та генеруванні людської мови. Підгалузь штучного інтелекту, яка зосереджена на наданні комп'ютерам можливості розуміти, інтерпретувати та генерувати людську мову.	▪ Аналіз операторських журналів та звітів; ▪ Підтримка рішень операторів при аварійних ситуаціях; ▪ Інтерфейси взаємодії людина-машина.
Експертні системи	Системи, засновані на знаннях, які використовують правила для імітації процесів прийняття рішень експертів-людей у конкретних доменах. Вони розроблені для надання порад і рекомендацій експертного рівня.	▪ Підтримка прийняття рішень; ▪ Інтелектуальна діагностика; ▪ Планування технічного обслуговування.

Галузь/технологія ШІ	Визначення/сутність технології	Застосування
Алгоритми пошуку	Алгоритми пошуку, такі як пошук у глибину та пошук у ширину, використовуються для дослідження та навігації складними проблемними просторами для знаходження оптимальних рішень.	▪ Оптимізація завантаження палива в реакторі; ▪ Пошук оптимальних сценаріїв аварійного реагування.
Логічне представлення знань	Логічні методи, такі як предикатна та нечітка логіка, представляють і обґрунтовують знання та невизначеність в системах штучного інтелекту.	▪ Інтелектуальний аналіз стану систем.

Прогнозне технічне обслуговування

Прогнозне технічне обслуговування (англ. Predictive Maintenance, PdM) є найбільш розвинутим напрямом впровадження ШІ в ядерній енергетиці. Його мета – виявлення імовірних відмов до їх фактичного настання шляхом аналізу історичних та оперативних (онлайн) даних моніторингу. Такий підхід дозволяє запобігти неплановим зупинам АЕС та продовжити термін експлуатації обладнання.

Машинне навчання в цьому контексті використовується для моделювання залежностей між технічними параметрами обладнання та його станом Прогнозне технічне обслуговування використовує дані з датчиків контролю (температура, вібрація, акустика, тиск) для виявлення закономірностей у деградації обладнання. ШІ, зокрема машинне навчання, застосовується для автоматичної обробки цих даних та побудови моделей, здатних передбачити майбутні збої.

Серед найбільш поширених моделей – логістична регресія, дерева рішень, нейронні мережі та алгоритми виявлення аномалій [[1]]. Такі моделі не потребують точного фізичного опису процесу деградації, а працюють на основі даних про поведінку системи.

Особливої популярності набули глибокі нейронні мережі, включаючи LSTM (довготривала короткочасна пам’ять), що здатні враховувати динаміку параметрів у часі [[2]]. Це є актуальним для діагностики обладнання, яке працює в змінних режимах або під впливом циклічних навантажень.

Як приклад, логістична регресія оцінює імовірність відмови системи за допомогою функції (1):

$$P(\text{відмова}) = 1 / (1 + \exp(-(w1*x1 + w2*x2 + ... + wn*xn + b))), \quad (1)$$

де x1, x2, ..., xn — виміряні параметри (наприклад, температура, вібрація), а w1, w2, ..., wn і b — параметри моделі, які підбираються під час навчання на історичних даних.

Ця модель дозволяє ухвалювати рішення: якщо імовірність перевищує певний поріг, то обладнання підлягає обслуговуванню.

У випадках, коли важливо передбачити не просто факт відмови, а її часовий горизонт, застосовують регресійні моделі або нейромережі з можливістю оцінки залишкового ресурсу (Remaining Useful Life, RUL).

Застосування PdM у ядерній енергетиці вже дало позитивні результати. Зокрема, компанія EDF (Франція) впровадила машинне навчання для обробки акустичних сигналів насосного обладнання, що дозволило виявляти відхилення у поведінці механізмів ще до появи фізичних ознак зношування [[3]]. Компанія Siemens Energy [[4]] використовує цифрових двійників для аналізу поведінки турбін, комбінуючи фізичні моделі та дані моніторингу, а Rolls-Royce [[5]] у проєкті малого модульного реактору застосовує ШІ для моніторингу насосів охолодження.

Висновки

Аналіз наукових джерел і практичних прикладів свідчить, що застосування ШІ має перспективи у ядерній енергетиці, зокрема для прогнозного технічного обслуговування обладнання атомних станцій.

Моделі машинного навчання, зокрема логістична регресія та нейронні мережі, дозволяють ефективно виявляти потенційні відмови на основі даних моніторингу.

Попри виклики, пов’язані з валідацією моделей і якістю даних, впровадження таких технологій вже довело свою ефективність.

[1] Bishop, C. M. (2006). Pattern recognition and machine learning. Springer.

[2] Malhotra, P., Vig, L., Shroff, G., & Agarwal, P. (2015). Long short term memory networks for anomaly detection in time series. In Proceedings of the 23rd European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning (ESANN 2015) (pp. 89–94). Bruges, Belgium. https://www.esann.org/sites/default/files/proceedings/legacy/es2015-56.pdf

[3] Tran, D. D., Auger, F., & Simonin, O. (2020). Anomaly detection using acoustic signals in industrial machines. In Proceedings of the PHM Conference 2020. Prognostics and Health Management Society. https://www.phmsociety.org/proceedings/article/1234

[4] Siemens Energy. (2022). Harnessing digital twins and AI for predictive maintenance in power plants [White paper]. Siemens Energy. https://www.siemens-energy.com/global/en/home/stories/unleashing-ai-in-power-plants.html

[5] Rolls-Royce. (2021). Artificial intelligence applications in SMR design and operations [Technical briefing document]. Rolls-Royce. https://www.rolls-royce.com/~/media/Files/R/Rolls-Royce/documents/technical-briefings/ai-applications-smr-design-operations.pdf

В.С. Ракович, В.В. Цуркан, Г.В. Чурсін, О.М. Прокопець

ФУНКЦІЯ ВІЗУАЛІЗУВАННЯ ІНФОРМАЦІЇ ПРО ПОДІЇ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ГАЛУЗІ ЕНЕРГЕТИКИ

Встановлено [1], що в процесі пізнання навколишнього світу одне з найбільш важливих значень має зорове (візуальне) сприймання. Тому для аналізування та приймання рішень в будь-якій ситуації дуже важливо візуалізувати інформацію у зручному та зрозумілому для людини вигляді. Серед таких ситуацій виокремлюється виявляння і реагування на загрози в кіберпросторі. За аналогією з іншими галузями, в енергетиці це досягається створенням галузевої системи забезпечування кібербезпеки об'єктів критичної інформаційної інфраструктури [2, 3]. Одним із основних її складників є центри кібербезпеки (англ. Security Operation Center, SOC), наприклад [2], створений на базі НЕК «Укренерго». До того ж команди реагування на кіберінциденти, кібератаки, кіберзагрози [4]. В обох випадках запорукою успішності діяльності кожного з виокремлених складників є реалізованість функції візуалізування інформації про події кібербезпеки.

Під візуалізуванням інформації (англ. Information Visualization) розуміється процес представляння даних про події кібербезпеки у візуальній і змістовній формі на певному носієві [5], наприклад (рис. 1), моніторі, панелі. Тож реалізування даної функції передбачає використання різноманітних джерел, а саме: мережевого обладнання, брандмауерів, систем виявлення/запобігання вторгненням, операційних систем, антивірусного програмного забезпечення. Результати обробляння отриманих від них даних про події кібербезпеки відображаються у реальному часі на інформаційних панелях. Зазначений формат передбачає налаштування залежно від потреб діяльності організації. Це може стосуватися мереж, застосунків, доступності інформаційних активів, класифікування подій кібербезпеки [6, 7].

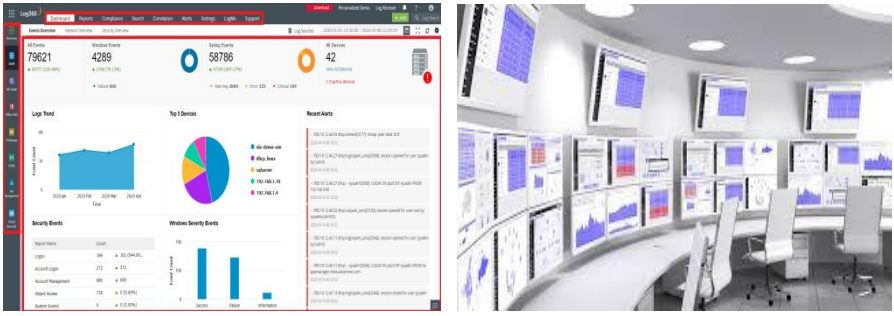


Рисунок 1 – Приклади реалізацій функції візуалізування інформації про події кібербезпеки [6, 7]

З огляду на призначеність функції візуалізування інформації, нею обумовлюється, по-перше, наявність відповідних інформаційних панелей. По-друге, якість аналізування подій кібербезпеки та, як наслідок, реагування на кіберінциденти. На це впливає складність отримання корисної інформації у реальному часі з великого обсягу даних з різноманітних джерел. Крім того узагальнене її відображення на інформаційних панелях з недостатнім урахуванням потреб зацікавлених сторін [8]. Водночас спостерігається тенденція до необхідності розширення площі відображення інформації. Загалом цим ускладнюється зосередженість зацікавлених сторін на інформації про важливі події кібербезпеки з ознаками кіберінциденту [6–8]. Запобігання виокремленим обмеженням можливо досягнути використанням технології доповненої реальності. Нею поєднуються переваги об'єднання декількох моніторів та потребується менший обсяг фізичного простору для функціонування [9].

Отже, запорукою успішності діяльності складників системи забезпечування кібербезпеки об'єктів критичної інформаційної інфраструктури галузі енергетики є реалізованість функції візуалізування інформації. Її поєднання з технологією доповненої реальності дозволить подолати встановлені обмеження і забезпечити якісне реагування на загрози в кіберпросторі.

[1] Кобильченко, В. (2019). Зорове сприймання та його порушення в дитячому віці. Особлива дитина: навчання і виховання, 4, 2019, 46–59.

[2] Міністерство енергетики України. (б. д.). Кібербезпека енергетичної галузі. https://mev.gov.ua/storinka/kiberbezpeka-enerhetychnoyi-haluzi.

[3] Постанова Кабінету Міністрів України «Про затвердження Положення про організаційно-технічну модель кіберзахисту» № 1426 (2021). https://zakon.rada.gov.ua/ laws/show/1426-2021-%D0%BF#Text.

[4] Закон України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури» № 4336-IX (2025, 27 березня). https://zakon.rada.gov.ua/ laws/show/4336-20#Text.

[5] Interaction Design Foundation. (2016, June 01). What is Information Visualization?. https://www.interaction-design.org/literature/topics/information-visualization.

[6] Logsign. (2020, February 05). What is a SOC Framework? https://www.logsign.com/ blog/what-is-a-soc-framework/.

[7] Miguel, P.G. (2025, March 24). Guide to the 22 Best SIEM Tools of 2025. https://thectoclub.com/tools/best-siem-tools/#full-listing-1904781.

[8] González-Granadillo, G., González-Zarzosa, S., Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors, 21, 4759. https://doi.org/10.3390/s21144759.

[9] Ракович, В.С., & Цуркан, В.В. (2023). Аналіз прикладних застосувань технології доповненої реальності. У В.Д. Самойлов, & І.В. Плетяний (Ред.) Науково-практичній конференції Технології створення і використання засобів підготовки персоналу на об'єктах критичної інфраструктури (с. 12–14). Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. https://doi.org/10.5281/ zenodo.15130175.

Р.І. Драгунцов, В.Ю. Зубок

ПРОБЛЕМАТИКА ІНТЕГРАЦІЇ ДЖЕРЕЛ ВИЯВЛЕННЯ ТЕХНІЧНИХ ВРАЗЛИВОСТЕЙ В РОЗРІЗІ ПІДТРИМКИ КІБЕРСТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

У сучасних умовах зростання складності інформаційно-комунікаційних систем критичної інфраструктури (КІ), інтеграція джерел технічного виявлення вразливостей є невід'ємною складовою забезпечення процесу управління вразливостями. Специфіка архітектури КІ, що охоплює поєднання фізичні, інформаційні та організаційні аспекти, а також складність їх поєднання, неоднорідність та великий масштаб, зумовлюють специфічні складності у побудові процесу управління вразливостями. Застосування технологій автоматизованого сканування, моніторингу та тестування на проникнення дає змогу виявляти вразливості для їх подальшого усунення.

Використання багаторівневих методів аналізу (топологічних, логічних, феноменологічних) у поєднанні з активним моніторингом може застосовуватись для побудови стратегій управління ризиками та вразливостями [1], однак не розв'язує ряд специфічних проблем пов'язаних з інтеграцією засобів виявлення вразливостей та розбудови процесу в цілому.

В контексті побудови процесу управління вразливостями специфіка критичної інфраструктури має наступні визначні фактори впливу:

- Масштаб інфраструктури;
- Топологічна та складова неоднорідність інформаційної інфраструктури [2][3];
- Нерозповсюджені або унікальні програмно-апаратні рішення впроваджені в ІКС [3];
- Складність поверхні атаки для багатьох інфраструктурних об'єктів [4].

Менш специфічними для КІ, але важливими для управління вразливостями є фактор обмеження ресурсів для усунення вразливостей, складності в розподілі відповідальності власників активів.

Модель управління вразливостями може бути охарактеризована формулою (1).

$$(\mathcal{A}, \mathcal{T}) \xrightarrow{D} G \xrightarrow{F} G_1 \xrightarrow{M} Z \xrightarrow{U} G_2 \quad (1)$$

де:

1. A — множина активів, T — множина засобів виявлення.
2. D (Detection) — функція виявлення вразливостей (сканування тощо), що генерує множину G зв'язків «Актив – Вразливість».
3. F (Filtering) — функція аналітики (фільтрація, нормалізація, агрегування) множини G, у результаті якої утворюється підмножина G_1 без хибнопозитивів та дублікатів.

4. M (Mapping або Mapping to Remediation) — відображення, яке зіставляє кожній парі «Актив – Вразливість» (з G_1) відповідні задачі з усунення. Після цього формується сукупність Z (зв'язки «Актив – Вразливість – Задача»).
5. U (Updating або Remediation Update) — функція усунення (remediation) вразливостей власниками активів, яка повертає множину G_2 залишкових пар «Актив – Вразливість» після впровадження заходів безпеки.

При цьому, множина активів A може бути структурно складною та багатовимірною, враховуючи необхідність розгляду складених активів, таких як SCADA-система, що складається з багатьох контролерів ICS та керуючих пристроїв, що в свою чергу містять різні рівні абстракції – апаратне, програмне забезпечення, ОС. Дана модель також спрощена фактом відсутності власників активів, відповідальних за усунення вразливостей.

Якщо врахувати, що кожен засіб t_i виявлення вразливостей має атрибут «покриття» (здатність виявляти вразливості на активах певного класу, $C(t_i)$) та «повнота» (співвідношення вразливостей, що виявляються засобом та усіх теоретично можливих вразливостей активу), то стає очевидним проблематика покриття, тобто метрики ефективності процесу D та достатності впровадженої множини T за умови поточного стану A. Враховуючи складність інфраструктури ІКС критичної інфраструктури та фактору так званого Shadow IT точно оцінити покриття процесу управління вразливостями є складною задачею, що, відповідно, зумовлює складність інтеграції та контролю успішності впровадження нових засобів виявлення вразливостей.

Якщо розглянути кожен засіб виявлення t як приблизно типізоване рішення з приблизно однаковим співвідношенням a: G , то стає очевидним факт пропорційного збільшення множини G з впровадженням нових засобів t. Таким чином зростає навантаження в процесі F на фільтрацію вразливостей, оскільки складність структури A зумовлює ймовірність дублювання вразливостей виявлених різними джерелами. Враховуючи складність в автоматизації процесу F та великої частки ручної роботи, даний фактор може стати або перешкодою до впровадження нових засобів виявлення вразливостей та розширення покриття, або фактором суттєвого здороження та ускладнення процесу.

При інтеграції нових засобів t_i та масштабуванні ресурсів аналітики (F) вихідна множина G_1 не має збільшуватись пропорційно, однак у разі відмови від посилення F, навантаження в процесі U (усунення вразливостей) зростає непропорційно та викликає адміністративні складнощі, що призводять до накопичення технічного боргу в розрізі усунення вразливостей та збільшення множини G_2 (залишкові вразливості), що, фактично нівелює ефект впровадження нового засобу виявлення вразливостей.

Таким чином, проблематика інтеграції нових джерел виявлення вразливостей (t_i) може бути сформульована тезами, описаними в таблиці 1.

Таблиця 1 – фактори складності інтеграції джерел технічних вразливостей

Фактор	Опис
Покриття та контроль покриття	Складність структури інформаційних активів критичної інфраструктури та наявність необлікованих активів зумовлює складність визначення та контролю покриття процесами управління вразливостями, та ускладнює визначення ефективності та доцільності впровадження нових засобів виявлення вразливостей.
Збільшення навантаження та ускладнення аналітики вразливостей	Збільшення обсягу виявлених вразливостей у комбінації з складністю структури інформаційних активів зумовлює дублювання виявлених вразливостей, складнощі в розподілі та збільшує навантаження на процес аналітики вразливостей.
Адміністративні складнощі під час усунення вразливостей	Складність визначення відповідальних за усунення вразливостей осіб у структурно-складних активах.
Непропорційне зростання технічного боргу усунення вразливостей	Збільшення навантаження на процес усунення вразливостей зумовлює зменшення ефективності усунення вразливостей та накопичення неусунених дефектів.

Впровадження нових засобів автоматизованого виявлення вразливостей в ІКС критичної інфраструктури може зумовити ряд проблем, що зменшать результуючу ефективність процесу управління вразливостями. Структурна складність інформаційних активів зумовлює проблематику ідентифікації та контролю покриття виявлення вразливостей, збільшує навантаження та ресурсоємність ручної обробки вразливостей та суттєво впливає на вартість усунення вразливостей та необхідний для цього ресурс.

[1] Zio, E. (2016). Critical Infrastructures Vulnerability and Risk Analysis. European Journal for Security Research, 1(2), 97–114. https://doi.org/10.1007/s41125-016-0004-2

[2] DIGITAL SECURITY AND RESILIENCE IN CRITICAL INFRASTRUCTURE AND ESSENTIAL SERVICES (DSTI/CDEP/GD(2018)14/FINAL). (2019). OECD.

[3] Ning Cai, Jidong Wang & Xinghuo Yu. (2008). SCADA system security: Complexity, history and new developments. У 2008 6th IEEE International Conference on Industrial Informatics (INDIN). IEEE. https://doi.org/10.1109/indin.2008.4618165

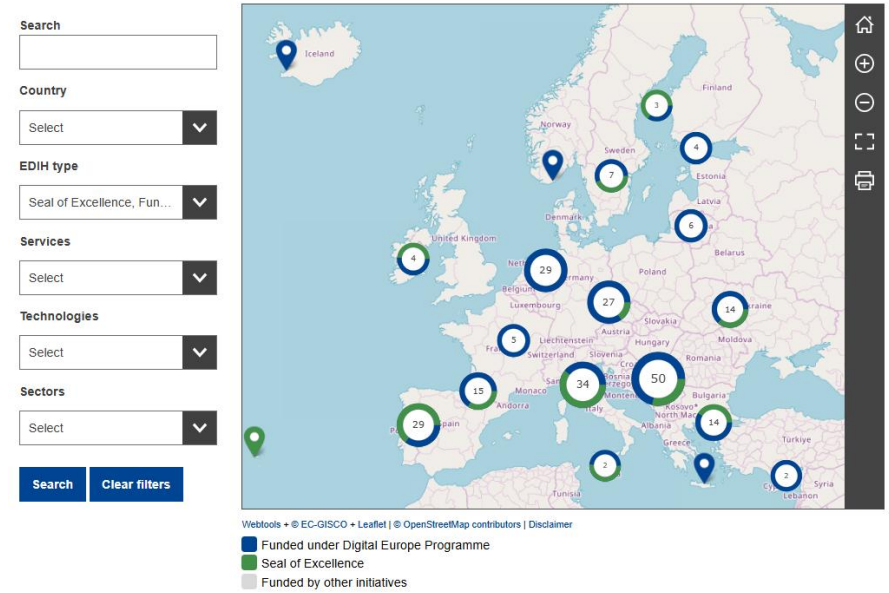
[4] Shalini, S. (2022). Cyber Attacks on SCADA Systems. International Journal of Science and Research (IJSR), 11(3), 1433–1434. https://doi.org/10.21275/sr22327211749

O.O. Tsypliak, Y.S. Dmytruk, O.O. Cheban, V.O. Artemchuk

EUROPEAN DIGITAL INNOVATION HUB OPTIMIZATION USING GENERATIVE ARTIFICIAL INTELLIGENCE TOOLS

1. Introduction

"European Digital Innovation Hubs" (EDIHs) stands for the network of organizations in Europe [1]. Co Founded and financed by European Union (EU) and local governments since 2016 in scope of following global EU strategy **"Digital Europe Programme work programme"** [2] to organize provision of free services for local public sector organizations and small medium private businesses (later in text clients) to boost their productivity and competitiveness [3], this process is called **"Digital Transformation Acceleration"** or simpler "digitalization".

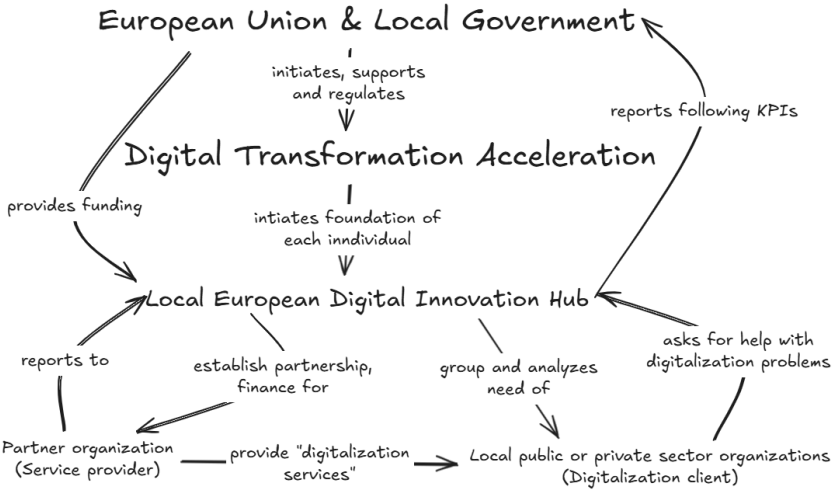


Picture 1 – European Digital Innovation Hub catalogue and map on official EU site

Each individual EDIH finds a set of partner organizations (later in text service providers) that will be providing services to clients for free at 50% cost from the EU and 50% cost from local government following EU approved standard guideline [4].

The cooperation between clients and digital innovation services is evaluated using the "client digital maturity" Key Performance Indicator (KPI). This complex metric assesses a single organization's ability to maintain competitiveness and productivity in light of technological advancements in their industry. To determine the effectiveness of the cooperation, this KPI is measured at the beginning of the

engagement and then reassessed after services are provided, with an increase in the metric indicating successful digital transformation.



Picture 2 – European Digital Innovation Hub business model

When local EDIH can't provide required service it can cooperate with any other EDIH in Europe. As of May 2025 there are 457 EDIHs on the European continent including Ukraine [5] with a total EU budget of 4.5 million euros for the next 4 years[6].

Generative artificial intelligence(later in text AI) impacted business processes around the world a lot with automating and semi-automating previously formerly manual business processes. On the other hand, AI based web systems ability for text summarization unlocked cost effective personalized services that can resolve multiple problems of an individual EDIH.

In scope of work for WIN2EDIH [7], a new multidisciplinar EDIH opened and coordinated in Ukraine by Kyiv National Economic University based on Innovation Ukraine Digital Accelerator [8]. Let's analyze experience of EDIHs across EU and design prototype of AI usage to boost WIN2EDIH competitiveness.

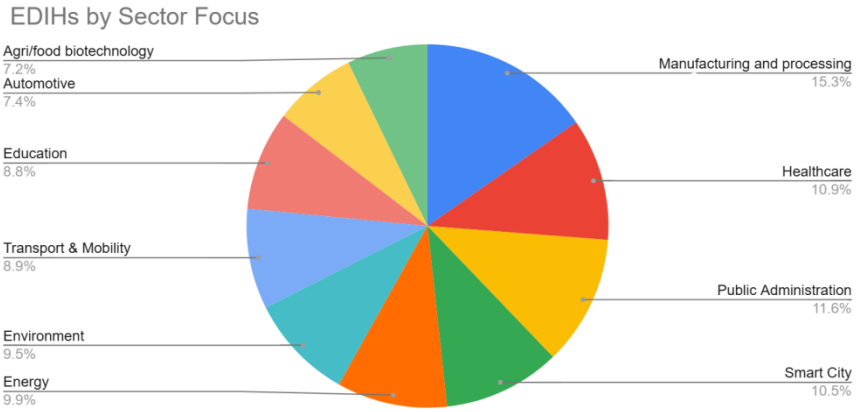
2. Analysis

European Digital Innovation Hubs can be distinguished based on three key criteria [5]: sector focus, technological specialization, and types of services offered. These criteria determine the industries a hub supports, the digital technologies it promotes (such as AI or internet of things), and the range of support services it provides, including training, testing, and access to funding.

We consider these three categories because they provide a structured way to evaluate the capabilities and relevance of each EDIH to specific organizational needs. By assessing sector focus, technological specialization, and service

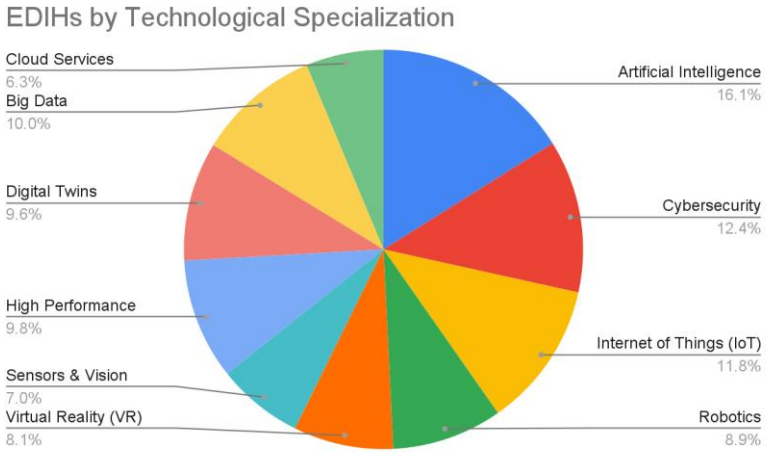
offerings, stakeholders can identify the most suitable hubs for collaboration, innovation support, and digital transformation efforts.

Sector Focus refers to the specific industries or domains (e.g., manufacturing, healthcare, public administration) that the EDIH is designed to support.



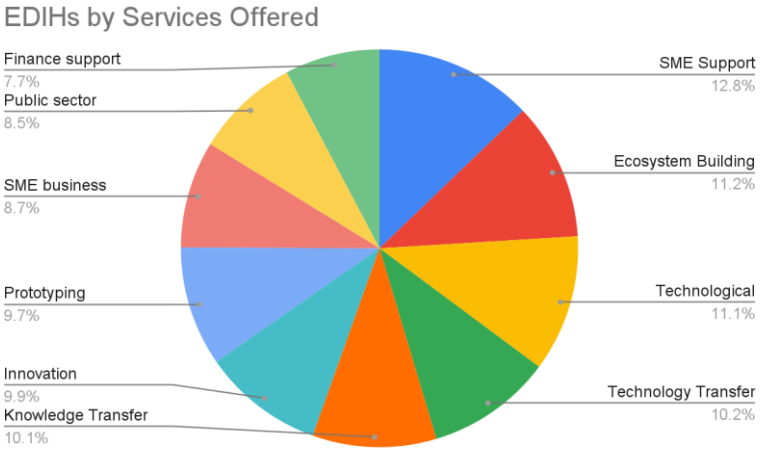
Picture 3 – EDIHs by Sector Focus

Technological Specialization indicates the core digital technologies (such as AI, cybersecurity, or IoT) in which the hub offers expertise and infrastructure.



Picture 4 – EDIHs by Technological Specialization

Service Offerings encompass the types of support provided by the hub, including training, technology testing, innovation consulting, and access to funding.



Picture 5 – EDIHs by Services Offered

Despite all the differences there are common problems for all multidisciplinar EDIHs face as organizations that they need to solve to effectively follow EU digital strategy and achieve KPIs:

- Effectively collect clients needs and find corresponding service
- Involve, motivate and filter reliable partners
- Engage and estimate digital maturity of clients after services receivement

Initial client needs assessment via AI based chatbots can significantly reduce time investment compared to human-conducted assessments. However, implementation challenges include the need for integration with existing service databases and automated data synchronization. Current prototypes from related fields demonstrate that these challenges are feasible [9].

Partner communication is a sensitive topic to delegate to any AI agent, moreover mostly there are less than dozen partners for each EDIH and effective partnership requires life communication and individual conditions discussions based on sensitive data. [11]

Estimation and engagement problems can only be partially solved with AI, because it requires expert contact in specific fields with local limitations understanding. But there are some examples of using AI for test material generation [10], so this option is also worth consideration.

Table 1. All official EDIH KPIs

KPI Category	Indicator	Target/Notes
Outreach	Number of SMEs/public sector entities contacted	Shows awareness-raising success.
	Number of events/workshops organized	Measures outreach activities.
Client Engagement	Number of clients served (SMEs/public sector)	Key measure of hub reach and utility.
	Number of first-time users	Demonstrates ability to engage new clients.
Service Provision	Number of Test Before Invest (TBI) services delivered	Shows technological support provided.
	Number of digital maturity assessments conducted	Assesses client readiness and areas for improvement.
	Number of clients receiving skills/training services	Reflects support for digital skill-building.
	Number of clients supported in accessing finance	Shows facilitation of investment for digitalization.
	Number of services provided related to innovation ecosystem & networking	Reflects collaboration with other hubs and stakeholders.
Impact	Number of clients adopting digital technologies after support	Direct measure of transformation impact.
	Estimated jobs created or maintained due to EDIH support	Socio-economic impact metric.
Collaboration & Network	Number of joint actions with other EDIHs or networks (e.g., EEN, clusters)	Indicates cooperation within the digital ecosystem.
	Number of referrals to other EDIHs or initiatives	Shows integration and inter-hub cooperation.
Satisfaction & Quality	Client satisfaction score (survey-based)	Quality of service delivery.
Administrative	Reports delivered on time	Compliance indicator.

3. Results

Some remarkable EDIH projects that are already using AI to boost their process described below.

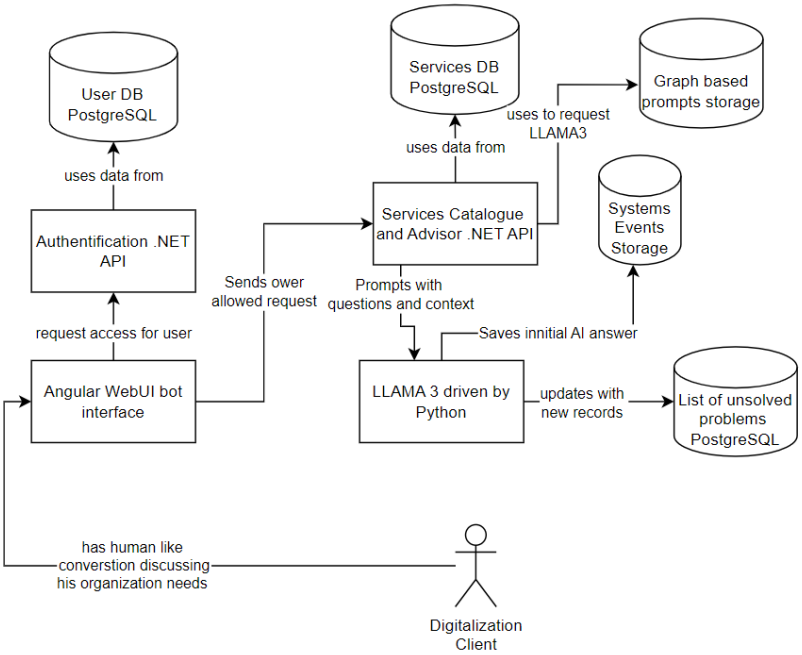
1. Innomine AI EDIH (Hungary)

Innomine has developed a Digital Readiness Assessment **[**12**]** tool tailored for Hungarian SMEs. This tool employs automated evaluation methods to generate a Digital Readiness Index, comparing companies against industry averages. The insights help in crafting customized digital transformation strategies.

2. DIGIS3 (Spain)

DIGIS3 (Spain) focuses on *Trusted Artificial Intelligence* [13] and stands out for using AI internally to **assess the digital maturity** of SMEs and public sector organizations. This internal use of AI enables more accurate evaluations and supports the design of effective digital transformation strategies.

Considering existing systems, EDIH KPIs and currently available technologies, suggestion is to build a chat bot that will in human-like manner discuss client's problems. The idea is to use the LLAMA 3 system, which will be able to analyze existing services across all existing EDIHs and recommend them to clients in live chat without involving humans. The architecture of possible solutions described in the picture below.



Picture 6 – Chatbot with AI for EDIH client support

Also, inspired by the DIGIS3 approach, we propose to develop a system that can autonomously analyse customer needs after submitting Digital Maturity Assessment[8] and recommend relevant services from the entire EDIH network without requiring human involvement. This will enable more accurate assessments and more targeted transformation strategies.

4. Conclusion

This paper presents a model for accelerating digital transformation in the EU through European Digital Innovation Hubs (EDIHs). Given recent advances in generative AI, we examined current EU EDIHs' experiences with AI applications. We describe a generative AI architecture for customer support that could help the new Ukrainian EDIH WIN2EDIH become more competitive.

Prospects of further work on the article are in depth analysis of EDIHs KPI, prototyping of alternative AI solutions to test them and pick the most suitable for WIN2EDIH project. Other aspect of further research will be finding common traits of EDIHs with high KPIs to reuses their best processes

[1] European Digital Innovation Hubs. (n.d.). Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/policies/edihs

[2] The DIGITAL Europe Programme – Work programmes. (n.d.). Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/activities/work-programmes-digital

[3] Get to know us | European Digital Innovation Hubs Network. (n.d.). https://european-digital-innovation-hubs.ec.europa.eu/get-know-us#:~:text=EDIHs%20work%20as%20one-stop,their%20path%20towards%20digital%20transformation

[4] Cooperation guidelines for a seamless digitalization support to European SME. (n.d.). In https://european-digital-innovation-hubs.ec.europa.eu/system/files/2023-11/20231116_DTA_CooperationGuidelines_EDIH_EEN_Clusters_final.pdf.

[5] EDIH Catalogue | European Digital Innovation Hubs Network. (n.d.). https://european-digital-innovation-hubs.ec.europa.eu/edih-catalogue

[6] New European Digital Innovation Hubs set up across the Western Balkans, Ukraine and Türkiye. (n.d.). EEAS. https://www.eeas.europa.eu/delegations/ukraine/new-european-digital-innovation-hubs-set-across-western-balkans-ukraine-and-t%C3%BCrkiye_en

[7] WIN2EDIH | European Digital Innovation Hubs Network. (n.d.). https://european-digital-innovation-hubs.ec.europa.eu/edih-catalogue/win2edih

[8] Innovation Ukraine – Digital accelerator. (n.d.). http://innovationukraine.com/

[9] O. Tsypliak, V. Artemchuk, Console Application Development for Articles' Highlights Generation Based on Artificial Intelligence Designed Using Autonomous Large Language Model, Springer Nature Switzerland, 2024, pp. 53–64. doi:10.1007/978-3-031-71801-4_5.

[10] Samoylov, V., Abramovych, R., & Taranowski, A. (2023). Перспективи побудови тестів контролю знань персоналу АЕС з використанням штучного інтелекту. Nuclear and Radiation Safety, 3(99), 67–74. https://doi.org/10.32918/nrs.2023.3(99).07

[11] Minaee, S., Mikolov, T., Nikzad, N., Chenaghlu, M., Socher, R., Amatriain, X., & Gao, J. (2024). Large Language Models: a survey. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2402.06196

[12] AI EDIH Hungary | European Digital Innovation Hubs Network. (n.d.). https://european-digital-innovation-hubs.ec.europa.eu/edih-catalogue/ai-edih-hungary

[13] Project granted by the European Union: European Digital Innovation Hub (EDIH) | DIGIS3. (n.d.). https://digis3.eu/en/edih

І.О. Сергієнко, В.О. Артемчук

МЕТОДИ ВИКОРИСТАННЯ ВІДНОВЛЮВАНОЇ ЕНЕРГІЇ ТА ТЕХНОЛОГІЙ ЦИФРОВИХ ДВІЙНИКІВ В МЕРЕЖАХ 5G

Стрімке глобальне розгортання мереж 5G супроводжується значно вищим споживанням енергії порівняно з попередніми поколіннями бездротових мереж. Це призводить до суттєвого зростання енергоспоживання порівняно з попередніми поколіннями бездротового зв'язку. За даними GSMA на телекомунікаційні мережі припадає 2-3% всієї спожитої енергії [3]. Це сподвигає операторів шукати стійкі джерела енергії – увага приділяється відновлюваним джерелам енергії (ВДЕ) – сонячна, вітрова, гідроенергія – як ключової стратегії для досягнення цілей сталого розвитку та зменшення залежності від інших видів палива. Важливу роль в оптимізації інтеграції в мережі п’ятого покоління відіграє технологія цифрових двійників – віртуальних копій фізичних об'єктів та систем, що дозволяють здійснювати моніторинг, моделювання та оптимізацію складних інфраструктур [6].

Технологія 5G пропонує унікальні можливості для ефективного управління ВДЕ. Висока швидкість та низька затримка мереж 5G забезпечують збір та аналіз даних у реальному часі з розподілених джерел ВДЕ. Значна пропускна здатність 5G є критично важливою для обробки великих обсягів даних, що генеруються сучасними системами ВДЕ. Це дозволяє здійснювати детальний моніторинг стану обладнання, погодних умов та виробництва енергії. 5G сприяє інтеграції пристроїв Інтернету речей (IoT) для розширеного моніторингу, підтримує граничні обчислення для швидкої обробки даних на місцях та дозволяє використовувати мережевий слайсинг для створення виділених віртуальних мереж під критично важливі функції управління енергією [8].

Технологія цифрових двійників є основою для створення ефективних мереж 5G, що живляться ВДЕ. Цифрові двійники можуть створювати віртуальні представлення інфраструктури мережі 5G та об’єктів відновлюваної енергетики (вітряних турбін, сонячних панелей, гідроелектростанцій), це забезпечує безперервний моніторинг та аналіз продуктивності обох систем [5]. Алгоритми штучного інтелекту (ШІ) та машинного навчання (МН), що інтегровані в цифрових двійників, аналізують дані для прогнозування потенційних проблем (прогностичне обслуговування), оптимізації виробництва та споживання енергії, а також моделювання сценаріїв експлуатації [2]. Це також сприяє покращенню планування мережі, розподілу ресурсів та дотриманню угод про рівень обслуговування (SLA) [7].

Інтеграція ВДЕ для живлення мереж 5G надає низку суттєвих переваг:

- Хоча початкові інвестиції можуть бути значними, експлуатаційні витрати на ВДЕ зазвичай нижчі, що веде до зниження загальних витрат на енергію в довгостроковій перспективі [2].

- Підвищена енергоефективність підтримує цілі корпоративного сталого розвитку шляхом зменшення викидів вуглецю та впливу на навколишнє середовище [2].
- Використовуючи ВДЕ, ми можемо не лише зменшити викиди, але й захистити наші викопні палива від виснаження в майбутньому [1].

Незважаючи на переваги, інтеграція ВДЕ в інфраструктуру 5G стикається з певними викликами:

- Витрати на розгортання інфраструктури ВДЕ можуть бути значними. Стратегії подолання включають державні стимули, державно-приватні партнерства та поетапне розгортання [8].
- Комбінування сонячної, вітрової та інших відновлюваних джерел енергії не лише зменшує вплив 5G на навколишнє середовище, але й гарантує більш стале та енергоефективне функціонування [8].
- Складність інтеграції даних з різноманітних джерел у платформи цифрових двійників. Для більшої точності необхідно враховувати такі фактори, як щільність населення, попит на підключення та цілі цифрової трансформації для кожного сектора [8].
- Зростаючі ризики через велику кількість підключених пристроїв. Необхідні комплексні заходи безпеки: фаєрволи, механізми виявлення загроз в реальному часі, наскрізне шифрування. Передові методи шифрування: квантово-безпечна криптографія, виявлення загроз на основі ШІ [8].
- Труднощі розгортання у віддалених районах. Можливі рішення: приватні мережі 5G, розподілене виробництво ВДЕ [8].
- Відсутність сумісності та стандартизації між платформами розумних міст перешкоджає ефективному використанню 5G. Необхідно сприяти розробці загальногалузевих стандартів [8].

Синергія 5G, ВДЕ та цифрових двійників вже знаходить практичне застосування:

- Вітрові електростанції: Приватні мережі 5G використовуються для покращеного моніторингу та прогностичного обслуговування [4].
- Дубай активно впроваджує відновлювані джерела енергії, включаючи сонячну енергію, у свої функції 5G [8].
- Розумні енергосистеми: 5G та цифрові двійники використовуються для динамічного керування навантаженням та інтеграції ВДЕ [5].
- Живлення базових станцій 5G: Використання ВДЕ, виробленої на місці, та систем накопичення енергії [3].
- Розумні будівлі та міста: Оптимізація споживання енергії, що опосередковано зменшує попит на електроенергію з мережі [8].

Інтеграція відновлюваних джерел енергії для живлення мереж 5G, оптимізована за допомогою технології цифрових двійників, відкриває шлях до більш сталого, надійного та економічно ефективного майбутнього для телекомунікаційного та енергетичного секторів. Потрібно вміти приймати такі виклики як переорієнтація інфраструктури 5G на використання ВДЕ,

інтеграція технології цифрових двійників для оптимізації та управління, оцінка економічної доцільності, впровадження найдіних заходів з кібербезпеки. Важливо також враховувати нестабільності ВДЕ та використовувати комбіновані рішення для уникнення переривань.

[1] arXiv.org e-Print archive. URL: https://arxiv.org/pdf/2403.12283 (дата звернення: 01.05.2025).

[2] Digital twins for energy management in manufacturing explained - shoplogix. Shoplogix | Continuous Improvement Platform for Manufacturers. URL: https://shoplogix.com/digital-twins-for-energy-management/ (дата звернення: 03.05.2025).

[3] Energy efficiency for 5G and beyond 5G: potential, limitations, and future directions - PMC. PMC Home. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC11598088/ (дата звернення: 01.05.2025).

[4] Harnessing the power of private 5G networks for offshore energy: revolutionising wind farms with cutting-edge connectivity - clarus networks. Clarus Networks. URL: https://www.clarus-networks.com/2024/06/05/harnessing-the-power-of-private-5g-networks-for-offshore-energy-revolutionising-wind-farms-with-cutting-edge-connectivity/ (дата звернення: 02.05.2025).

[5] Innovative horizons for sustainable smart energy: exploring the synergy of 5G and digital twin technologies. researchgate.net. URL: https://www.researchgate.net/publication/388485027_Innovative_Horizons_for_Sustainable_Smart_Energy_Exploring_the_Synergy_of_5G_and_Digital_Twin_Technologies (дата звернення: 02.05.2025).

[6] Machine Learning-Based Digital Twin for Predictive Modeling in Wind Turbines, M. Fahim, V. Sharma, T. -V. Cao, B. Canberk and T. Q. Duong, in IEEE Access, vol. 10, pp. 14184-14194, 2022, doi: 10.1109/ACCESS.2022.3147602. (дата звернення: 03.05.2025).

[7] Network digital twins: transforming 5G network management with wipro. Digital Transformation Services for Global IT Solutions - Wipro. URL: https://www.wipro.com/engineering/embracing-network-digital-twins-in-the-5g-era/ (дата звернення: 03.05.2025).

[8] Unleashing the potential of 5G for smart cities: a focus on real-time digital twin integration. MDPI. URL: https://www.mdpi.com/2624-6511/8/2/70 (дата звернення: 02.05.2025).

В.Ф. Залужний

ЗАБЕЗПЕЧЕННЯ ЖИВУЧОСТІ РОЗПОДІЛЕНИХ АВТОМАТИЗОВАНИХ СИСТЕМ ОРГАНІЗАЦІЙНОГО УПРАВЛІННЯ СИЛАМИ ТА ЗАСОБАМИ: ЕНЕРГЕТИЧНА СКЛАДОВА

Вступ. Збільшення просторових меж, висока маневреність і активність бойових дій, різкі зміни обстановки, зростання ролі та місця фактору часу, збільшення обсягу управлінських функцій, потреба оперативно та обґрунтовано формувати варіанти рішень на застосування військ та зброї в умовах невизначеності вхідних даних для вироблення рішень, постійне оновлення технологічної бази систем ситуаційної обізнаності та управління, складність забезпечення їх живучості, потребують нових підходів до подальшого розвитку управлінської діяльності.

Сьогодні ефективне застосування сил і засобів на полі бою забезпечується шляхом використання розподілених автоматизованих систем організаційного управління (РАСОУ) силами і засобами (СЗ). Таким системам притаманні розгалужена мережа засобів зв'язку і комунікацій, використання різноманітних інформаційних технологій, насиченість комплексами засобів автоматизації та *складна структура системи їх енергозабезпечення*.

Механізми, методи та способи забезпечення живучості РАСОУ СЗ є їх невід'ємною частиною. При цьому, еволюція систем управління військами та зброєю обумовлює еволюцію механізмів, методів та способів забезпечення їх живучості. Вагомим внеском у забезпеченні живучості РАСОУ СЗ є гарантоване, якісне, економне та безпечне *енергозабезпечення* її підсистем та елементів, розміщених як у стаціонарних, так і в польових умовах.

Тенденції розвитку збройної боротьби переконливо свідчать, що в майбутньому кількість джерел енергозабезпечення військ буде неухильно зростати. Це обумовлює доцільність створення розподіленої автоматизованої системи організаційного управління енергозабезпеченням ЗС, у якій генеруючі потужності будуть більш розподіленими, ніж концентрованими, що і обумовлює *актуальність* даної теми.

Основна частина. Зміна ландшафту бойових дій обумовлена, насамперед, використанням високотехнологічних та проривних технологій реалізація яких на полі бою вимагає значної енергії.

Мультидоменість, нелінійний характер ведення збройної боротьби вимагають значних обсягів енергії. Виробництво, накопичення та генерування енергії є *критичним аспектом підтримки* поля бою, у тому числі РАСОУ СЗ.

Озброєння та військова техніка завжди потребувала енергії і завжди використовувалась у боротьбі за енергію. Енергія залишається і ресурсом, за який ведеться боротьба, і зброєю, з допомогою якої ведеться ця боротьба.

Досвід російсько-української війни переконливо свідчить, що сьогодні на перший план виходять вперед *методи та способи зберігання* електроенергії та відновлюваних джерел енергії. Ці досягнення ґрунтуються на розробці нових матеріалів, методах виробництва, управлінні енергозабезпеченням військ, у тому числі використанні штучного інтелекту, нових підходах, методах та способах збору енергії.

Наукові дослідження *енергозабезпечення* СЗ охоплюють широкий спектр тем та підходів відповідно до нових вимог ведення збройної боротьби. Особливого значення набувають дослідження, спрямовані на забезпечення СЗ технологіями збору, виробництва, зберігання та управління *новою енергією*:

— поновлюваних джерел енергії, таких як сонячна, вітрова, геотермальна та біопаливо; водню; термоядерного синтезу (синтез з інерційним утриманням, магнітне утримання); поділу (розплавлена сіль, торій, міні-реактори тощо);

— збирання енергії (бездротове, біо-, механічне) та мережевого сховища енергії;

— управління споживанням енергією з підтримкою систем штучного інтелекту;

— створенням акумуляторів на нових технологіях (графен, вуглецеві нанотрубки, твердотільні, металевоповітряні тощо).

Ефективне енергозабезпечення РАСОУ СЗ безпосередньо пов’язане із здатністю військ забезпечити надійний захист від впливу противника стаціонарних та польових місць генерування енергії, мережі її передавання та систем (елементів) енергозабезпечення ЗС.

Вирішення проблеми *ефективного енергозабезпечення РАСОУ СЗ* можливе за рахунок:

— організації розподіленого генерування електроенергії;

— створення на тактичному та оперативному рівні високостійких енергетичних систем військового призначення;

— розвитку резильєнтних мобільних енергетичних систем;

— розвиток автоматизованих систем організаційного управління в системах енергозабезпечення ЗС;

— впровадження у військових мережах енергозабезпечення ЗС технології Smart Grid.

Необхідність організації розподіленого генерування електроенергії, насамперед, обумовлена масовим впровадженням у військах новітніх та проривних технологій, які приводять до виникнення дисбалансу між генеруванням і споживанням енергії або між потребою в її видах.

Реалізація такої концепції передбачає формування *раціональної топології* мереж генерування енергії та її передавання, створення автономних додаткових джерел енергозабезпечення СЗ в безпосередній близькості від споживачів.

У якості додаткових джерел електроенергії можуть застосовуватися:

1) в польових умовах – засоби альтернативної енергетики (сонячні батареї, вітрові генератори, паливні елементи тощо);

2) для стаціонарних умов – традиційні когенераційні установки малої і середньої потужності, що працюють на природному газі. В останньому випадку завдяки розташуванню когенераційних установок безпосередньо у споживачів, стає можливим використання не тільки вироблюваної електроенергії, але і побічної теплової енергії на потреби опалення, гарячого водопостачання або абсорбційного холодопостачання самого власника КГУ.

Для створення на тактичному та оперативному рівні високостійких енергетичних систем військового призначення необхідно:

— визначити вимоги до резильєнтної енергетичної системи військового призначення на підставі математичної моделі HESMA (включає рівняння кінетики, гідродинаміки та теплообміну(;

— розробити модель організаційного управління системою енергозабезпечення СЗ;

— створити полігон для проведення випробувань як елементів, так і високостійких енергетичних систем військового призначення.

На сьогодні актуальність поняття “резильєнтності” набуває все більшої ваги, особливо у контексті триваючих атак країни-агресора на енергетичний сектор України.

Резильєнтність як властивість системи, що полягає у здатності “підготуватися” до несприятливих подій, планувати такі події, сприймати їх, відновлюватися від наслідків зазначених подій і більш успішно адаптуватися до них, передбачає надання відповідної мобільності енергетичним системам військового призначення.

Розвиток резильєнтних мобільних енергетичних систем здійснюється за рахунок впровадження ядерних (*ядерний мікрореактор Holos, США*) та космічних технологій (*результати випробувань в космосі сонячної панелі, прототипу системи надсилання електроенергії з космосу у будь-яку точку Землі*) виробництва електроенергії, впровадження технологій виробництва альтернативної енергетики та систем зберігання енергії.

Зростання попиту на енергетичні ресурси в польових умовах, обумовлює доцільність проведення оптимізації структури генеруючих потужностей резильєнтних мобільних енергетичних систем військового призначення за рахунок розроблення відповідної математичної моделі

При цьому, важливим аспектом надійного постачання в польових умовах СЗ енергетичних ресурсів є автоматизація управління резильєнтними мобільними енергетичними системами військового призначення.

Впровадження *технології Smart Grid* у ЗС передбачає використання інформаційно-комунікаційних технологій для більш ефективного управління процесами генерування, передачі та споживання електроенергії. Концепція Smart Grid розглядається на основі структури “генерування електроенергії – мережі передавання – споживання”.

Технології Smart Grid передбачають: облік енергоресурсів; автоматизацію розподільних мереж управління та моніторинг стану обладнання; автоматизацію магістральних електричних мереж; впровадження технологій використання альтернативних джерел енергії; передавання і розподіл енергоресурсів.

Реалізація концепції Smart Grid дозволить забезпечити підвищення надійності електропостачання, безвідмовності роботи енергосистем, підвищення енергетичної ефективності, збереження навколишнього середовища у частині впровадження відновлювальних джерел енергії.

Висновки. Забезпечення живучості РАСОУ СЗ ЗС можливе за умови гарантованого, якісного, економного та безпечного енергозабезпечення її підсистем та елементів розташованих як у стаціонарних, так і польових умовах.

Забезпечення стійких та адаптивних процесів одержання, опрацювання і пересилання даних, що забезпечують належне функціонування систем РАСОУ СЗ, потребує вирішення проблеми стійкості та адаптивності систем енергозабезпечення ЗС.

Стійкість та адаптивність енергозабезпечення СЗ ЗС вимагають оперативного впровадження резильєнтних енергетичних систем військового призначення, пошуку нестандартних інноваційних рішень для автономізації енергозабезпечення військ від тактичного до стратегічного рівнів управління.

Н.В. Заїка, М.Ю. Комаров, І.В. Мартинюк, О.В. Глущенко

СТІЙКІСТЬ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В КІБЕРПРОСТОРІ: МОДЕЛІ ТА ВДОСКОНАЛЕННЯ МЕТОДІВ ЗАХИСТУ

Доступність критичної інфраструктури (КІ) через кіберпростір робить забезпечення національної безпеки залежним від ступеня її захищеності. Під критичною інфраструктурою слід розуміти сукупність автоматизованих систем управління, що забезпечують функціонування інформаційно-телекомунікаційних мереж, які виконують завдання державного управління, забезпечують обороноздатність, безпеку, правопорядок тощо. Порушення або припинення функціонування цих мереж може призвести до серйозних наслідків.

Захищеність критичної інфраструктури залежить від наявності сучасних технологічних рішень, які відповідають середовищу їх використання, методів їх застосування та засобів захисту від загроз противника. Всі ці аспекти формують основу для ефективного протистояння загрозам у кіберпросторі.

Стійкість є фундаментальною властивістю будь-якої системи, оскільки вона визначає здатність протистояти зовнішнім і внутрішнім загрозам без втрати конфіденційності, цілісності, доступності.

Згідно із загальною теорією систем, однією з ключових характеристик є здатність до самозбереження, яка можлива лише за умови ефективної нейтралізації загроз та мінімізації можливих втрат. Забезпечення стійкості інформаційних і технічних систем потребує комплексного підходу, що включає оцінку ризиків, розробку адаптивних механізмів та вдосконалення заходів безпеки [1]. Оцінка стійкості може здійснюватися як кількісними, так і якісними методами, що дозволяє формувати стратегії захисту критичної інфраструктури та зменшувати негативний вплив кризових ситуацій.

Модель забезпечення стійкості критичної інфраструктури. Ефективне забезпечення стійкості критичної інфраструктури можливе лише на основі комплексного підходу, що включає всі відомі методи та механізми захисту [2-4]. Основні вимоги до такої моделі включають:

Розробку та впровадження механізмів забезпечення захищеності КІ на постійній основі;

Практичну реалізацію засобів захисту для підтримки необхідного рівня безпеки;

Використання сучасних технологій і методів для оптимальної організації процесів захисту;

Постійний моніторинг стану захищеності та виявлення аномалій;

Гнучкість та адаптацію систем безпеки до нових загроз і викликів.

Функція захищеності критичної інфраструктури полягає у виконанні комплексу заходів, що забезпечують стабільність і безпеку системи. Для досягнення необхідного рівня захисту всі заходи мають відповідати критерію

повноти та системності.

Виходячи з визначення стійкості, можна сформулювати її як стан критичної інфраструктури, за якого гарантується її здатність виконувати всі функції захисту, працювати у штатному режимі, адаптуватися до змінних умов та швидко відновлюватися після деструктивних впливів. Крім того, високий рівень сприйнятливості до дестабілізуючих чинників є серйозним викликом, особливо в умовах сучасних загроз.

Основні критерії забезпечення стійкості критичної інфраструктури [5]:

1. Надійність (RL – Reliability Level) – забезпечення безперервної роботи системи через резервні ресурси та альтернативні канали постачання.

2. Стійкість до фізичних загроз (RPT – Resilience to Physical Threats) – здатність інфраструктури витримувати природні катастрофи, техногенні аварії, військові удари та інші фізичні впливи.

3. Кібербезпека (CS – Cyber Security) – рівень захисту інформаційних систем від кібератак, шкідливого програмного забезпечення та витоків даних.

4. Оперативність відновлення (RS – Recovery Speed) – швидкість і ефективність реагування на надзвичайні ситуації та здатність швидко відновлювати критично важливі функції.

5. Гнучкість та адаптивність (FLA – Flexibility and Adaptability) – можливість системи змінюватися відповідно до нових загроз, впроваджувати інноваційні рішення та коригувати сценарії роботи.

6. Координація та управління ризиками (CRM – Coordination and Risk Management) – ефективність взаємодії між державними, приватними та міжнародними партнерами у сфері захисту критичної інфраструктури.

7. Фінансова та ресурсна забезпеченість (FRS – Financial and Resource Support) – рівень фінансування заходів із забезпечення стійкості, наявність людських і матеріальних ресурсів для реалізації запланованих заходів.

8. Сприйнятливість до дестабілізуючих чинників (SDF – Susceptibility to Destabilizing Factors) – рівень впливу політичних, економічних, соціальних та інформаційних загроз на функціонування критичної інфраструктури.

Моделі забезпечення стійкості критичних інформаційних систем (КІС). Ефективне забезпечення стійкості критичних інформаційних систем можливе лише на основі комплексного використання найбільш відповідних моделей та підходів для вирішення цієї проблеми. Під функцією захищеності КІС розуміють сукупність функціонально однорідних заходів, які регулярно здійснюються в інформаційних системах різними засобами та методами з метою створення, підтримки та забезпечення умов, об’єктивно необхідних для ефективного забезпечення стійкості КІС.

Виходячи із визначення стійкості, можна описати можливість забезпечення стійкості як стан захищеності КІС, за якого гарантується її спроможність виконувати повну множину функцій захисту, функціонувати у штатному режимі, адаптуватися до умов, що постійно змінюються, виявляти аномалії, протистояти загрозам та швидко відновлюватися після впливу дестабілізуючих чинників будь-якого виду.

Продовженням дослідження стане використання запропонованої моделі

забезпечення стійкості КІС у майбутньому, після збільшення та удосконалення повноти множини функцій захищеності. Це дозволить підвищити рівень кібербезпеки, гнучкості та стійкості (резильєнтності) критичної інфраструктури в умовах воєнного стану та післявоєнного відновлення.

Пристрої IoT є основними складовими систем КІС та найбільш вразливі для атак, оскільки більшість сучасних IoT-пристроїв не підтримують шифрування. Це ускладнює захист інформації, адже такі пристрої часто використовують бездротовий зв'язок, що робить їхні передачі даних вразливими до перехоплення. Для забезпечення зв'язку між такими пристроями шифрування зазвичай не реалізується через недостатню обчислювальну потужність. Частково проблему можна вирішити за допомогою шлюзу, який зазвичай має достатньо обчислювальних ресурсів для підтримки шифрування та сучасних інтерфейсів обміну інформацією. Проте питання шифрування даних на всіх етапах життєвого циклу пристрою залишається відкритим.

Водночас шифрування залишається необхідним компонентом їхньої безпеки. Одним із можливих рішень є розробка та процес створення обфускатора для захисту програмного забезпечення критичної інфраструктури та поєднує аналіз загроз, розробку методів заплутування коду, тестування та інтеграцію в цикл розробки для підвищення безпеки. Алгоритми обфускації побудовані на зміні структури коду, модифікації змінних, шифруванні текстових даних, переміщенні блоків коду. Методи захисту охоплюють мобільні додатки, IoT-пристрої, SCADA-системи, використання графів та динамічного коду для ускладнення зворотного інжинірингу.

Захист програмного забезпечення від шкідливого коду включає комплексний підхід до безпеки вузлів у гетерогенному середовищі [6-9]. Для ефективного захисту розробляється політика безпеки, що враховує специфіку вузлів (апаратне й програмне забезпечення, операційна система). Важливо регулярно оновлювати компоненти для підтримки актуальності захисних механізмів.

Необхідно інтегрувати механізми виявлення шкідливого коду на рівні вузлів і через мережу, зокрема системи виявлення вторгнень (IDS) і криптографічні методи для захисту даних. Політика безпеки повинна включати контроль доступу та аутентифікацію для мінімізації несанкціонованого доступу. Особливу увагу потрібно приділяти впровадженню моніторингу стану компонентів та вузлів системи та машинного навчання, на основі зібраних історичних даних, для виявлення аномалій, нових загроз і адаптивності системи.

Контроль доступу до пам'яті та даних важливий для запобігання несанкціонованому доступу або модифікації. Верифікація вихідного коду допомагає виявити уразливості, які можуть призвести до виконання шкідливого коду [10-11]. Також важливим є динамічний аналіз для виявлення небезпечних операцій, що можуть бути пропущені при статичній перевірці.

Механізми ізоляції обмежують поширення шкідливого коду, а постійний моніторинг стану компонентів та вузлів системи допомагає виявляти загрози та збої в реальному часі , а також використання оповіщення відповідальних осіб пришвидшує реагування та прийняття рішення щодо подальших дій.

Статичний аналіз перевіряє вихідний код на порушення безпекових політик і виявляє потенційно небезпечні ділянки.

Динамічний аналіз дозволяє відстежувати стан програми під час її роботи і автоматично припиняти виконання при виявленні порушень.

Висновки

Аналіз підходів до забезпечення стійкості критичної інфраструктури показав, що найбільш критичними аспектами є надійність, оперативність відновлення та координація управління ризиками. Водночас менше уваги приділяється питанням кібербезпеки та фінансового забезпечення, що потребує подальших досліджень та вдосконалення методик захисту. Крім того, встановлено, що високий рівень сприйнятливості до дестабілізуючих чинників є серйозним викликом, особливо в умовах сучасних загроз.

Заходи захисту інформаційних систем в комплексі з використанням обфускаційних методів створюють надійний захист і підвищують стійкість ОКІ до кібератак. Комплекс дій щодо підвищення кваліфікації персоналу, компетенцій адміністраторів безпеки призводить до зниження ризику проведення успішних атак на об'єкти критичної інфраструктури.

Подальші дослідження мають зосередитись на розвитку моніторингу та автоматизованих методах виявлення шкідливого коду на основі поведінкового аналізу стану систем, розробці універсальних методів захисту для різнорідних середовищ. Отримані результати можуть бути корисними для розробки та вдосконалення стратегій забезпечення стійкості критичної інфраструктури України.

[1] Sharma R., Shahi M. (2019). Neural Network Models for Cyber Risk Assessment.Springer.

[2] Chen M., Zhang H. (2020). Integrating Fuzzy Logic in Information Security Risk Assessment.Journal of Risk Analysis, 31(4), 202–211.

[3] Gupta R., Soni A. (2020). Evaluation of Risk Factors in Information Security Using Fuzzy Logic. International Journal of Computer Science and Information Security, 18(4), 191–198.

[4] Shevchenko N.I., Plahotniuk R.V. (2024). Methodological approaches to assessing the stability of the functioning of criticalinfrastructure facilities in the conditions of a special period of the functioning of the economy of Ukraine. Reforming the economy and innovative development strategies, 14 (21), 12–126.

[5] Сидоренко В.М., Максимець А.В. (2025). Модель забезпечення стійкості критичних інформаційних систем в умовах впливу внутрішніх та зовнішніх дестабілізуючих чинників. Кібербезпека: освіта, наука, техніка, 3 (27), 560-571.

[6] Костюк Ю.В., Довженко Н.М., Мазур Н.П., Складанний П.М., Рзаєва С.Л. (2025). Методика захисту grid-середовища від шкідливого коду під час виконання обчислювальних завдань. Кібербезпека: освіта, наука, техніка, 3 (27),

22-40.
[7] Yaremenko O.I., Strahnitsky Y.I. (2023). Theoretical approaches to determining the definition of critical infrastructure as an object of state administration. Bulletin of State Administration, (2), 47–58.
[8] Kovalchuk I. (2023). Critical Infrastructure Protection: International Experience and Ukrainian Realities. Strategic Priorities, 1(10), 23–38.
[9] Kyrylenko S.P., Tyshchenko V.V. (2023). Risk Assessment Models for Critical Infrastructure in Armed Conflict. Life Safety, 3(9), 74–88.
[10] Dang B., Gazet A., Bachaalany E. (2014). Practical Reverse Engineering.
[11] Іванченко С.О., Гавриленко О.В., Липський О.А. [та ін.] (2016). Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації: навчальний посібник. Київ: НТУУ «КПІ».

М.С. Кондратенко

ЗАГРОЗИ ДЛЯ ЦИФРОВОЇ ЕНЕРГЕТИКИ ТА РОЛЬ ТЕХНОЛОГІЇ БЛОКЧЕЙН У ЗАБЕЗПЕЧЕННІ КІБЕРСТІЙКОСТІ

Цифровізація енергетичної галузі відкриває нові можливості для автоматизації, гнучкості управління та підвищення енергоефективності. Водночас, інтеграція інформаційних технологій у критичну інфраструктуру енергосистем породжує серйозні кібернетичні виклики. Зокрема, загрози підміни даних та атаки на SCADA-системи вимагають негайного впровадження інноваційних засобів захисту, здатних протистояти подібним атакам.

Переважна більшість автоматизованих систем управління будується на базі промислових контролерів, які є первинними засобами збору, обробки інформації, регулювання технологічними параметрами, аварійної сигналізації, захисту і блокування (нижній рівень системи). Оброблена контролерами інформація передається до комп'ютеризованих систем, які є робочим місцем оператора-технолога, де відбувається подальша обробка даних процесу і представлення оператору в інтуітивно зрозумілому вигляді (верхній рівень АСУ ТП). SCADA-системи в ієрархії програмно-апаратних засобів промислової автоматизації знаходяться на верхньому рівні. Якщо спробувати стисло охарактеризувати основні функції, то можна сказати, що SCADA-система збирає інформацію про технологічний процес, забезпечує інтерфейс з оператором, зберігає історію процесу і здійснює управління процесом в тому об’ємі, в якому це необхідно.[1]

Розглянемо детальніше проблеми підміни даних та атаки на SCADA. SCADA (Supervisory Control and Data Acquisition) — це серце багатьох автоматизованих енергетичних систем. Вразливість SCADA часто полягає у відсутності шифрування або слабких механізмах автентифікації. У разі компрометації зловмисник може:

- **Підмінити показники** споживання або генерації;
- **Змінити параметри керування обладнанням**, що загрожує виходом з ладу або навіть аварією;
- **Блокувати або викривляти сигнал** моніторингу, залишаючи операторів у невіданні.

Сучасні приклади атак, як-от **BlackEnergy** чи **Industroyer**, продемонстрували реальну шкоду від зламу систем керування енергетичними об’єктами. Саме в результаті виконання троянської програми BlackEnergy 23 грудня 2015 року протягом трохи більше однієї години була виведена з ладу підстанція «Північна» енергокомпанії «Укренерго», без струму залишились споживачі північної частини правого берегу Києва та прилеглих районів області. Найбільше постраждали споживачі «Прикарпаттяобленерго»: було

вимкнено близько 30 підстанцій, близько 230 тисяч мешканців залишались без світла протягом від однієї до шести годин.[2]

Розглянемо ключові особливості та переваги технології блокчейн, оскільки саме вона може слугувати захистом від подібних атак. Деякі концепції технології блокчейн було описано ще 30 років тому, проте перше її практичне застосування відбулося у 2008 р. — була створена криптовалюта Bitcoin на основі блокчейну. З кожним днем ця технологія стає все більш популярною, набуває ширшого спектру застосування. Блокчейн — це новий вид зберігання інформації, децентралізована БД, подана неперервним ланцюгом зв'язаних між собою блоків. Блокчейн використовує різні криптографічні механізми для забезпечення роботи системи. Основними з них є наступні:

- геш-функції — базовий механізм блокчейну, що забезпечує безпосередньо його функціонування;
- цифрові підписи — кожен користувач, який вносить якусь інформацію в блок, повинен підписати цю інформацію;
- протоколи доведення без розголошення, або алгоритми кільцевих підписів, якщо цей блокчейн має функцію підвищеної анонімності.

Крім основних, блокчейн може використовувати такі криптографічні примітиви, як симетричне, асиметричне або гібридне шифрування (наприклад, якщо в нього вбудовано функцію таємного голосування), та деякі інші алгоритми.[3] Технологія блокчейн пропонує концепцію **незмінного журналу подій** (immutable ledger), який децентралізовано фіксує всі транзакції або зміни в системі. Це забезпечує:

- **Неможливість прихованої підміни даних**, оскільки всі зміни записуються з криптографічними підписами;
- **Децентралізацію довіри**: не потрібен єдиний адміністратор або сервер;
- **Прозорість змін** у режимі реального часу.

У разі атаки зловмисника, система одразу зафіксує відхилення, яке не можна буде ретроспективно приховати або видалити.

Також, одним з ключових викликів у захисті енергетичних систем є **ідентифікація та автентифікація** польових пристроїв (сенсори, RTU, PLC). Використовуючи блокчейн, кожному пристрою можна надати:

- **Цифровий ідентифікатор**, записаний у блокчейн;
- **Криптографічний ключ**, з яким він підписує свої дії;
- **Політику довіри**, що контролюється смарт-контрактами.

Це дозволяє гарантувати, що лише авторизовані пристрої можуть взаємодіяти в системі, а всі їхні дії будуть підтверджені та прозорі.

Окрім цього, розглянемо питання відстеження історії конфігурацій і змін у ролі ще одного виклику для цифрової енергетики. У великих енергосистемах часто виникає потреба у веденні історії змін налаштувань обладнання, зокрема: оновлення ПЗ мікроконтролерів; зміни логіки

керування; підключення нових вузлів.Замість традиційних логів на централізованих серверах, блокчейн може стати **єдиним джерелом правди** (single source of truth). Наприклад, кожна зміна в налаштуваннях записується у вигляді транзакції, що підписується відповідальним оператором. Це:

- Забезпечує **повну трасованість (**відстежуваність**)** змін;
- Запобігає несанкціонованому втручанню;
- Полегшує аудит та, за необхідності, процес розслідування у разі інциденту.

Як висновок, варто зазначити, що технологія блокчейн може стати ключовим компонентом нової архітектури **захищеної та прозорої цифрової енергетики**. Вона вирішує низку критичних проблем, серед яких: підміна даних, автентифікація пристроїв, захист SCADA-систем і ведення журналу змін. Інтеграція блокчейну в енергетику не є панацеєю, але це потужний інструмент підвищення **резильєнтності та довіри** до систем, від яких залежить національна безпека.

[1] «Обробка інформації». Вікіпедія. Вільна енциклопедія. https://uk.wikipedia.org/wiki/Обробка_інформації

[2] «Кібератака на енергетичні компанії України». Вікіпедія. Вільна енциклопедія. https://uk.wikipedia.org/wiki/Кібератака_на_енергетичні_компанії_України

[3] Кондратенко, М.С. (2023). Використання технології блокчейну при побудові ієрархічної структури на множині державних реєстрів для захисту від підробки інформації. Електронне моделювання, 45(3), 43–56. https://www.emodel.org.ua/images/em/45-3/45-3-4.pdf

І.Г. Гіваргізов, А.С. Недашківський

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ЛОГІСТИЧНИМИ КОМПАНІЯМИ

У період з 2021 по 2024 рік інформаційні технології зазнали значних змін, найбільше уваги було зосереджено на прориві у розвитку квантових комп'ютерів та штучному інтелекту. Наприклад, у 2023 році компанія IBM представила новий квантовий процесор "Condor", який працює на 1121 кубіті, згодом, компанія Google також представила свою квантову систему "Sycamore". [11] У сфері штучного інтелекту вагомих результатів за останні роки досягли компанії OpenAI, Google та Meta, які активно ведуть подальшу роботу над вдосконаленням своїх моделей. Наприклад, у 2022 році компанія OpenAI презентувала першу загальнодоступну всім модель штучного інтелекту. За перші два місяці користування платформа зібрала понад 100млн користувачів. [10]

Стрімке впровадження ШІ в різні сфери діяльності такі як медицина, фінанси, логістика - створило конкуренцію між провідними технологічними компаніями, зокрема Microsoft, OpenAI, Google, Meta та інші. [6] Це призвело до інвестування значних ресурсів у вдосконалення моделей, їх роботу та функціоналу. Наприклад, у 2023 році компанія Microsoft інвестувала 13млрд доларів в компанію OpenAI, що дозволило впровадити штучний інтелект у продукти від Microsoft 365. [9] Станом на сьогодення існує вже безліч різноманітних ШІ моделей, кожна з яких адаптована під найрізноманітніші потреби суспільства. Вагомою перевагою ШІ стала його доступність, адже були розроблені мобільні застосунки та веб-сайти, що дало змогу мільйонам користувачів використовувати штучний інтелект.

Інтеграція штучного інтелекту в наявні інформаційні системи дозволила компаніям запровадити його використання та ефективно оптимізувати свої внутрішні процеси. Використання логістичними компаніями штучного інтелекту значно спрощує виконання різноманітних складних математичних розрахунків, які допомагають ефективному управлінню великою кількістю логістичних процесів. Наприклад, компанія UPS впровадила систему "ORION", яка за допомогою алгоритмів штучного інтелекту оптимізовує логістичні маршрути. Впровадивши систему "ORION" компанія UPS зекономила близько 100 млн доларів та 10 млн галонів палива на рік. [8] Раніше, оптимізацію логістичних маршрутів виконувалася за допомогою задачі комівояжера, яка передбачає пошук найкоротшого маршруту. Зокрема, найпоширенішим напрямком застосування ШІ у транспортній сфері є планування та оптимізація маршрутних перевезень, де використовуються складні математичні обрахунки. Завдяки алгоритмам машинного навчання з'являється можливість аналізувати великі масиви даних в режимі реального часу та скорегувати маршрут відповідно до цих даних, які можуть включати погодні умови, завантаженість доріг та інші параметри [2] Це дає змогу

компаніям скоротити час доставки та зменшити витрати на пальне, наприклад, як це реалізувала компанія UPS. Окрім оптимізації логістичних маршрутів, ШІ розпочали активно залучати і до процесів прийняття рішень. Він здатний проаналізувати великий об'єм аналітичних даних та формувати детальні прогнози на основі важких математичних обчислень, які допоможуть логістичним компаніям приймати стратегічні рішення. [4] Це дозволяє компаніям підвищити точність прогнозування, зменшити ризики та покращити довгострокове планування.

Впровадження штучного інтелекту охоплює не лише оптимізацію маршруту, обробку великих даних, але й здійснює зміни на глобальному ринку праці. ШІ все частіше починає виконувати роботу, яку раніше виконували люди, від оптимізації логістичних маршрутів до складських операцій. За прогнозами, до 2030 року приблизно 41% компаній планують скорити численність персоналу внаслідок впровадження автоматизованих робочих процесів із використанням штучного інтелекту та розумних роботів. [5] За даними дослідження McKinsey, логістичні компанії які впровадили ШІ у свої процеси оптимізації маршруту та складські операції, змогли зменшити витрати на логістику на 15%. Великі компанії уже розробляють плани щодо подальшого впровадження та використання ШІ, зокрема увага зосереджена на залученні роботизованих систем до логістичних процесів. Наприклад, інтернет магазин Amazon активно залучає роботизовані системи до складських операцій. [7]

Отже, використання ШІ у сфері логістики значно покращує логістичні операції та зменшує витрати. Завдяки можливості аналізувати великий обсягів даних, це дозволяє оптимізувати логістичні маршрути в режимі реального часу, враховуючи різноманітні типи даних. Також, ШІ допомагає здійснювати моніторинг технічного стану транспортних засобів та сприяти підтримці у прийнятті рішень. У підсумку, це дозволяє компаніям покращити логістичні та операційні процеси, а також заощаджувати чималі кошти.

[1] ШІ в логістиці. [Електронний ресурс] URL: https://surl.li/jzclgm (дата звернення 07.04.2025)

[2] Штучний інтелект у логістиці та як його використовують світові й українські компанії. [Електронний ресурс] URL: https://surl.li/ndshba (дата звернення 07.04.2025)

[3] Succeeding in the AI supply-chain revolution. [Електронний ресурс] URL: https://surl.li/dtuakq (дата звернення 09.04.2025)

[4] How AI and Machine Learning Enhance Route Optimization. [Електронний ресурс] URL: https://surl.li/vpihwq (дата звернення 10.04.2025)

[5] 41% of companies worldwide plan to reduce workforces by 2030 due to AI. [Електронний ресурс] URL: https://surl.li/cdwfhq (дата звернення 11.04.2025)

[6] Майбутнє ШІ. Amazon, Google, Meta та Microsoft планують інвестувати у ШІ 300 млрд доларів. [Електронний ресурс] URL: https://surl.lu/kbtqib (дата звернення 09.04.2025)

[7] Amazon представила свого першого повністю автономного мобільного складського робота Proteus. [Електронний ресурс] URL: https://surl.li/suqang

(дата звернення 12.04.2025)
[8] Route Smarter, Not Harder: UPS's ORION Success. [Електронний ресурс] URL: https://surl.li/yfidng (дата звернення 12.04.2025)
[9] Microsoft інвестує 13 млрд доларів в OpenAI. [Електронний ресурс] URL: https://surl.li/kawsna (дата звернення 12.04.2025)
[10] Феномен ChatGPT. [Електронний ресурс] URL: https://surl.li/kzizlw (дата звернення 12.04.2025)
[11] IBM створила другий по величині квантовий комп'ютер у світі. [Електронний ресурс] URL: https://surl.li/sfopuj (дата звернення 12.04.2025)

І.Г. Гіваргізов, А.С. Недашківський

ВИКОРИСТАННЯ ЧАТ-БОТА В ІНФОРМАЦІЙНІЙ СИСТЕМІ ТРАНСПОРТНОЇ КОМПАНІЇ

У сучасному світі транспортні компанії відіграють ключову роль у повсякденному житті всього людства. Вони щодня виконують величезну кількість логістичних операцій для своєчасної доставки товарів споживачам, підприємствам, об'єктам критичної інфраструктури та іншим. За даними Євростату у 2023 році обсяг автомобільних вантажних перевезень у ЄС склав понад 13,2 мільярда тон і приблизно 1 857 мільярдів тонно-кілометрів. [1] З кожним роком дана статистика буде тільки збільшуватися, адже логістичні компанії покращують свої маршрути, роботу складський операцій та багато чого іншого.

У покращенні логістичних операцій вагому роль відіграє штучний інтелект, який здатен аналізувати великі обсяги даних та оптимізувати логістичні перевезення. Це особливо важливо для транспортних компаній, які прагнуть забезпечити своїм клієнтам швидку доставку, що є ключовим фактором конкурентоспроможності на ринку. Проте за кожним доставленим товаром стоїть складний процес, який вимагає злагодженої роботи багатьох етапів. Багато факторів впливає на успішну доставку замовлення, зокрема це обробка, сортування, пакування замовлення, планування маршрутів, відстеження замовлення та інші складні процеси. Кожна із цим операцій вимагає точності, реагування на різноманітні ситуації та взаємодії. За допомогою штучного інтелекту транспортні компанії можуть спростити свої внутрішні операції, однак не менш важливою є й клієнтська сторона, яку необхідно також обслуговувати та роботи її процеси більш автоматизованими.

Споживачі очікують від логістичних компаній не лише швидкої доставки, але й повної інформації на всіх етапах транспортування. Із розвитком та зростанням популярності електронної комерції все більше споживачів віддають перевагу онлайн-покупкам. Наприклад, у 2024 році українці витратили на онлайн шопінг понад 239 мільярдів гривень, що на 25% більше ніж у 2023 році. [2] Клієнтам важливо мати доступ до актуальної інформації щодо свого замовлення та в разі непередбачуваних ситуацій вносити зміни. Більшість логістичних компаній мають власні веб-сторінки, які дозволяють клієнтам відстежувати своє замовлення за допомогою трек номера, який автоматично генерується при створення транспортної накладної.

У зв'язку зі стрімким зростання популярності мобільних додатків, логістичні компанії розпочали розробку та впровадження до своїх інформаційних систем мобільних застосунків. Наприклад, за 2023 рік користувачі завантажили понад 110 мільярдів додатків на Google play та понад 41 мільярдна на App store. [3] Відома українська логістична компанія

“Нова пошта”, яка впроваджує в свої логістичні процеси цифрові рішення, повідомила, що понад 70% користувачів взаємодіють із своїми замовленнями через мобільний застосунок.

Розвиток мобільних застосунків суттєво вплинув і на електронну комерцію, яка змістила свій фокус в бік соціальних мереж. Такі платформи, як Instagram, Telegram, Facebook та TikTok деталі частіше стали використовуватися, як торгівельні майданчики. Наприклад, найпопулярнішою соціальною мережею у світі за кількістю щомісячних активних користувачів є Facebook та Telegram. [4][5] Окрім, створення інтернет магазинів, соціальна мережа Telegram також дозволяє створювати чат-ботів, які набувають все більшої популярності серед користувачів та як інструмент взаємодії для компаній. Компанії можуть розробляти ботів та впроваджувати їх до своїх інформаційних систем для виконання широкого спектру задач, таких як оформлення замовлень, сповіщення про статус, отримання консультацій та інші.

Велика популярність серед соціальних мереж, змушує компанії інтегрувати свої інформаційні системи до відповідного тренду. При створенні інформаційної системи транспортної компанії, її унікальність буде полягати у створенні чат-бота, який буде слугувати для взаємодії між клієнтом. Він буде давати змогу користувачеві створювати замовлення, шляхом введення ключових даних, таких як: вага вантажу, пункт відправлення і доставки, терміновість перевезення.

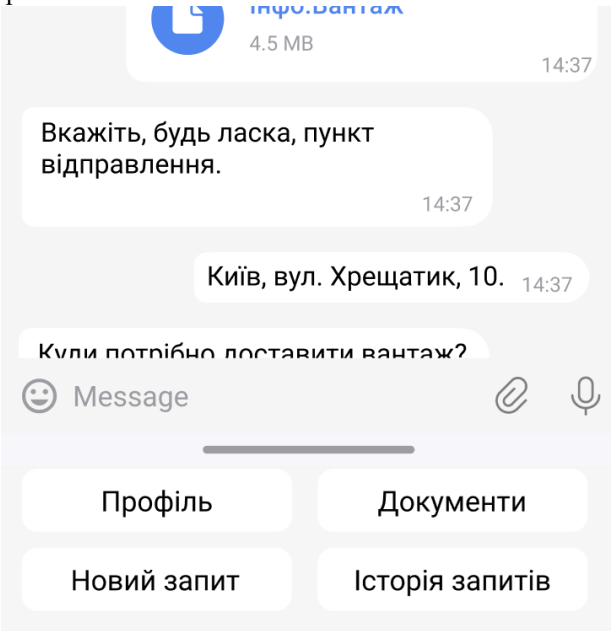


Рис. 1 – Інтерфейс чат-бота

Інтерфейс чат-бота буде досить простим та зрозумілим для використання. Зокрема він матиме наступні пункти: Документи, Відстеження, Новий запит, Історія запитів. Кожен із цим пунктів буде відображати відповідно інформацію, а зібрані дані будуть передаватися до аналітичного модуля, який виконуватиме підбір транспорту, оптимізацію маршруту та формувати заявки для менеджера.

Отже, інтеграція чат-ботів у логістичні процеси суттєво підвищує ефективність взаємодії між користувачами та компаніями. Можливість впровадження чат-ботів, які набувають все більшої популярності, дозволяє компаніям максимально покращити взаємодію з користувачами. Розробка та інтеграція бота з основною системою, де вся інформація буде автоматично оброблятися та передаватися менеджерам, значно зменшить можливість виникнення помилок та пришвидшить роботу.

[1] Road freight transport statistics. [Електронний ресурс] URL: https://surl.li/aysygk (дата звернення 12.04.2025)
[2] Як змінились ключові показники українського e-commerce у 2024 році. [Електронний ресурс] URL: https://surl.li/ljmqbh (дата звернення 12.04.2025)
[3] Річний звіт про ринок мобільних додатків. [Електронний ресурс] URL: https://surl.li/foopfg (дата звернення 12.04.2025)
[4] Соціальні мережі 2024. [Електронний ресурс] URL: https://surl.li/qosydy (дата звернення 12.04.2025)
[5] Кількість активних користувачів Telegram перевищила 1 млрд. [Електронний ресурс] URL: https://surl.li/bydcfd (дата звернення 12.04.2025)

В.Р. Герасимов, В.В. Душеба

НОРМАТИВНЕ РЕГУЛЮВАННЯ МІГРАЦІЇ ТА УПРАВЛІННЯ ДАНИМИ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

З розвитком цифрових технологій та зростанням обсягів даних, що потребують зберігання й обробки, підприємства та організації стикаються з необхідністю модернізації інформаційних систем. Одним із ключових напрямів такої модернізації є міграція з традиційних реляційних баз даних (РБД) до NoSQL-систем, які забезпечують більшу масштабованість, гнучкість структури та ефективну обробку неструктурованих даних.

Однак міграція баз даних є складним процесом, що вимагає не лише технічних знань, але й чіткого дотримання стандартів якості, інформаційної безпеки, а також відповідності чинному законодавству. У цьому контексті особливого значення набуває аналіз міжнародних і національних нормативних документів, які регламентують процеси управління інформацією.

Щоб забезпечити надійність міграційних процесів, важливо дотримуватися міжнародних стандартів, які регламентують управління інформаційними активами, розробку та супровід систем, а також забезпечення якості даних:

ISO/IEC 27001:2013 — Цей стандарт визначає вимоги до створення, впровадження та вдосконалення системи управління інформаційною безпекою (СУІБ). У контексті міграції даних до NoSQL важливо враховувати питання захисту конфіденційної інформації, безпечного зберігання резервних копій, контроль доступу, ведення журналів змін [1].

ISO/IEC 25012:2008 — Модель якості даних, що визначає такі характеристики, як точність, повнота, узгодженість, актуальність, доступність. У процесі міграції необхідно забезпечити відповідність даних цим критеріям, щоб уникнути втрати або спотворення інформації [2].

ISO/IEC 12207:2017 — Описує життєвий цикл програмного забезпечення, включаючи проектування, розробку, експлуатацію та підтримку. Стандарт дозволяє формалізувати процеси, пов’язані з перенесенням БД, включаючи вимоги до тестування після міграції [3].

ISO/IEC 27002:2022 — Регламентує управління IT-активами, у тому числі даними та ПЗ. Під час міграції актуальним є аудит використовуваних ресурсів, контроль версій систем, відстеження змін у структурі даних [4].

ДСТУ ISO/IEC 2382:2015 — Українська адаптація міжнародного стандарту, який забезпечує єдину термінологічну базу в IT-сфері. Стандартизація понять є важливою для уніфікації проектної документації та забезпечення міжсистемної сумісності [5].

В Україні правову основу для міграції інформаційних систем визначають закони, що стосуються захисту персональних даних, інформаційної безпеки та правового статусу цифрових ресурсів:

Закон України «Про захист персональних даних» — регулює збір, обробку та зберігання персональних даних, забезпечуючи, що міграція СУБД не порушує прав користувачів та гарантує належний рівень захисту особистої інформації [6].

Закон України «Про інформацію» — встановлює правові засади інформаційних відносин, зокрема принципи доступу, достовірності та правомірного використання даних [7].

Окрім базових законів, важливе значення для регулювання процесів міграції даних мають й інші нормативні акти. Зокрема, Постанова Кабінету Міністрів України № 373 «Про затвердження Порядку забезпечення кіберзахисту державних інформаційних ресурсів» встановлює вимоги до організації захисту інформації в державному секторі, що є важливим у випадках перенесення баз даних, які містять критичну або чутливу інформацію. ДСТУ ISO/IEC 27002:2020 містить практичні рекомендації щодо впровадження політик інформаційної безпеки, включаючи захист даних на етапах обробки, зберігання та передачі. Також варто враховувати нормативні документи, видані Державною службою спеціального зв'язку та захисту інформації України, що регулюють питання криптографічного захисту, електронного документообігу та інші аспекти технічного захисту інформації.

Міграція реляційних баз даних у NoSQL не може розглядатися виключно як технічна процедура. Це складний процес, що має відповідати міжнародним стандартам якості та інформаційної безпеки, а також бути узгодженим з вимогами національного законодавства щодо захисту даних. Недотримання цих вимог може призвести до юридичних наслідків, втрати довіри користувачів або фінансових втрат. Водночас комплексний підхід до міграції, з урахуванням регуляторного середовища, забезпечує не лише ефективність трансформації IT-інфраструктури, але й її правову безпеку та стабільність.

[1] ISO/IEC 27001:2022 - Information security management systems. — URL: https://www.iso.org/standard/27001 (дата звернення: 2025-04-17)

[2] ISO/IEC 25012:2008 - Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Data quality model — URL: https://www.iso.org/standard/35736.html (дата звернення: 2025-04-17)

[3] ISO/IEC/IEEE 12207:2017 - Systems and software engineering — Software life cycle processes — URL: https://www.iso.org/standard/63712.html (дата звернення: 2025-04-18)

[4] ISO/IEC 27002:2022 - Information security controls — URL: https://www.iso.org/standard/75652.html (дата звернення: 2025-04-18)

[5] ISO/IEC 2382:2015 - Information technology — Vocabulary — URL: https://www.iso.org/standard/63598.html (дата звернення: 2025-04-18)

[6] ЗАКОН УКРАЇНИ. Про захист персональних даних | від 01.06.2010 № 2297-VI — URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 2025-04-20)

[7] ЗАКОН УКРАЇНИ. Про інформацію | від 02.10.1992 № 2657-XII— URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 2025-04-21)

О.М. Джигун, К.В. Булда

ЕЛЕКТРОЕНЕРГЕТИКА УКРАЇНИ НАПЕРЕДОДНІ І ПІД ЧАС ВІЙСЬКОВОЇ АГРЕСІЇ

Електроенергетика України — базова галузь економіки України, є однією з найстарших. Генерація електроенергії ґрунтується на атомній енергетиці, спалюванні вугілля, мазуту, природного газу, біопалива, а також застосуванню відновлювальних джерел енергії вітру, води, сонця. 24 лютого 2022 року, за декілька годин до початку повномасштабного вторгнення, Україна від'єдналась від енергосистем росії і білорусі. Це був режим ізоляції, запланований на 3 дні, але більше Україна не повернулась до енергосистеми ворога. За три роки повномасштабної війни росія здійснила понад 30 масованих атак на енергетичну інфраструктуру України та окупувала об'єкти генерації загальною потужністю 18 ГВт

Об'єднана енергетична система України (ОЕСУ) — сукупність електростанцій, електричних і теплових мереж, інших об'єктів електроенергетики, що об'єднані спільним режимом виробництва, передавання та розподілу електричної й теплової енергії за їхнього централізованого керування.

Виробництво електроенергії в ОЕСУ у 2021 році, за оперативними даними, збільшилося на 5,2% (на 7 млрд 719,5 млн кВт-год) порівняно з 2020 роком, до 156 млрд 575,7 млн кВт- год. Атомні електростанції (АЕС) збільшили вироблення електроенергії на 13,1% – до 86 млрд 205,4 млн кВт-год. Зокрема, виробництво на Запорізькій АЕС становило 35 млрд 457,5 млн кВт-год (+23,4% до 2020-го), Южно-Українській – 18,626 млрд кВт-год (-3,8%), Рівненській – 18 млрд 827,3 млн кВт-год (+10,3%), Хмельницькій – 13 млрд 294,6 млн кВт-год (+20,5%). Теплові електростанції (ТЕС), а також теплоелектроцентралі (ТЕЦ) та когенераційні установки (КУ) знизили вироблення на 12,5% – до 45,834 млрд кВт-год. У тому числі генкомпанії ТЕС зменшили виробництво 5,9% – до 37 млрд 224,9 млн кВт-год, ТЕЦ та КУ – на 32,7%, до 8 млрд 609,1 млн кВт-год. Гідро- та гідроакумулюючі електростанції (ГЕС та ГАЕС) збільшили виробництво на 37,7% – до 10 млрд 445,8 млн кВт-год, тоді як блок-станції зменшили на 14,9% – до 1 млрд 570,8 млн кВт- год. Виробництво електроенергії альтернативними джерелами (ВЕС, СЕС, біомаса) збільшилося на 15,3% – до 12 млрд. 519,7 млн. кВт-год [1]. Частка АЕС у структурі виробництва електроенергії становила 55,1% (у 2020 році – 51,2%), ТЕС, ТЕЦ та КУ – 29,3% (35,2%), ГЕС та ГАЕС – 6,7% (5, 1%, блок-станцій – 1% (1,2%), альтернативних джерел – 8% (7,3%). Відпуск теплової енергії в 2021 році зріс на 3,1% (на 645,9 тис. Гкал) порівняно з 2020-м – до 21 млн 560,7 тис. Гкал.

Споживання електроенергії в Україні в 2021 році з урахуванням технологічних втрат у мережах збільшилося на 5,7% (на 8 млрд 390,9 млн кВт-год) порівняно з 2020 роком, до 154 млрд 825,7 млн кВт-год.

Промисловість країни без урахування технологічних втрат наростила споживання електроенергії на 6% – до 52 млрд. 273,6 млн. кВт-год. У тому числі металургійна галузь спожила 28 млрд 872,8 млн кВт-год (+6,4% до 2020-го), паливна – 3 млрд 261,5 млн кВт-год (+0,9%), машинобудівна – 3 млрд 522,1 млн кВт-год (+11,3%), хімічна та нафтохімічна – 4 млрд 349,2 млн кВт-год (+4,6%), харчова та переробна – 4 млрд 404,7 млн кВт-год (+1,5%), будівельних матеріалів – 2 млрд 669,9 млн кВт-год (+14,4%), інша – 5 млрд 193,5 млн кВт-год (+5%). Сільгосппідприємства споживали 3,692 млрд кВт-год (-2,8%), транспортні – 6 млрд 171,2 млн кВт-год (+8%), будівельні – 1 млрд 64,2 млн кВт-год (+11, 2%).

Населення країни спожило 38 млрд 659,3 млн кВт-год (+5,8%), комунально-побутові споживачі – 15 млрд 23,6 млн кВт-год (+5,8%), інші непромислові споживачі – 8,599 млрд кВт-год (+16,5%). Частка промисловості у загальному обсязі споживання електроенергії за підсумками 2021 року знизилася до 41,7% із 41,8%, а частка населення – до 30,8% із 31%.

Енергетика України перебуває в стані війни з 2014 року, тому з 24-го лютого 2022 року з повномасштабним вторгненням на територію України певні рішення були вже відпрацьовані на територіях України, де раніше велися активні бойові дії та тимчасово окупованих територіях. В той же час, українська енергетика зустрілася з переліком нових, ще більш загрозливих викликів, як то ядерний тероризм із захопленням Запорізької АЕС, численні пошкодження критичної інфраструктури — електричних і газових мереж, критичне зниження попиту на енергетичні продукти у зв'язку з виїздом населення і припиненням бізнесу, ще більш критичне зниження рівня оплат в енергетичній системі, та рішення не дивлячись на бойові дії по всій території країни продовжувати синхронізацію енергетичної системи України з енергосистемою Континентальної Європи, паливна криза та ін. [2]

У сфері енергетики з 24-го лютого 2022 року було запроваджено ряд регуляторних змін, покликаних стабілізувати галузь та вирішити критичні проблеми. З початку повномасштабного вторгнення в Україні є зруйнованими та окупованими 42% генеруючих потужностей енергосистеми. Найбільшим окупованим об'єктом є Запорізька АЕС (6 ГВт), а найсуттєвіших втрат зазнала теплогенерація, в структурі якої 87% вугільних ТЕЦ є безповоротно втраченими. Руйнації та пошкодження зазнали 2,3 тисячі МВт потужностей гідрогенерації.

Якщо територіально аналізувати зони пошкодження, то найбільших втрат зазнали генеруючі потужності регіонів, наближених до зони бойових дій, що до обстрілів енергосистеми були енергетично профіцитними, а наразі мають дефіцит електричної енергії. Також, є руйнування великих генеруючих об'єктів у глибокому тилу, зокрема — на Прикарпатті та Поділлі.

В енергетичній системі, основа якої була побудована у радянській період працює два основні принципи: генерація електроенергії на потужних атомних електростанціях (які дають рівний графік на базі денного споживання на рівні 7,78 ГВт годин, а балансуються, покриваючи ранкові та

вечірні піки тепловою та гідроенергетикою), її передача лініями НЕК «Укренерго» від об'єктів генерації до обленерго, окремого у кожній області.

Зокрема, із встановлених потужностей теплової генерації 30,545 ГВт, в роботі (із частковим пошкодженням) залишилось 7,96 МВт. Враховуючи низький рівень ККД (на рівні 29-31%) дозволяє при максимальному завантаженні згенерувати 2,3-2,4 ГВт години.

Обстріли призвели до пошкодження й гідроенергетики. Так, із 6,64 ГВт потужностей ГЕС та ГАЕС, безповоротно зруйновано 351 МВт (підірвана півтора роки тому гідроспоруда Каховської ГЕС), а видача у мережу здійснюється на рівні 2,17 ГВт годин, за умови високого рівня водності річок. Наразі цей показник є на рівні 1,2 ГВт годин через період осінньої межені (найнижчий рівень річок) та посушливе (маловодне) літо.

Руйнування зазнали й потужності «зеленої» генерації. Так, із 6,23 ГВт введених в експлуатацію промислових сонячних електростанцій на тимчасово окупованих територіях знаходиться 3,72 ГВт (60% СЕС), пошкодженими є 1,12 ГВт у прифронтових регіонах на ТОТ. Сумарно, у пік вони можуть видати у енергомережу до 2,2 ГВт годин, а в зимовий час до 502 МВт годин вдень.

В Україні загальна потужність встановлених вітроелектростанцій становить 1,9 ГВт. Великі вітропарки в Україні зосереджені у Запорізькій, Миколаївській, Одеській та Львівській областях. За даними Української вітроенергетичної асоціації в Україні зупинено понад 2/3 вітрогенераторів через військову агресію росії. Наразі не працює 1162,5 МВт встановлених потужностей, залишаються у роботі 372,5 МВт, що зосереджені, переважно, у Одеській та Львівській областях. За даними Української вітроенергетичної асоціації на тимчасово окупованих територіях знаходиться 71% генерації. Також, постійного руйнування зазнають елементи магістральних електромереж та підстанції НЕК «Укренерго».

З початку повномасштабного вторгнення та масованих обстрілів об'єктів інфраструктури основний акцент спрямований в бік вирішення нагальних питань для уникнення загрози зупинки обладнання, наслідком чого можуть бути блекаути. У сфері енергетики наявна значна кількість критичних активів, якими необхідно управляти ефективно, зокрема, планувати і вчасно виконувати технічне обслуговування та ремонти, щоб зменшити незаплановані простої та збільшити доступність обладнання. Потрясіння спричинені війною в Україні показали, як автоматизація процесів управління активами допомагає оперативно реагувати на аварії та забезпечувати стабільність енергетичної системи.

[1] Виробництво електроенергії в Україні у 2021 році. Режим доступа. https://vse.energy/news/pek-news/electro/1935-power-generation-202112.

[2] Ігнатьєв С. Енергетична система України: стан на кінець 2024 року та сценарії на 2025. https://oil-gas.com.ua/statti/enerhetychna_systema_ukrainy_stan_na_kinets_2024_roku_ta_stsenarii_na_2025

О.С. Георгадзе

СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ

Система підтримки прийняття рішень (СППР) — це комплекс інформаційних та аналітичних інструментів, які призначені для збору, обробки, аналізу та подання інформації, необхідної для прийняття найкращих рішень в умовах невизначеності, важливості та обмежень.

Для сучасного етапу розвитку суспільства характерний неперервний процес інформатизації і вдосконалення інформаційних технологій. Середовище впровадження телекомунікаційної і обчислювальних систем постійно розширюється, залучаючи усе нові сторони життя суспільства. У зв'язку з цим важливою задачею є забезпечення достатньої міри захищеності цих систем для їх ефективного функціонування в умовах прояву інформаційних загроз, для чого необхідно наявність адекватного методологічного аналізу і управління інформаційними ризиками.

У сучасному воєнному конфлікті, де стратегічні рішення можуть визначити кінцевий результат, важливим є використання передових технологій для прийняття обдуманих та стратегічно обґрунтованих рішень [1]. Збройні Сили України постійно стикаються з низкою складних завдань та викликів, пов'язаних з забезпеченням національної безпеки та оборони. У таких ситуаціях рішення, прийняті командуванням та військовими лідерами, мають критичне значення для успішного виконання завдань та досягнення стратегічних цілей. Однією з ключових компонентів ефективної системи управління в Збройних Силах України є СППР.

1. Підвищення швидкості реагування. У воєнних операціях час — це часто критичний ресурс. СППР дозволяє оперативно збирати, аналізувати та обробляти дані, що допомагає командувачам приймати швидкі та обґрунтовані рішення.

2. Підвищення точності рішень. СППР використовує аналітичні моделі та сучасні технології для обробки інформації, що дозволяє уникати помилок, які можуть мати фатальні наслідки.

3. Підвищення ефективності використання ресурсів. Збройні Сили мають обмежені ресурси, і важливо їх використовувати максимально ефективно. СППР допомагає оптимізувати використання військового персоналу, техніки та зброї. Військові конфлікти часто мають непередбачувані обставини.

4. Підвищення стійкості та адаптивності. СППР допомагає армії бути готовою до різних сценаріїв і адаптуватися до змінних умов.

5. Покращення комунікації та співпраці. СППР сприяє обміну інформацією між різними рівнями командування та військовими підрозділами, що підвищує співпрацю та координацію дій.

6. Навчання та підготовка персоналу. Військові лідери та оператори системи повинні бути наділені необхідними навичками та знаннями для

користування СППР.

7. Забезпечення кібербезпеки. Системи СППР мають бути захищені від кіберзагроз, оскільки їхнє порушення може призвести до серйозних наслідків.

8. Збір та обробка великих обсягів інформації. СППР вимагає потужних обчислювальних ресурсів та здатності обробляти великі обсяги даних.

9. Постійне вдосконалення. Технології швидко розвиваються, і СППР мають оновлюватися та адаптуватися до нових викликів та можливостей.

Системи підтримки прийняття рішень є необхідним інструментом для модернізації військового управління. Вони допомагають зробити рішення більш обдуманими та раціональними, що має визначальне значення для успіху національних оборонних стратегій [2].

Система підтримки прийняття рішень є важливим інструментом для ЗСУ в умовах сучасних геополітичних викликів. Вона допомагає підвищити ефективність та точність рішень, що може вирішально вплинути на успіх воєнних операцій. Проте важливо розуміти, що СППР — це не панацея, і вона має використовуватися разом із досвідом, інтуїцією та стратегічним мисленням військових лідерів. ЗСУ повинні продовжувати вдосконалення своєї СППР, щоб залишатися готовими до викликів сучасного світу. Автоматизація процесів підтримки прийняття рішень зумовило появу кількох підходів до побудови СППР. Системи СППР ґрунтуються на застосуванні сучасних математичних методів прийняття рішень, різноманітних математичних моделях, технічних і програмних засобах. Тому визначення поняття систем підтримки прийняття рішень часто пов’язують з цими методами, моделями, засобами.

СППР – комп’ютерна інформаційна система, яка використовується для підтримки різних видів діяльності під час прийняття рішень у ситуаціях, коли неможливо або небажано мати автоматичну систему, яка повністю виконує весь процес створення рішень у складних умовах. Використання «досвіду», дасть змогу порівняти експертну оцінку з вже прийнятими рішеннями, що отримали позитивну чи негативну оцінку. Таким чином, система підтримки прийняття рішень, вірогідно, зможе зменшити час на генерування рішення, а ввід додаткових релятивних критеріїв для перевірки вірогідності успіху, у випадку прийняття рішення на основі вже здобутих знань, підвищить ефективність [3].

[1] Системи підтримки прийняття рішень: важливість впровадження у структури Сил оборони України. Режим доступа: https://softline.org.ua/news/sistemi-pidtrimki-prijnatta-risen-vazlivist-vprovadzenna-u-strukturi-sil-oboroni-ukraini.html

[2] Система підтримки прийняття рішень: переваги для ЗСУ. Режим доступа: https://softline.org.ua/news/sistema-pidtrimki-prijnatta-risen-perevagi-dla-zsu.html

[3] П. І. Бідюк, О. Л. Тимощук, А. Є. Коваленко, Л. О. Коршевнюк Системи і методи підтримки прийняття рішень: підручник. Київ : КПІ ім. Ігоря Сікорського, 2022, 610 с.

Ю.Г. Сапсай, А.О. Запорожець

ВИМОГИ ДО ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНОЇ СИСТЕМИ МОНІТОРИНГУ ТЕХНІЧНОГО СТАНУ УСТАНОВОК ЗБЕРІГАННЯ ЕНЕРГІЇ

Сучасний світ стикається з викликами, пов'язаними з енергетичною безпекою та зміною клімату. Відновлювані джерела енергії (ВДЕ) набувають дедалі більшого значення, а установки зберігання енергії (УЗЕ) стають невід'ємною частиною сучасної енергетичної інфраструктури. Зростання потреб у стабільному постачанні електроенергії та збільшення виробництва ВДЕ спричиняє активний розвиток акумуляторних установок. За прогнозами Bloomberg New Energy Finance, глобальний ринок УЗЕ зросте до 137ГВт/442ГВт-год до 2030 року, що підкреслює їхню зростаючу важливість [1]. Проте із збільшенням їх потужності та експлуатаційного часу виникають нові виклики, пов’язані з безпекою роботи акумуляторних батарей. Однією з найважливіших проблем є перегрів батарей, яка може призвести до зниження їх характеристик, деградації компонентів, а в крайніх випадках – до самозаймання та вибуху. Саме тому розробка та впровадження ефективних систем діагностики технічного стану акумуляторних батарей є актуальним завданням для своєчасного виявлення потенційно небезпечних станів.

Аналіз статистики відмов та інцидентів, пов'язаних з експлуатацією акумуляторних батарей, свідчить про те, що значна частина з них спричинена саме підвищенням їх температури [2]. Перегрів може бути зумовлений різними чинниками, такими як: 1. Перезаряджання (надмірна напруга зарядки може призвести до виділення тепла та газів, що підвищує внутрішній тиск і температуру батареї); 2. Перерозряджання (розряд акумулятора нижче встановленого мінімального порогу може призвести до незворотних хімічних змін у матеріалах електродів, що при наступному заряді супроводжується підвищеним тепловиділенням); 3. Коротке замикання (внутрішні дефекти або зовнішні причини можуть спричинити коротке замикання, що супроводжується швидким зростанням температури).

Інформаційно-вимірювальні системи діагностики технічного стану акумуляторних батарей можуть допомогти запобігти вищезгаданим проблемам, забезпечуючи безперервний збір та аналіз важливих параметрів в реальному часі. Завдяки використанню IoT сенсорів, контролерів та програмного забезпечення, такі системи здатні:

1. Здійснювати моніторинг температури в різних точках акумуляторної батареї та своєчасно виявляти локальні перегріви; 2. Контролювати напругу та струм кожного акумулятора установки для виявлення відхилень та дисбалансу; 3. Вимірювати внутрішній опір акумуляторних батарей для оцінки їхнього технічного стану та прогнозування терміну служби; 4. Точно визначати стан заряду (SOC) та стан здоров’я (SOH) для оптимізації режимів роботи та запобігання глибокому розряду або перезаряду; 5. Надавати

оператору інформацію про поточний стан акумуляторної системи, потенційні ризики та рекомендації щодо їхнього усунення; 6. Інтегруватися з системами управління батареями (BMS) для автоматичного регулювання режимів роботи та вжиття запобіжних заходів у разі виявлення небезпечних ситуацій.

Таким чином впровадження інформаційно-вимірювальних систем діагностики технічного стану акумуляторних батарей є ефективним інструментом для підвищення безпеки УЗЕ. Завдяки безперервному моніторингу ключових параметрів, такі системи дозволяють своєчасно виявляти відхилення від нормальних режимів роботи, прогнозувати потенційні несправності та запобігати виникненню термічного розгойдування, займання або вибуху

[1] Global Energy Storage Market Records Biggest Jump Yet | BloombergNEF. BloombergNEF. URL: https://about.bnef.com/blog/global-energy-storage-market-records-biggest-jump-yet/.

[2] A review of lithium-ion battery safety concerns: The issues, strategies, and testing standards. ScienceDirect. URL: https://www.sciencedirect.com/science/article/pii/S2095495620307075.

О.А. Шемелюк

РОЗВИТОК ХМАРНИХ ОБЧИСЛЕНЬ В УКРАЇНІ: ПОТЕНЦІАЛ ТА ВИКЛИКИ ДЛЯ ЕНЕРГЕТИЧНОЇ ГАЛУЗІ

Дата центри - це спеціалізовані об'єкти, які забезпечують зберігання, обробку та розподіл великих обсягів даних. Вони відіграють ключову роль у забезпеченні високої доступності, ефективності та безпеки інформаційних ресурсів. Дата центри також можуть мати зони доступності (ЗД) – це ізольовані або відокремлені центри обробки даних, розташовані в певних регіонах, де створюються та працюють публічні хмарні сервіси. Хмарні обчислювальні компанії зазвичай мають кілька зон доступності. Це допомагає забезпечити хмарним клієнтам стабільне підключення до хмарного сервісу в географічній зоні доступності, яка знаходиться найближче до них.

Ізоляція та відстань між зонами доступності знижує ймовірність того, що більше однієї ЗД постраждає від несприятливих погодних умов, відключень електроенергії або інших стихійних лих у цьому географічному місці. Таким чином, навіть якщо одна ЗД вийде з ладу через стихійне лихо, решта ЗД продовжуватимуть підтримувати регіональні сервіси, забезпечувати обчислювальні та сховищі потужності, а також забезпечувати високу доступність для користувачів хмари. Водночас відстань між ЗД достатньо коротка, щоб забезпечити дуже низьку затримку в обох напрямках (зазвичай кілька мілісекунд) для будь-якої необхідної передачі даних.

На світовому ринку домінують такі компанії, як Amazon Web Services, Microsoft Azure та Google Cloud. В Україні ж активно розвиваються місцеві провайдери, такі GigaCloud, та Ukrtelecom, які пропонують хмарні рішення, адаптовані під місцеві потреби.

Для чого потрібні державні дата центри в Україні і які виклики вони ставлять для енергетичної галузі?

Перш за все в Україні дата центри сприяють цифровізації країни, забезпечуючи безпеку та надійність зберігання даних (наприклад реєстри даних якими оперує застосунок Дія). Згідно з законодавством, персональні дані громадян України мають зберігатися на території країни, що підкреслює важливість розвитку внутрішніх дата-центрів.

Також, у зв’язку зі збройною агресією РФ на Україну, виникає потреба в сильному ОПК, який потрібно розвивати задля захисту нашої держави. Так як в сучасній війні використовується штучний інтелект (ШІ) для управління дронами, ракетами тощо, ШІ потребує велику кількість пам’яті для зберігання даних та достатньо велику потужність процесорів для його навчання, тобто дата центри. Крім того, зберігання поточної обстановки на лінії бойового зіткнення, розташування ППО чи іншої вразливої інформації повинно бути лише в дата центрах на території держави, щоб унеможливити потрапляння її до ворога.

Викликом для енергетичної галузі в створенні дата центрів є забезпеченням їх безперебійним джерелом живлення, так як доступ до даних є критично важливим для військових і державних сервісів. Дата центри, які обслуговують великі обчислювальні потреби, такі як ті, що використовуються для військових симуляцій або обробки великих даних, можуть вимагати значної кількості енергії. Великі дата центри можуть споживати від 10 до 100 мегават електроенергії або більше. Ефективність дата центрів часто вимірюється показником PUE (Power Usage Effectiveness), який є відношенням загального споживання енергії дата центру до енергії, що використовується безпосередньо обладнанням для обчислень.

Особливо актуально, є вироблення електроенергії для дата центрів зараз, після того як Росія зруйнувала і пошкодила велику кількість енергетичних об'єктів в Україні. Вирішенням цієї проблеми, повинно бути побудова нових електростанцій, які повинні бути захищеними від зовнішніх чинників, для забезпечення електроенергією в пріоритеті дата центрів. Водночас, потрібно диверсифікувати джерела енергії, наприклад використання сонячної або ж вітряної енергії, задля зменшення залежності на певний тип електростанції.

Безумовно, для забезпечення безперебійної роботи та високої доступності, дата центри, особливо ті, що використовуються військовими, зазвичай обладнані різними резервними джерелами живлення: Дизельні генератори - забезпечують електроенергію у випадку відключення основного джерела. Безперебійні джерела живлення (UPS) - використовуються для миттєвого реагування на відключення електроенергії та забезпечення безперервної роботи критично важливого обладнання до запуску генераторів. Батареї - додаткове джерело живлення для підтримки систем у випадку збоїв. Ці системи резервного живлення розроблені таким чином, щоб забезпечити неперервність роботи дата центру навіть у випадку тривалих перебоїв у постачанні електроенергії. Але вони повинні застосовуватися лише у крайніх випадках.

Отже, створення державних дата центрів для забезпечення власних потреб, є необхідним кроком в подальшому розвитку цифрових і оборонних технологій в Україні. Це ставить виклик енергетичній галузі в забезпеченні дата центрів безперебійними джерелами живлення в якості побудови укріплених ТЕС, які будуть захищенні від ударів ракетами або стихійних лих, на додачу до цього - диверсифікація джерел електроенергії, а також використання резервних джерел живлення.

[1] IBM. Визначення поняття дата центрів і їх зон доступності. https://www.ibm.com/think/topics/data-centers

[2] Закон України №2297-VI про захист персональних даних https://www.president.gov.ua/documents/2297vi-11567

[3] DEVCOM. Аналітичний центр армії Сполучених Штатів Америки який використовує власний дата центр для власних потреб. https://dac.devcom.army.mil/

С.С. Шевченко

СИНХРОНІЗОВАНЕ КООПЕРАТИВНЕ НАВЧАННЯ ЯК ІНСТРУМЕНТ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ КОМАНДНОЇ РОБОТИ В ЕНЕРГЕТИЦІ

Сучасна енергетична галузь, особливо об'єкти критичної інфраструктури, характеризується високим рівнем складності технологічних процесів та підвищеними вимогами до безпеки. Ефективне функціонування таких систем значною мірою залежить не лише від індивідуальної кваліфікації персоналу, але й від злагодженості та ефективності командної роботи, особливо під час виконання складних операційних завдань чи реагування на нештатні та аварійні ситуації. Традиційні методи навчання та тренування персоналу часто зосереджені на розвитку індивідуальних навичок, приділяючи недостатньо уваги формуванню навичок кооперативної взаємодії в реальному часі.

Розвиток інформаційних технологій, зокрема інтерактивних автоматизованих навчально-тренувальних систем (АНТП) на базі 3D-середовищ, віртуальної (VR) та доповненої (AR) реальності, відкриває нові можливості для вирішення цієї проблеми [1, 2]. Такі системи є важливою ланкою у забезпеченні резильєнтності критичної інфраструктури через якісну підготовку персоналу [3]. Однак, багато існуючих АНТП все ще орієнтовані переважно на індивідуальне навчання. Для ефективної підготовки команд необхідно впроваджувати підходи, що моделюють спільну діяльність кількох фахівців.

Одним із таких підходів є **синхронізоване кооперативне навчання (СКН)** у віртуальному середовищі. СКН передбачає одночасну участь кількох користувачів у спільному віртуальному просторі, де вони взаємодіють між собою та з віртуальними об'єктами в режимі реального часу для досягнення спільної навчальної мети або вирішення поставленого завдання.

Ключові особливості та переваги СКН:

1. **Моделювання реальних командних завдань:** СКН дозволяє створювати сценарії, що точно імітують виробничі ситуації, які вимагають скоординованих дій кількох спеціалістів (наприклад, складний ремонт обладнання, спільне управління технологічним процесом, ліквідація аварії).
2. **Розвиток комунікативних навичок:** Учасники змушені активно спілкуватися та координувати свої дії для успішного виконання завдання, що сприяє розвитку навичок вербальної та невербальної комунікації в професійному контексті.
3. **Формування рольової взаємодії:** Можливість призначення різних ролей учасникам у межах сценарію дозволяє відпрацьовувати

специфічні обов'язки, взаємодію між різними позиціями та розуміння загальної структури командної роботи.

4. **Безпечне середовище для відпрацювання критичних ситуацій:** Віртуальне середовище дозволяє без ризику для персоналу та обладнання відпрацьовувати дії в умовах аварійних ситуацій, тестувати різні стратегії реагування та аналізувати наслідки помилок.
5. **Підвищення залученості та мотивації:** Інтерактивний та кооперативний характер навчання сприяє підвищенню залученості користувачів порівняно з пасивними методами навчання.
6. **Об'єктивна оцінка командної роботи:** Сучасні АНТП можуть фіксувати параметри взаємодії між учасниками (час реакції, послідовність дій, комунікаційні патерни), що дає можливість для подальшого аналізу та об'єктивної оцінки ефективності командної роботи.

Аспекти реалізації:

Впровадження СКН вимагає відповідної технологічної платформи, яка забезпечує:

- Стабільний мережевий зв'язок для синхронізації дій усіх учасників у реальному часі.
- Архітектуру "клієнт-сервер" або P2P для управління спільним віртуальним середовищем.
- Інструменти для взаємодії користувачів з віртуальним оточенням та між собою (наприклад, спільне маніпулювання об'єктами, інтегрований голосовий або текстовий чат).
- Підтримку багатокористувацьких сценаріїв та гнучкі інструменти для їх розробки.

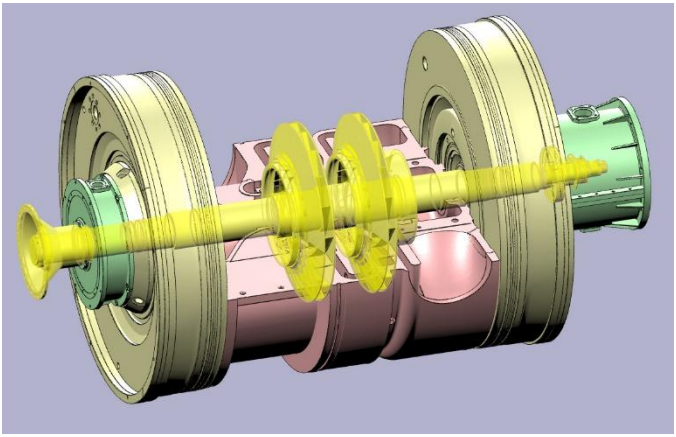


Рисунок 1 – Приклад роботи інтерактивної системи,
що може працювати у режимі СКН [2]

Прикладом технологічної основи для реалізації СКН можуть слугувати як спеціалізовані платформи, так і сучасні ігрові рушії (наприклад, Unreal Engine, Unity) або веб-технології (WebGL, WebXR) у поєднанні з відповідною серверною логікою [1, 2]. Приклад інтерактивної системи, яка розроблена автором і може працювати у режимі СКН, наведено на рис. 1.

Висновки

Синхронізоване кооперативне навчання у віртуальному середовищі є потужним інструментом для підготовки персоналу енергетичних підприємств до ефективної командної роботи. Воно дозволяє розвивати не лише технічні, але й комунікативні та координаційні навички, що є критично важливим для забезпечення надійності, безпеки та резильєнтності енергетичних систем [3]. Подальші дослідження можуть бути спрямовані на розробку методологій створення ефективних кооперативних сценаріїв, інтеграцію засобів автоматизованої оцінки командної ефективності та адаптацію СКН для різних типів завдань в енергетиці.

[1] Шевченко С.С. Вибір технологій для створення інтерактивних автоматизованих дистанційних навчально-тренувальних систем. // Науково-практична конференція «Технології створення і використання засобів підготовки персоналу на об’єктах критичної інфраструктури – 2023», 08 листопада 2023 року.

[2] Shevchenko S.S. Patent UA 149786 U, G09B 19/00, publ. 01.12.2021, Bull. No. 48

[3] Шевченко С.С. Інтерактивні автоматизовані дистанційні навчально-тренувальні системи як важлива ланка у резильєнтності критичної інфраструктури. // Науково-практична конференція «Резильєнтність критичної інфраструктури – 2023», 21 червня 2023 року.

І.М. Корнієнко, О.О. Кузнєцова, Л.С. Ястремська, М.М. Барановський

РЕЗИЛЬЄНТНІСТЬ ТА СТАЛИЙ РОЗВИТОК ЕНЕРГЕТИКИ ЗА ПРИНЦИПАМИ ЦИРКУЛЯРНОЇ БІОЕКОНОМІКИ В УКРАЇНІ ТА КРАЇНАХ ЄС

Європа перебуває на вирішальному етапі свого енергетичного майбутнього. Зіткнувшись із проблемами конкурентоспроможності, геополітичним тиском і необхідністю стратегічної автономії, Європейський союз намагається прискорити свою адаптацію, щоб забезпечити безпечну, стійку і конкурентоспроможну енергетичну систему. Виникають три основні осі: енергетична незалежність, технологічні інновації та інвестиції в інфраструктуру. Мета Європи щодо інновацій в енергетичній сфері полягає в упровадженнях технологій, які стосуються джерел відновлюваної енергії, використання яких до 2030 року повинно сягати 45% — це сонячна та вітрова енергія, а також, біоконверсія органічних відходів у водень або метан із використанням сучасних біотехнологій, котрі дозволяють вести технологічний процес за принципами циркулярної економіки.

Циркулярна економіка в технологічному процесі орієнтована на те, щоб продукти і матеріали використовувалися повторно, в безперервному циклі. Фонд Еллен Макартур був заснований 2010 року для прискорення переходу технологій до циклічної (циркулярної) економіки. У циклічній економіці продукти використовуються повторно. Продукти, які не можуть бути використані повторно, переробляються за допомогою хімічних та механічних процесів, або за допомогою біотехнологічних практик, таких як компостування, біоконверсія або біодеградація відходів — саме такі європейські підходи забезпечують сталий розвиток енергетики. Циркулярна біоекономіка — це економіка, що враховує принципи відновлення навколишнього природного середовища на шляху сучасного технологічного прогресу. Це нова економічна модель, яка підкреслює використання відновлюваного природного капіталу та зосереджується на мінімізації відходів, замінюючи широкий спектр невідновлюваних продуктів на основі різних видів палива на відновлювальні джерела енергії. Принципи циркулярної економіки [1-2] реалізуються через наукові підходи та технологічні інновації, що використовуються для створення більш стійких матеріалів та стимулювання регенерації — це економічна можливість для розширеного використання біопродуктів, які можуть в майбутньому не тільки доповнювати, але і замінювати традиційні джерела енергії (рис.1).

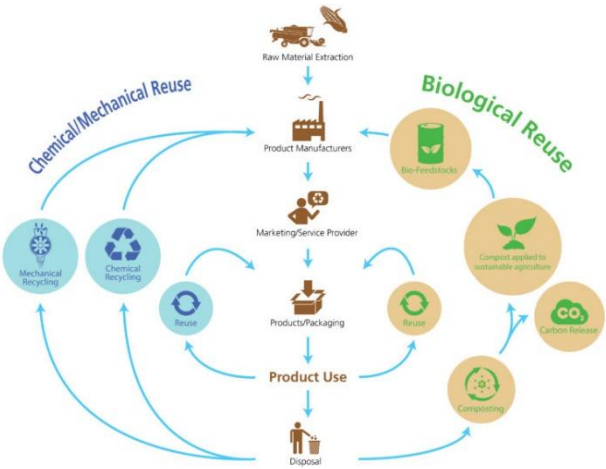


Рисунок 1 — Принципи циркулярної економіки [1]

Близько 34,2 млрд євро виділено країнами ЄС на підтримку більш швидкого розгортання відновлюваної енергетики з акцентом на використання біомас. 23 країни ЄС включили реформи з видачі дозволів на поновлювані джерела енергії, а 9 країн включили реформи з поліпшення нормативно-правової бази для роботи енергетичних співтовариств. Ці реформи відповідають рекомендаціям і вказівкам Комісії з видачі дозволів, ухваленим у травні 2024 року в рамках пакету «REPowerEU ».

Фонд відновлення та підвищення енергетичної стійкості в країнах ЄС (RRF) - це тимчасовий інструмент, запущений 2021 року, покликаний допомогти ЄС стати сильнішим і стійкішим задля підвищення стійкості національних економік. RRF є найбільшою програмою фінансування ЄС, на яку виділено загалом 648 млрд євро.

Усі країни ЄС мають виділити щонайменше 37% на заходи з підтримки зеленого переходу у своїх Планах відновлення та підвищення стійкості. Згідно звітності, всі країни перевищили цей показник, досягнувши в середньому 42% до травня 2024 року.

Фонд відновлення RRF підтримує виробництво і використання відновлюваного і низьковуглецевого водню (близько 13,6 млрд євро).Заходи включають підтримку ізольованих, самостійних систем виробництва і споживання водню («водневих долин») і зміцнення ланцюжка поставок, зокрема за допомогою пілотних проектів.

Циркулярну економіку важливо доповнити біоекономікою, а саме, концепцією, що може включати економічну діяльність, пов'язану з винаходом, розробкою, виробництвом і використанням біологічних продуктів або процесів для отримання енергії, матеріалів і хімікатів. Дане поєднання процесів можна назвати «круговою біоекономікою», тобто

терміни «циркулярна біоекономіка» і «стійкість» можна вважати синонімами.

З точки зору виробництва і споживання, циркулярна економіка визначається як «ініціатива сталого розвитку з метою скорочення лінійних матеріальних та енергетичних потоків суспільних систем виробництва і споживання шляхом застосування матеріальних циклів, поновлюваних і каскадних потоків енергії до лінійної системи. Вона просуває високоцінні матеріальні цикли поряд з більш традиційною переробкою, і розробляє системні підходи до співпраці виробників, споживачів та інших суспільних суб'єктів у роботі зі сталого розвитку.

У рамках цих визначень можна прийти до висновку, що біоекономіка пов'язана з використанням поновлюваних біологічних ресурсів, таких як біомаса, для виробництва поновлюваного біопалива, біопродуктів і біоенергії для економічних, екологічних і соціальних вигод. В сучасному світі біопродукти вважаються поновлюваними і потенційно чинять менший вплив на навколишнє середовище порівняно з їхніми аналогами, отриманими з нафти. Біопродукти замінюють викопний вуглець біогенним вуглецем, отриманим із біомаси, а їхні викиди вуглекислого газу (CO_2) наприкінці терміну служби являють собою біогенний CO_2, який вважається вуглецево-нейтральним. Крім того, при використанні у якості джерела енергії біопалива, біоенергія є відновлюваною енергією, яка може замінити викопне паливо та електроенергію для пом'якшення виснаження викопних ресурсів [2-3].

Щодо плану дій з боку України відносно цього питання: Міненерго активно працює над поліпшенням позицій щодо біогазових технологій та ринків біометану. Наголошено, що наразі реалізуються спільні ініціативи з ЄС щодо експорту біометану. Також наразі розробляється дорожня карта спільно з Європейською комісією. Міністерство працює над створенням фундаментальної правової бази для експорту біометану в ЄС.

Експерти та члени правління Bioenergy Europe зауважують, що ринок виробництва біометану в Європі переживає суттєве глобальне зростання. Також, відзначається прорив України в цьому питанні, оскільки станом на зараз в Україні вже працює 83 біогазові заводи з потужністю 140 МВт [4]. Експерти зазначають, що найближчим часом планується запуск семи українських біометанових заводів загальною потужністю 111 млн куб. м на рік. Голова правління наголошує, що сировинна база на Україні для виробництва біометану та біогазу велика, серед основних джерел: промислове тваринництво, промислове рослинництво, виробництво продуктів харчування/кормів для тварин/напоїв, а також послідовне землеробство. Розрахунками встановлено, що рентабельність біометанових проєктів із внутрішньою нормою прибутковості становить до 28,4% для підприємств, під'єднаних до газорозподільної мережі (ГРМ), і 25,7% - для газотранспортної системи (ГТС). Базове законодавство України у сфері біометану повністю готове до впровадження.

Отже, враховуючи позитивний досвід країн ЄС щодо принцип циркуляності відходів, Україна має усі можливості щодо сталого розвитку енергетики найближчим часом, оскільки циркулярну біоекономіку слід розглядати як нову концепцію, котра має на меті вирішити проблеми сталого розвитку. Циркулярна біоекономіка - це не просто прийняття принципів циклічності, таких як каскадування біомаси (тобто використання матеріалів у різних сферах після завершення їхнього життєвого циклу в різних потоках – це ієрархія відходів та ефективність використання біомаси або відновлюваних ресурсів (тобто отримання максимальної практичної користі від продуктів та утворення мінімальної кількості відходів). Також, циркулярна біоекономіка насправді є чимось більшим, ніж просто біоекономіка, або економіка замкненого циклу, тому що існування циркулярної біоекономіки має сенс лише тоді, коли ці дві концепції доповнюють одна одну.

Дана тематика вивчається в рамках діючого гранту Жана Моне: Waste Management in the Context of Transition to a Circular Economy: the EU Experience (101172378 — CIRCLEMAN — ERASMUS-JMO-2024-HEI-TCH-RSCH)).

Co-funded by the European Union

Фінансується Європейським Союзом. Однак висловлені думки та погляди належать лише авторам і не обов'язково передають погляди Європейського Союзу або Європейського виконавчого агентства з питань освіти та культури. Ні Європейський Союз, ні орган, що надає грант, не можуть нести за них відповідальність.

[1] Ensuring Resilient and Sustainable Energy Security in Europe (2024, 25 March). https://www.europeanfiles.eu/magazine/ensuring-resilient-and-sustainable-energy-security-in-europe

[2] Kardung, M., Cingiz, K., Costenoble, O., Delahaye, R., Heijman, W., Lovrić, M., et al. (2021). Development of the circular bioeconomy: drivers and indicators. Sustainability 13:413. doi: 10.3390/su13010413

[3] Leipold, S., and Petit-Boix, A. (2018). The circular economy and the bio-based sector–perspectives of european and german stakeholders. J. Clean. Prod. 201, 1125–1137. doi: 10.1016/j.jclepro.2018.08.019

[4] Георгій Гелетуха: до 2050 року Україна може виробляти 20 млрд кубів біометану в рік і перетворитися в потужного енергоекспортера.(2023, 07 лютого). https://uspp.ua/news/novyny-hromadskykh-partneriv/2018/heorhii-heletukha-do-2050-roku-ukraina-mozhe-vyrobliaty-20-mlrd-kubiv-biometanu-v-rik-i-peretvorytysia-v-potuzhnoho-enerhoeksportera

А.В. Ониськова

ОСОБЛИВОСТІ ВСТУПУ НА НАВЧАННЯ ДЛЯ ЗДОБУТТЯ СТУПЕНЯ ДОКТОРА ФІЛОСОФІЇ В 2025 РОЦІ

Порядок організації та проведення в 2025 році вступних випробувань визначає процедуру організації та проведення вступних випробувань у формі комп'ютерного тестування з використанням організаційно-технологічних процесів здійснення зовнішнього незалежного оцінювання для вступу на навчання для здобуття ступеня доктора філософії. [1]

Порядком прийому на навчання для здобуття вищої освіти в 2025 році [2] визначено, що вступники на навчання для здобуття ступеня доктора філософії складатимуть єдиний вступний іспит (ЄВІ), а також проходитимуть єдине вступне випробування з методології наукових досліджень (ЄВВ).

ЄВІ – форма вступного випробування для вступу на навчання для здобуття ступеня доктора філософії, яка поєднує тест загальної навчальної компетентності (ТЗНК) і тест з іноземної мови *(англійської, німецької, французької або іспанської на вибір вступника).*

ЄВВ – форма вступного випробування для вступу на навчання для здобуття ступеня доктора філософії, яка передбачає оцінювання рівня підготовленості вступника до здобуття третього рівня вищої освіти.

Український центр оцінювання якості освіти [3] затвердив загальні характеристики тестів ЄВІ [4], якими визначено кількість завдань у кожному тесті, їх форми, час, відведений на їх виконання, схеми нарахування балів.

Завдання ТЗНК буде укладено відповідно до Програми тесту загальної навчальної компетентності [5], **з іноземних мов** – до Програми єдиного вступного іспиту з іноземних мов [6].

Блок ТЗНК складатиметься з двох компонентів: вербально-комунікативного й логіко-аналітичного.

Тест міститиме 27 завдань двох форм. На проходження тесту буде відведено орієнтовно 75 хвилин. Максимальна кількість балів, яку можна набрати, правильно виконавши всі завдання тесту, – 33 бали: 10 балів за виконання завдань 1–4 (підзавдань 1–10) і 23 бали за виконання завдань 5–27.

Блок з іноземної мови *(англійської, німецької, французької або іспанської на вибір вступника)* складатиметься з двох частин: читання і використання мови.

Тест міститиме 30 запитань трьох форм. На виконання завдань тесту буде відведено орієнтовно 45 хвилин. За виконання завдань блоку з іноземної мови можна отримати від 0 до 30 балів.

Свої результати (тобто кількість набраних тестових балів за правильно виконані завдання) учасники тестування будуть знати після завершення роботи над тестами ЄВІ. За таблицею переведення тестових балів результат

кожного блоку буде переведено в рейтингову оцінку за шкалою 100–200 балів. [7]

Цьогоріч уперше для вступу на навчання для здобуття ступеня доктора філософії потрібні результати **єдиного вступного випробування з методології наукових досліджень (ЄВВ)**, яке передбачає оцінювання рівня підготовленості вступника до здобуття третього рівня вищої освіти з використанням організаційно-технологічних процесів здійснення зовнішнього незалежного оцінювання.

Розроблення програми ЄВВ, організацію укладення тестових завдань ЄВВ та підготовлення їх наборів забезпечує Науково-методичний центр ВФПО. [8]

Наразі Міністерство освіти і науки України запропонувало до громадського обговорення проєкт програми ЄВВ. Ознайомитися з ним можна за посиланням. [9]

Наказом Міністерства освіти і науки України від 25 березня 2025 року № 501 затверджено календарний план організації та проведення ЄВІ / ЄВВ для вступу на навчання для здобуття ступеня доктора філософії.

Основний етап реєстрації для участі в ЄВІ / ЄВВ триватиме **із 02 до 23 травня включно.** Реєстрацію здійснюватимуть приймальні комісії закладів вищої освіти. Зареєстровані учасники отримають екзаменаційні листки, у яких буде зазначено дані для здійснення входу на їхні інформаційні сторінки «Кабінет учасника вступних випробувань до аспірантури». У додатковий період (**16–17 червня**) матимуть змогу зареєструватися для складання ЄВІ / проходження ЄВВ ті особи, які не змогли цього зробити під час основного періоду реєстрації.

ЄВІ / ЄВВ проходитиме **у дві сесії:**

- основна: 07– 28 липня;
- додаткова: 18–28 серпня 2025 року.

До 12 червня учасники, зареєстровані на основну сесію ЄВІ / ЄВВ, отримають на своїх інформаційних сторінках «Кабінет учасника вступних випробувань до аспірантури» запрошення-перепустки, де буде зазначено дату, час і місце проведення тестування, а до **14 серпня** – учасники додаткової сесії.

Оголошення результатів основної сесії вступних випробувань відбудеться до **08 серпня**, а додаткової – до **03 вересня 2025 року**.

Календарним планом організації та проведення ЄВІ / ЄВВ для вступу на навчання для здобуття ступеня доктора філософії передбачено два періоди реєстрації:

основний — 2–23 травня (для участі в основній сесії);

додатковий — 16–17 червня (для участі в додатковій сесії — у цей період матимуть змогу зареєструватися ті, хто не зміг цього зробити під час основного періоду реєстрації).

Реєстрацію осіб, які бажають узяти участь у єдиному вступному випробуванні з методології наукових досліджень (ЄВВ) та/ єдиному

вступному іспиті (ЄВІ), здійснюють приймальні комісії закладів вищої освіти за умови особистої присутності вступника / вступниці та/або дистанційно.

Консультацію можна отримати електронною поштою або телефоном. Їх заклади вищої освіти розмістять на сторінках приймальних комісій на своїх офіційних вебсайтах.

Реєстрація відбуватиметься за допомогою взаємодії двох сервісів, роботу яких забезпечують Державне підприємство «Інфоресурс» та Український центр оцінювання якості освіти.

Рисунок 1 – Дати вступних іспитів в аспірантуру у 2025 році [10]

Для успішної **дистанційної реєстрації** необхідно діяти за таким алгоритмом:

1. **Сформувати комплект сканованих копій або фотокопій реєстраційних документів:**

- заповненої заяви-анкети [11] для оформлення екзаменаційного листка зі своїм накладеним кваліфікованим електронним підписом;
- документа, що посвідчує особу, зазначеного в анкеті-заяві;
- документа, що підтверджує інформацію про реєстраційний номер облікової картки платника податків (РНОКПП), або документа, що підтверджує причину невнесення до анкети-заяви інформації про РНОКПП;
- документа про здобутий ступінь вищої освіти магістра (освітньо-кваліфікаційний рівень спеціаліста) *(для осіб, які завершили навчання в минулі роки);*
- довідки щодо планового строку завершення навчання та отримання диплома магістра у відповідному році (для осіб, персональні дані яких не вносять до Єдиної державної бази з питань освіти);
- фотокартки для документів (кольорової або чорно-білої) із зображенням, що відповідає досягнутому віку вступника / вступниці.

Заповнюючи заяву-анкету з інформацією, необхідною для оформлення екзаменаційного листка, потенційні аспіранти мають указати населений пункт в *Україні* [12]*, у якому бажають взяти участь у ЄВВ та ЄВІ, назву іноземної мови, із якої хочуть скласти іспит в межах ЄВІ.*

Вступник / вступниця має право внести зміни до реєстраційних даних, здійснивши перереєстрацію протягом часу, відведеного для реєстрації.

Для перереєстрації учаснику / учасниці необхідно звернутися до приймальної комісії, яка його / її зареєструвала для участі у вступному випробуванні, і повернути раніше виданий екзаменаційний листок для його анулювання.

Якщо в процесі перереєстрації вступник / вступниця бажає змінити персональні дані ― він / вона має надати документ(-и), що підтверджує(-ють) зміну персональних даних.

2. **Надіслати на електронну адресу приймальної комісії скановані копії або фотокопії реєстраційних документів.**

Перш ніж надіслати лист, обов'язково потрібно перевірити правильність даних, зазначених у заяві-анкеті.

3. **Отримати скановану копію екзаменаційного листка.**

Представник приймальної комісії перевірить наявність необхідних для реєстрації документів та правильність їх оформлення.

У разі успішної реєстрації учаснику / учасниці буде надіслано скановану копію екзаменаційного листка на електронну адресу, зазначену ним / нею в заяві-анкеті. Оригінал екзаменаційного листка зберігатиметься в приймальній комісії. Якщо в екзаменаційному листку учасник / учасниця виявить помилки, йому / їй потрібно звернутися до приймальної комісії.

Оформлений оригінал екзаменаційного листка можна отримати особисто, звернувшись до приймальної комісії, або поштовим зв'язком, якщо учасник / учасниця зазначив / зазначила про таку необхідність у заяві-анкеті.

Якщо екзаменаційний листок не надійде на адресу, зазначену в заяві-анкеті, за два тижні до початку вступних випробувань ― учасник /

учасниця має звернутися до приймальної комісії, до якої надсилав / надсилала реєстраційні документи, для отримання відповідних роз'яснень.

Для зареєстрованих учасників / учасниць на вебсайті Українського центру оцінювання якості освіти створено інформаційну сторінку «Кабінет учасника вступних випробувань до аспірантури» [13], доступ до якої здійснюється за номером екзаменаційного листка та PIN-кодом, зазначеним у ньому.

ЄВІ / ЄВВ проводитимуть у пунктах тестування, створених у закладах освіти, де окремі класи / аудиторії будуть відповідним чином обладнані.

Після завершення виконання всіх завдань ЄВІ / ЄВВ кожен учасник отримає інформацію про кількість набраних тестових балів (за кожним блоком, якщо екзаменаційна робота поділена на блоки). Тестові бали переводять у рейтингові оцінки за шкалою 100–200 балів [14] за виконання завдань вступного випробування (певного блоку вступного випробування) лише тим вступникам, які подолали поріг «склав / не склав» (мінімальна рейтингова оцінка «100 балів» відповідає значенню порогового бала «склав / не склав»).

Офіційне оголошення результатів вступних випробувань здійснюють шляхом їх розміщення на інформаційних сторінках «Кабінет учасника вступних випробувань до аспірантури». Результати вступних випробувань у вигляді рейтингових оцінок за шкалою 100–200 балів зазначають в екзаменаційній картці, яку розміщують на інформаційній сторінці «Кабінет учасника вступних випробувань до аспірантури». Ця картка є додатком до екзаменаційного листка.

Результати вступних випробувань у вигляді рейтингових оцінок за шкалою 100–200 балів Український центр оцінювання якості освіти передає до ЄДЕБО наступного робочого дня після офіційного оголошення результатів.

[1] Порядок організації та проведення в 2025 році вступних випробувань, що проводяться з використанням організаційно-технологічних процесів здійснення зовнішнього незалежного оцінювання для вступу на навчання для здобуття ступеня доктора філософії, доктора мистецтва. - Наказ Міністерства освіти і науки України від 05.03.2025р., №410. https://zakon.rada.gov.ua/laws/show/z0434-25#Text

[2] Порядок прийому на навчання для здобуття вищої освіти в 2025 році. Наказ МОН України від 10.02.2025р., №168. https://mon.gov.ua/static-objects/mon/sites/1/vishcha-osvita/vstup-2025/03/03/poryadok-pryyomu-na-navchannya-dlya-zdobuttya-vyshchoyi-osvity-v-2025-rotsi-03-03-2025.pdf

[3] Український центр оцінювання якості освіти - https://testportal.gov.ua

[4] Загальні характеристики тестів ЄВІ. https://testportal.gov.ua/wp-content/uploads/2025/03/Nakaz-UTSOYAO-34-Zagalna-harakterystyka-YEVI_2025.pdf

[5] Програми тесту загальної навчальної компетентності. https://mon.gov.ua/storage/app/media/vishcha-osvita/vstup-2022/Prohramy-YEFVV/Zatverdzheni.prohramy.YEFVV/11.02/Pro.zatv.Prohr.predm.TZNK-nalaz-

158-11.02.2022.pdf
[6] Програми єдиного вступного іспиту з іноземних мов. https://testportal.gov.ua/wp-content/uploads/2019/03/nakaz-MON-vid-28.03.2019-411.pdf
[7] Таблиця переведення тестових балів результат кожного блоку буде переведено в рейтингову оцінку за шкалою 100–200 балів. https://ips.ligazakon.net/document/RE43718?an=3012
[8] Науково-методичний центр ВФПО. https://nmc-vfpo.com
[9] МОН пропонує до громадського обговорення проєкт програми ЄВВ з методології наукових досліджень для вступу на навчання для здобуття освітнього ступеня доктора філософії. https://mon.gov.ua/news/mon-proponuie-do-hromadskoho-obhovorennia-proiekt-prohramy-ievv-z-metodolohii-naukovykh-doslidzhen-dlia-vstupu-na-navchannia-dlia-zdobuttia-osvitnoho-stupenia-doktora-filosofii
[10] МОН назвало дати проведення вступних іспитів в аспірантуру. https://24tv.ua/education/vstup-aspiranturu-2025-koli-budut-vstupni-ispiti-dati_n2785052
[11] Заява-анкета. https://testportal.gov.ua/wp-content/uploads/2025/04/Zayava-anketa-YEVIYEVV_2025.pdf
[12] Про визначення переліку населених пунктів у 2025 році для проведення вступних випробувань. https://mon.gov.ua/npa/pro-vyznachennia-pereliku-naselenykh-punktiv-na-terytorii-iakykh-u-2025-rotsi-bude-stvoreno-punkty-provedennia-zovnishnoho-nezalezhnoho-otsiniuvannia-u-iakykh-provodiatsia-vstupni-vyprobuvann
[13] Кабінет учасника вступних випробувань до аспірантури. https://zno.testportal.com.ua/master/login
[14] Рейтингові оцінки за шкалою 100–200 балів. https://ips.ligazakon.net/document/RE43718?an=2909

В.О. Верпета, А.О. Запорожець

АДАПТИВНІ АЛГОРИТМИ ПРОГНОЗУ ВІТРОВОГО ПОТЕНЦІАЛУ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ВЕС

У сучасних умовах енергетичної трансформації та глобальних кліматичних змін Україна активно розвиває вітрову енергетику як один із ключових драйверів енергетичної безпеки та зниження викидів парникових газів [1]. Прогнозування швидкості вітру виступає фундаментальною складовою в операційній діяльності вітроелектростанцій (ВЕС), оскільки точність прогнозів безпосередньо впливає на балансування енергосистеми, планування технічного обслуговування та економічну ефективність генерації [2, 3]. З огляду на це комплексний аналіз існуючих підходів до прогнозування швидкості вітру дозволяє виявити їхні сильні й слабкі сторони та розробити рекомендації для підвищення надійності та точності прогнозних моделей.

Перш за все, фізичні (числові) методи прогнозування базуються на сполученні системи рівнянь Нав'є–Стокса з рівняннями збереження маси, енергії та імпульсу. Моделі WRF та ECMWF є найпоширенішими у світовій практиці й дозволяють отримати деталізовану картину атмосферної циркуляції на середньострокові горизонти (від кількох годин до кількох діб) шляхом розбиття обчислювальної області на тривимірну сітку [4-6]. Основною перевагою цих моделей є їхня фізична обґрунтованість: вони враховують такі процеси, як турбулентність, теплообмін і вплив рельєфу, що робить їх незамінними для масштабного прогнозування вітрового поля. Проте висока обчислювальна складність та залежність від якості вихідних метрологічних даних обмежують їхнє застосування в оперативному режимі без додаткової статистичної корекції [7,8].

Якщо фізичні моделі найкраще себе проявляють на середньо- та довгострокових горизонтах, статистичні підходи, зокрема моделі ARIMA, демонструють високу ефективність у короткостроковому прогнозі (до кількох годин). ARIMA-модель використовує лінійну комбінацію попередніх спостережень і ковзного середнього білого шуму, що дозволяє оператору швидко отримувати прогнози з невеликими обчислювальними витратами. Основний недолік ARIMA полягає у припущенні стаціонарності часових рядів і слабкій здатності моделі реагувати на різкі нелінійні зміни, такі як шторми або фронтальні проходи. Це спонукає фахівців обирати модифікації SARIMA або ARIMAX, а також поєднувати статистику з фізичним моделюванням для корекції систематичних похибок [9].

У рамках машинного навчання найбільшу популярність здобули рекурентні нейронні мережі, зокрема архітектура LSTM, здатна «пам'ятати» довготривалі залежності та виявляти складні нелінійні патерни у часових рядах вітру. LSTM-мережі успішно інтегрують вхідні ознаки з декількох джерел (швидкість вітру, температура, тиск тощо) та демонструють найкращі результати при високій частоті оновлення даних (сотні метрів та секунди-

минутний інтервал) [9, 10]. Однак для навчання таких мереж необхідні великі обсяги історичних даних і значні обчислювальні ресурси, а сам процес може виступати «чорною скринькою» без чіткої інтерпретації внутрішньої логіки прогнозу .

З огляду на обмеження окремих підходів, найбільш перспективними вважаються гібридні (ансамблеві) методи, які поєднують результати фізичних моделей із коригувальними блоками ARIMA або нейронними мережами. Така схема передбачає спочатку генерацію базового прогнозу за допомогою NWP-моделі, а потім адаптацію цього прогнозу на основі фактичних даних із локальних метеорологічних сенсорів. Вагові коефіцієнти при цьому обираються експериментально або автоматизовано (наприклад, за алгоритмом байєсівського зважування чи генетичного алгоритму), що дозволяє мінімізувати середньоквадратичну помилку та підвищити стабільність результатів у різних режимах роботи ВЕС [11].

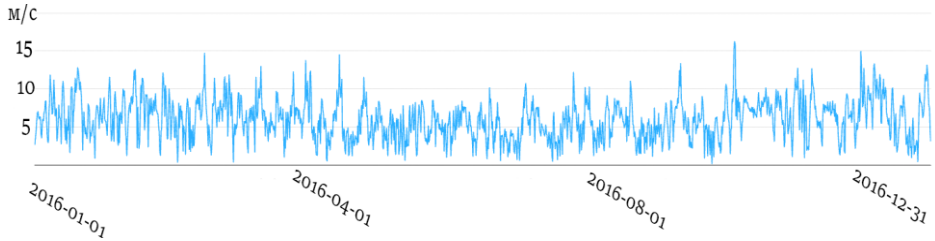


Рисунок 1 – Графік швидкості вітру протягом 2016 року на висоті 50 метрів над землею

Як приклад застосування на практиці, проведено аналіз даних швидкості вітру в Миколаївській області за 2016 рік на висоті 50 м над рівнем землі. Дані отримано з проєкту NASA POWER, що є відкритим джерелом супутникових та модельних метеорологічних параметрів. Для виявлення сезонних та добових закономірностей застосовано часові ряди зі згладжуванням та фільтрацією вхідних даних. Встановлено, що пікові зміни швидкості вітру повторюються з періодичністю 6–8 діб, особливо інтенсивні навесні та восени, у міжсезоння, тоді як зимовий та літній сезони характеризуються більш спокійними умовами з інтервалом коливань від 0 до 13–17 м/с .

Отримані результати свідчать про необхідність розробки адаптивних моделей прогнозу, які враховують регіональні особливості вітрового режиму. Зокрема, для міжсезонних місяців рекомендується застосовувати комбіновані підходи з акцентом на алгоритми машинного навчання для корекції систематичних похибок фізичних моделей. У той же час для стабільних періодів року достатньо модернізованих ARIMA-моделей із сезонними компонентами та фільтраційними алгоритмами, що забезпечить оперативність розрахунків і мінімальні обчислювальні ресурси.

[1] Нам'ясенко, В. (2024). Огляд пріоритетних напрямків повоєнного розвитку економіки України. Наукові перспективи (Naukovì perspektivi), (10), 52. http://dx.doi.org/10.52058/2708-7530-2024-10(52)-603-613
[2] Рябцев, Г., & Омельченко, В. (2024). Огляд роботи енергетичного сектору у вересні 2024 р.: жовтень 2024.
[3] Оберемок, Д. О. та ін. (2024). Аналіз стану електричних мереж та огляд сучасних проблем. Перспективи інтеграції сонячних електростанцій та систем зберігання енергії.
[4] Pape, M., & Kazerani, M. (2020). Turbine startup and shutdown in wind farms featuring partial power processing converters. IEEE Open Access Journal of Power and Energy, 7, 254–264. https://doi.org/10.1109/OAJPE.2020.3006352
[5] Hoksbergen, N., Akkerman, R., & Baran, I. (2022). The Springer model for lifetime prediction of wind turbine blade leading edge protection systems: A review and sensitivity study. Materials, 15(3), 1170. https://doi.org/10.3390/ma15031170
[6] Venkatramakrishnan, R. та ін. (2020). Low speed wind turbines for power generation: A review. https://doi.org/10.56532/mjsat.v4i3.352
[7] Babak, V. P. та ін. (2021). Models and Measures in Measurements and Monitoring. Springer International Publishing. https://doi.org/10.1007/978-3-030-70783-5
[8] Babak, V. P. та ін. (2021). Problems and features of measurements. Studies in Systems, Decision and Control, 360, 1–31. https://doi.org/10.1007/978-3-030-72361-3_1
[9] Application of material measure in measurements: Theoretical aspects. http://dx.doi.org/10.1007/978-3-030-69189-9_15
[10] Babak, V., Zaporozhets, A., Kuts, Y., Scherbak, L., & Eremenko, V. (2021). Studies in Systems, Decision and Control, 346, 261–269. https://doi.org/10.1007/978-3-030-69189-9_15
[11] Manwell, J. F., McGowan, J. G., & Rogers, A. L. (2010). Wind Energy Explained: Theory, Design and Application. John Wiley & Sons. http://dx.doi.org/10.1002/9781119994367

І.Е. Фуртат, Ю.О. Фуртат

INFLUENCE OF THE CHARGED LAYER ON THE MASS TRANSFER BETWEEN TWO ENVIRONMENTS

The influence of charged double layer (DL) on the processes occurring in biporous media, (for example, threads or fibers), is twofold: firstly, the effect on the kinetics of adsorption by a single inclusion and, secondly, the effect on the transport of ions in the space between inclusions. The repulsion of like-charged ions diffusing to the surface by the electric field of the DL can lead to a decrease in the adsorption rate by many orders of magnitude. The effect of the DL on the transport of ions in the space between the inclusions depends on the thickness of the DL. We will consider the process of dyeing of fibers as a simple enough example of a mass transfer between two environments. We will consider the case when the DL is thin, i.e. $\chi R_b \gg 1$, because the case of a thick DL is unacceptable for dyeing processes (and in the majority of other situations) due to the sorption of ions at the mouth of the pore, i.e. at the surface of the thread.

If the DL is thin, then the electrostatic interaction is distributed only inside the double layer. Outside it, the transport of ions is carried out purely by diffusion. Since the DS of individual fibers do not overlap, then the influence of the electrostatic factor on the kinetics of the process can be taken into account using the results of considering the kinetics of adsorption by a single inclusion. In view of the micropore structure of the fiber, the Crank equipotential volume model is applicable to it , i.e. it is valid to apply the results of considering the kinetics of adsorption by a single grain adsorbing only by the outer surface with the introduction of corrections to the inclusion form.

We will consider the kinetics of adsorption by a cylindrical grain. we will carry out at the stage when the factor of electrostatic slowing down of adsorption is sufficiently pronounced, i.e. under the condition that with

$$zf \gg 1, \tag{1}$$

where: z is the valence of the sorbed ion; f is the dimensionless surface potential.

Considering the complexity of the solution of the problem in general form, the assumption is made that the initially existing DS, formed by monovalent non-sorbed ions, does not change its thickness upon the addition of an electrolyte containing a strongly adsorbed ion in a low concentration. Limiting the generality of the consideration by condition (1) allows us to consider that the rate of adsorption and, accordingly, the rate of change of potential are small, and, consequently, the diffusion of ions to the surface at each moment of time and the restructuring of the DS over time can be considered as quasi-stationary processes.

The resulting flow of ions to the lateral surface of a cylindrical grain per unit of its length can be written in two ways: as an electrodiffusion flow:

$$\frac{dQ}{d\tau} = 2\pi R_1 \frac{d\sigma}{d\tau} = zlJ \tag{2}$$

and as the difference of streams adsorption and desorption

$$\frac{dQ}{d\tau} = 2\pi R_1 zl\left(J_1 - J_2\right) = 2\pi R_1 ze\left[K_1 c\left(R_1,\tau\right) - K_2\Gamma\left(\tau\right)\right]. \qquad (3)$$

Here Q is the increase in adsorbed charge, R_1 is the radius of the cylinder, e is the electron charge, σ is the density superficial charge , J_1 and J_2 are the diffusion flows of adsorption and desorption, respectively, K_1 and K_2 are the coefficients of adsorption and desorption, respectively, $c\left(R_1,\tau\right)$ is the concentration of adsorbing ions in the solution at the surface, $\Gamma\left(\tau\right)$ – the concentration of adsorbed ions on the grain surface.

The value of J in (2), taking into account the influence of the electric field, is a diffusion flux obtained from the diffusion equation

$$J\left(\tau\right) = \frac{2\pi D\left[c_\infty - c\left(R,\tau\right)\exp\left(zf\right)\right]}{K\left(f\right)}, \qquad (4)$$

where: D is the diffusion coefficient, f is the dimensionless surface potential of the grain, $K\left(f\right)$ is the Fuchs electrostatic repulsion factor, defined as

$$K\left(f\right) = \int_{R_1}^{L} \frac{\exp\left(zf\right)}{\rho} d\rho \approx \ln\frac{L}{R_1} + \frac{2}{\chi R_1}\sum_{n=1}^{|z|}\frac{\exp\left(\frac{2n-1}{2}|f|\right)}{2n-1}, \qquad (5)$$

(L is the distance measured from the center of the grain and determines the thickness of the diffusion layer, beyond which the ion concentration is equal to c_∞). Expressions (1)-(5) thus make it possible to determine the value $\Gamma\left(\tau\right)$.

$$\frac{d\Gamma}{d\tau} = \frac{D}{R_1 K\left(f\right)}\frac{c_\infty - \Gamma\left(\tau\right)\frac{K_2}{K_1}\exp\left(zf\right)}{1 + \frac{D\exp\left(zf\right)}{R_1 K_2 K\left(f\right)}}. \qquad (6)$$

In the case of a sphere $K\left(f\right)$ it has the form

$$K\left(f\right) = \frac{2}{\chi R_1}\sum_{n=1}^{|z|}\frac{\exp\left(\frac{2n-1}{2}|f|\right)}{2n-1}, \qquad (7)$$

i.e. (5) differs from (7) only by the presence of the term $\ln(L/R_1)$ responsible for purely diffusion transfer outside the DL. However, in the approximation of sufficiently high potentials and not too thin a double layer, the first term of (5) becomes small compared to the second and can therefore be omitted. Thus, the geometry of the particle does not play a role in such an analysis, and, as a consequence, all the results obtained for a simpler case of a sphere can be transferred without changes to the case of a cylindrical grain.

S. Kulyk, A. Davydiuk

AI-DRIVEN DATA MIGRATION CONTROLLER FOR INFORMATION SECURITY

In the modern world, critical infrastructure objects (CIOs) play a key role in ensuring the functioning of society, the economy, and national security. Disruptions to the operation of such objects due to crisis events—cyberattacks, natural disasters, technological accidents, or military actions—can have catastrophic consequences. One of the vital measures to enhance the resilience of CIOs is the timely and secure migration of data to alternative computing environments, particularly cloud infrastructures. The example of Ukraine, especially under the conditions of full-scale invasion, highlights the urgent need for rapid data migration and large-scale backup. Such processes were not typical before and had not been sufficiently tested, increasing the risk of critical errors. According to the Law of Ukraine "On Cloud Services," public users of cloud services are allowed to procure cloud services and/or data center services from providers not included in the official list [1] until December 31, 2025 [2]. Moreover, the National Cybersecurity Coordination Center under the National Security and Defense Council [3] of Ukraine has defined to governmental bodies of ensuring the return of state data placed in foreign cloud services after the end of martial law [4]. This underscores the importance of developing effective migration and data recovery strategies for the post-crisis period.

While detailed statistics on unsuccessful migrations are limited, existing cases of data loss or corruption during emergency transfers confirm the necessity of implementing intelligent systems to manage these processes. Therefore, research into the automation and optimization of data migration for CIOs under crisis conditions is highly relevant.

In this context, the idea of automated management of the migration process through artificial intelligence (AI) technologies becomes particularly relevant. AI enables dynamic assessment of the situation, risk forecasting, and real-time decision optimization, thus significantly enhancing the resilience and security of critical systems during emergency conditions.

The migration of critical infrastructure data under crisis conditions constitutes a complex multi-criteria optimization task. For example, in January 2024, the Parkovy Data Center in Ukraine, which serves dozens of government agencies, suffered a major cyberattack. As a result, critical services such as Naftogaz, Ukrposhta, Ukrzaliznytsia, and the Shlyakh border crossing system were disrupted, with full data access only restored after 48 hours, exposing the vulnerability of even certified cloud solutions under crisis conditions [5]. Additionally, the April 2025 official incident report from Denovo data center revealed a large-scale power failure that affected the operation of multiple cloud services [6]. Although the company swiftly activated backup systems, the event highlighted how infrastructure-level outages, such as unstable power supply, can jeopardize critical

data migration and continuity, especially during emergency scenarios. Key objectives include minimizing downtime and data loss, confirmation confidentiality and integrity, and optimizing the use of limited computing and network resources [7]. Additional priorities involve ensuring critical service continuity, reducing energy consumption, and maintaining compliance with cybersecurity standards. Traditional migration methods lack the necessary flexibility and adaptability for dynamic crisis environments, emphasizing the need for AI-driven decision support systems capable of real-time risk assessment and strategy optimization. Currently, many migration processes rely heavily on human input, where calculations, planning, and decision-making consume valuable time and increase the risk of errors. In contrast, AI-driven systems can perform such tasks more quickly and accurately, providing real-time optimizations that are crucial in emergency conditions.

The application of artificial intelligence technologies to data migration processes for critical infrastructure under crisis conditions is driven by AI's ability to rapidly analyze large volumes of information, predict evolving situations, and make optimal decisions in real time. Global solutions such as Google Cloud Transfer Service [8], AWS DMS, IBM Resiliency Orchestration, and Microsoft Azure Site Recovery already demonstrate the efficiency of AI-driven systems in managing complex data migrations under high-risk or crisis scenarios. Unlike traditional rule-based algorithms, AI models can adapt to changing conditions by dynamically adjusting migration strategies based on resource availability, security threats, and data prioritization. Examples of AI deployment in modern computing systems, such as AI-enhanced processors for personal computers, demonstrate the effectiveness of such approaches for dynamic resource management, supporting their extension to the domain of crisis-driven data migration in cloud environments [9].

Considering the previously identified risks of the migration process [10], and the critical need to provide a reliable sensory basis for AI systems, there is a clear rationale for the development and implementation of such a migration controller. Many of the current challenges, including lack of time, limited logistical resources, equipment compatibility issues, and unpredictable crisis scenarios, demand a system that can operate faster, more precisely, and with minimal human intervention. The AI-driven controller is thus positioned as a key innovation to address these challenges effectively.

The concept of an AI-based migration controller envisions the development of a specialized system capable of autonomously managing the data migration process for critical infrastructure objects under crisis conditions. This controller should be built on a modular architecture comprising several key components (see Table 1) [11]:

Table 1 – Components of a modular architecture for AI-based controller

Module	Function Description
Monitoring Module	Responsible for collecting data on network load, server status, cloud resource availability, and cybersecurity threats.
Prediction Module	Assesses the probability of adverse scenarios using machine learning models to anticipate risks and necessary adjustments.
Decision-Making Module	Develops optimal migration plans based on multi-criteria evaluation, including time, security, prioritization, and resource constraints.
Adaptation Module	Continuously adjusts the migration strategy in response to changes in the external environment, ensuring ongoing optimization.

The controller must operate in real time, ensuring dynamic optimization of the migration process with minimal human intervention. For the realization of such a controller, we propose to explore specific artificial intelligence methods such as reinforcement learning [12] and decision trees [13], which provide robust frameworks for adaptive decision-making under uncertainty. In particular, we consider implementing models like Deep Q-Networks (DQN), Long Short-Term Memory networks (LSTM), and Convolutional Neural Networks (CNN), each offering strengths in learning from sequences, patterns, and complex data representations. By employing these deep learning techniques and reinforcement learning approaches, the system will be able to improve its performance through experience, enhancing its effectiveness in handling recurring or novel crisis scenarios. Such an approach will contribute to maintaining the continuity of critical system operations, minimizing data loss, and provide the security and integrity of information during migration to alternative computing environments.

Thus, the development of an AI-based migration controller offers a promising approach to managing complex data migration processes under dynamic and uncertain crisis conditions. Its modular architecture, real-time operation, and ability to self-adapt provide the necessary foundation for achieving resilient, secure, and resource-efficient migration of critical infrastructure data. At different stages of the migration process, we have a set of practical controller benefits (see Table 2).

Table 2 - The controller's practical advantages

Migration Phase	AI Controller Benefits
Planning	Optimizes migration strategy by analyzing risks, predicting resource needs, and generating contingency plans.
Data Transfer	Monitors real-time performance, adjusts transfer rates, reroutes flows dynamically, and detects anomalies.
Post-Transfer Testing	Automatically validates data integrity, checks service functionality, and identifies configuration issues.
Optimization & Tuning	Learns from migration outcomes, updates models, and improves future performance through reinforcement learning.

This structured overview highlights how the AI-based controller adds value across all critical phases, not only accelerating operations but also increasing precision and resilience.

Overall, the controller will act not only as an intelligent orchestrator of migration tasks but also as a strategic asset for ensuring the operational continuity and cybersecurity of critical infrastructure in time of crisis [14]. It is important to note, however, that in its early stages, the controller's autonomous decision-making carries certain risks, including the potential for erroneous decisions, vulnerability to data poisoning attacks, and challenges related to explainability and trust. Nevertheless, in crisis situations where human experts may not have enough time to respond or may be unavailable, such an autonomous system has a real chance to preserve critical data and protect vital services. It is important to note, however, that in its early stages, the controller's autonomous decision-making carries certain risks, including the potential for erroneous decisions, vulnerability to data poisoning attacks, and challenges related to explainability and trust. Nevertheless, in crisis situations where human experts may not have enough time to respond or may be unavailable, such an autonomous system has a real chance to preserve critical data and protect vital services.

The scientific interest of the proposed AI-based migration controller lies in the integration of real-time multi-criteria optimization, risk prediction, and adaptive decision-making into a unified system for managing critical data migration processes under crisis conditions. Existing analogues, such as IBM Resiliency Orchestration, AWS Elastic Disaster Recovery, and Azure Site Recovery, provide valuable tools but are largely built on static rule sets and predefined workflows, which limit their adaptability in highly dynamic, unforeseen situations. The proposed controller improves upon these analogues by introducing adaptive learning mechanisms (e.g., reinforcement learning) and combining models such as DQN, LSTM, and CNN, enabling the system to self-optimize in real time, continuously learn from evolving conditions, and provide decisions even when human intervention is impractical or unavailable. This integration represents a fundamentally new approach to ensuring both operational continuity and cybersecurity resilience for critical infrastructure systems during emergencies.

The development of an AI-based migration controller offers a new paradigm for managing the secure and resilient transfer of critical infrastructure data during crisis conditions. The proposed approach demonstrates the feasibility of integrating intelligent, adaptive, and proactive mechanisms into traditionally static migration processes, opening new opportunities for enhancing the stability and security of critical systems [15]. Building upon these foundations, future research directions can further expand the capabilities and application domains of such controllers.

Promising avenues for future work include extending the controller's functionality to support multi-cloud and hybrid-cloud migration scenarios, where dynamic resource allocation and cross-cloud security policies will be critical. Another important direction involves the integration of advanced threat detection and response modules, enabling the controller not only to optimize migration logistics but also to actively defend against cyber threats during critical transitions.

Furthermore, research into federated learning approaches [16] could allow controllers deployed across different infrastructures to collaboratively learn from distributed data while maintaining data privacy [17]. Finally, extensive real-world validation and the development of standardized evaluation benchmarks will be essential steps toward practical deployment in mission-critical environments.

[1] Cabinet of Ministers of Ukraine. (n.d.). Procedure for the provision of cloud services and/or data center services, related to the processing of state information resources or information with restricted access, the requirement for the protection of which is established by law. https://www.kmu.gov.ua/storage/app/uploads/public/67a/cce/a44/67accea44f17c113534567.pdf

[2] Cabinet of Ministers of Ukraine. (2025, February 11). Resolution No. 154 on certain issues of the provision and use of cloud services and/or data center services. https://www.kmu.gov.ua/npas/deiaki-pytannia-nadannia-ta-vykorystannia-khmarnykh-posluh-taabo-posluh-tsentru-obrobky-danykh-154-110225

[3] National Cybersecurity Coordination Center (NCSCC). (n.d.). Official website. https://www.ncscc.gov.ua/

[4] National Cybersecurity Coordination Center (NCSCC). (2024). The meeting of the national cybersecurity coordination body. LinkedIn. https://www.linkedin.com/posts/nataliya-tkachuk-2981b8196_the-meeting-of-the-national-cybersecurity-activity-7317812280866336768-GkeQ

[5] Forbes Ukraine. (2024, January 26). Cyberattack on Parkovy data center: The company promises to restore full access to data within 48 hours. https://forbes.ua/news/kiberataka-na-data-tsentr-parkoviy-kompaniya-obitsyae-vidnoviti-povniy-dostup-do-danikh-protyagom-48-godin-26012024-18812

[6] De Novo. (2025, April 26). Official report on the causes and resolution of the incident. https://denovo.ua/blog/official-report-on-the-incident-26-apr-2025

[7] Altahat, M. A., Daradkeh, T., & Agarwal, A. (2024). Optimized encryption-integrated strategy for containers scheduling and secure migration in multi-cloud data centers. IEEE Access, 1. https://doi.org/10.1109/access.2024.3386169

[8] Google Cloud. (n.d.). Storage Transfer Service: Transfer data quickly and securely between object and file storage across Google Cloud, Amazon, Azure, on-premises, and more. https://cloud.google.com/storage-transfer-service

[9] Maldonado Carrascosa, F. J., Seddiki, D., Jiménez Sánchez, A., García Galán, S., Valverde Ibáñez, M., & Marchewka, A. (2024). Multi-objective optimization of virtual machine migration among cloud data centers. Soft Computing. https://doi.org/10.1007/s00500-024-09950-2

[10] Davydiuk A., Kulyk S. Data center infrastructure in the context of national resilience. existing risks, solutions, and prospects. Матеріали науково-практичної конференції «Резильєнтність динамічних систем», Kyiv, 27 December 2024. P. 170–175.

[11] Harika, A., Balan, G., Thethi, H. P., Rana, A., Rajkumar, K. V., & Al-Allak, M. A. (2024). Harnessing the power of artificial intelligence for disaster response and crisis management. У 2024 International conference on communication, computer sciences and engineering (IC3SE). IEEE. https://doi.org/10.1109/ic3se62002.2024.10593506

[12] Reinforcement Learning: An Introduction. Richard S. Sutton and Andrew G. Barto. 2015. A Bradford Book. The MIT Press, Cambridge, Massachusetts, London, England. https://web.stanford.edu/class/psych209/Readings/SuttonBartoIPRLBook2ndEd.pdf

[13] Quinlan, J. R. (1986). Machine Learning, 1(1), 81–106. https://doi.org/10.1023/a:1022643204877

[14] Atharva Subandha, Sahil Pathan, Pratiksha Parkhe. AI-Driven optimization strategies in cloud computing: A comprehensive review. International Journal on Science and Technology, 16(2). https://doi.org/10.71097/ijsat.v16.i2.3426

[15] G. Glory, M. Vaidhegi (2025). AI-Powered Cloud Migration: Automating the Transition from On-Premises to Cloud Environments with Zero Downtime. International Journal of Innovative Research in Science Engineering and Technology (Ijirset) 14 (1):747-752. https://philpapers.org/rec/GGLACM

[16] Kairouz, P., McMahan, H. B., Avent, B., et al. (2021). Advances and Open Problems in Federated Learning. Foundations and Trends® in Machine Learning, 14(1–2), 1–210. https://doi.org/10.1561/2200000083

[17] Dr.A.Shaji George. Emerging Trends in AI-Driven Cybersecurity: An In-Depth Analysis. Partners Universal Innovative Research Publication (PUIRP), 02(04), 15-28, ISSN: 3048-586X, 2024. https://doi.org/10.5281/zenodo.13333202

Г.П. Костенко

ВТОРИННІ БАТАРЕЇ ЕЛЕКТРОТРАНСПОРТУ ЯК ОБ'ЄКТ МОДЕЛЮВАННЯ В СИСТЕМІ ФОРМУВАННЯ ПОЛІТИКИ ЦИРКУЛЯРНОЇ ЕНЕРГЕТИКИ

Виклики сучасної енергетики, пов'язані зі зростанням споживання енергії, розвитком відновлюваних джерел енергії (ВДЕ), необхідністю декарбонізації та забезпечення енергетичної безпеки, вимагають переосмислення не лише технологічних, а й управлінських парадигм. У цьому контексті циркулярна економіка поступово перетворюється з концептуальної рамки на інструмент реального регулювання ресурсних потоків і формування довгострокової політики. Одним із ключових напрямів циркулярної енергетики є оптимізація використання літій-іонних батарей (ЛІБ), зокрема їх повторне використання після завершення ресурсу в транспорті.

Вторинні батареї елктротранспорту, Second-Life Batteries (SLB) — це відпрацьовані тягові батареї, які, хоча й не відповідають вимогам автомобільної індустрії, зберігають значну залишкову ємність і можуть бути застосовані в менш критичних стаціонарних сферах. Їх потенціал охоплює підтримку ВДЕ, балансування навантажень, резервне живлення, зменшення пікових навантажень тощо. Проте широкомасштабне впровадження SLB натрапляє на низку бар’єрів — технічних, економічних, регуляторних, а також пов’язаних із відсутністю системного бачення.

Попри зростаючу кількість досліджень і пілотних проєктів, повторне використання батарей досі розглядається переважно як питання економічної доцільності і технологічної реалізації. Недостатньо уваги приділяється моделюванню SLB як елемента системи прийняття рішень у сфері управління ресурсами, екологічного регулювання, інноваційного розвитку та енергетичної безпеки. Системне моделювання дозволяє виявити вузькі місця, потенціал, сценарні ризики та стратегічні точки втручання. Водночас такий підхід потребує мультидисциплінарності та інтеграції економічних, технічних, соціальних і правових аспектів.

У зв’язку з цим видається необхідним формування концептуальної основи моделювання потенціалу повторного використання SLB в енергетичних системах як елемента формування політики циркулярної енергетики. Такий підхід передбачає створення узагальненої моделі, що дозволяє оцінити вплив сценаріїв повторного використання SLB на сталість, гнучкість і ефективність енергетичних систем, а також визначити вимоги до політик і регуляторних інструментів.

Зважаючи на поточну невизначеність щодо того, яка частка відпрацьованих акумуляторів буде придатна для повторного використання, аналітичні оцінки вказують на значний потенціал їх перепрофілювання [1]. Для України це означає одночасно і серйозні виклики, і нові можливості. З

одного боку, постає завдання налагодити ефективну систему діагностики, відновлення та інтеграції акумуляторів у нові застосування. З іншого — відкривається перспектива розробки і впровадження інноваційних рішень у сфері накопичення енергії, як на рівні домогосподарств, так і в комерційному та промисловому сегментах.

Запропонований підхід до моделювання повторного використання вторинних батарей електротранспорту є комплексним і багаторівневим. Він включає низку взаємопов'язаних моделей, кожна з яких виконує окрему функцію в межах загальної системи підтримки рішень.

До складу підходу входять:

1. ***Модель оцінки деградації,*** що базується на спеціалізованому індексі деградації (ІД), який об'єднує календарне, циклічне та стохастичне старіння [2]. Такий індекс дозволяє здійснювати кількісну оцінку залишкового технічного потенціалу батареї незалежно від джерела даних про її історію. Для побудови моделі можуть використовуватись емпіричні криві старіння, машинне навчання (наприклад, регресія або дерева рішень), а також статистичне згладжування.

2. ***Модель розрахунку залишкового ресурсу*** (Rest of Useful Life, RUL) та прогнозованого строку ефективного використання SLB [3]. Вона базується на динаміці індексу ІД та SOH (State of Health) і дозволяє визначити оптимальний часовий горизонт для експлуатації в заданому сценарії. Тут застосовуються методи прогнозування часових рядів, експоненційного згладжування, а також граничні правила на основі порогових значень деградації.

3. ***Модель економічної доцільності***, яка дозволяє зіставити альтернативи використання SLB за допомогою таких показників як LCOS (Levelized Cost of Storage), внутрішня норма прибутку (IRR), чиста приведена вартість (NPV). Вона враховує витрати на відбір, діагностику, відновлення, монтаж і обслуговування, а також доходи або зекономлені витрати впродовж періоду повторного використання [4]. Може застосовуватись як в ізольованому аналізі, так і як частина сценарного порівняння.

4. Оптимізаційна ***модель розподілу батарей,*** яка формалізується як задача багатокритеріальної оптимізації з обмеженнями. Вона дозволяє визначити найкращий варіант розміщення SLB з урахуванням витрат, надійності, просторової доцільності, екологічного ефекту та технічної сумісності [5]. Застосовуються методи кластерного аналізу, цілочисельного програмування, лінійного та нелінійного програмування, а також еволюційні алгоритми у випадку складних топологій.

5. ***Просторова модель***, яка забезпечує прив'язку рішень до конкретних об'єктів енергосистеми (домогосподарства, підстанції, розподільчі центри тощо). Вона враховує параметри локального навантаження, доступності інфраструктури, частки ВДЕ в регіоні, а також просторові ризики (повені, пошкодження мереж). Для реалізації можуть використовуватись GIS-системи, картографічна статистика, методи оцінки густини потенціалу та агреговані багатошарові карти прийняття рішень.

6. ***Модель прогнозування та планування заміни батарей***, яка визначає момент, коли батарею слід виводити з експлуатації або переводити на менш критичне навантаження. Рішення ґрунтується на досягненні критичних значень деградації або зниженні техніко-економічних параметрів нижче допустимого порогу. Модель може бути реалізована у вигляді порогових правил, а також включена в оптимізаційний блок із урахуванням прогнозу попиту, наявності замінників та стратегій управління запасами.

Узагальнені характеристики кожної з моделей повторного використання вторинних батарей електротранспорту представлені в Табл.1.

Таблиця 1 - Структура підходу до моделювання використання вторинних батарей електротранспорту в енергетичних системах

Назва моделі	**Вхідні параметри**	**Вихідні показники**	**Використані методи**
Модель деградації	Календарний вік, кількість циклів, температура, історія навантажень	Індекс деградації (ІД), темпи втрати ємності	Емпіричне моделювання, регресія, машинне навчання
Модель залишкового ресурсу (RUL)	SOH(t), індекс деградації, історія експлуатації	Оцінка залишкового ресурсу, прогнозований строк служби	Прогнозування, експоненційне згладжування, часові ряди
Модель економічної доцільності	Витрати, строк служби, ефективність, тариф/прибуток	LCOS, NPV, IRR, термін окупності	Фінансове моделювання, сценарний аналіз, LCO/LCOS
Оптимізаційна модель розподілу бататрей	Витрати, надійність, розташування, екологічні вигоди	Найкраще розміщення SLB за обраними критеріями	Багатокритеріальна оптимізація, математичне програмування
Просторова модель	Навантаження, інфраструктура, ВДЕ, ризики території	Карта доцільності, рейтинг об’єктів	ГІС-аналіз, просторове багатокритеріальне оцінювання
Модель планування заміни	SOH, індекс деградації, граничні пороги	Момент заміни, рекомендації щодо подальшого використання або утилізації	Порогові правила, логіка заміни, динамічне планування

Ці моделі об'єднуються в узгоджену методологічну рамку, що дозволяє здійснювати порівняльну оцінку сценаріїв повторного використання SLB у різних контекстах: стаціонарні накопичувачі, мікромережі, гнучкість навантаження, резервне живлення тощо. Кожен сценарій оцінюється з урахуванням технічної придатності, економічної ефективності, екологічних вигод та регуляторних обмежень, що забезпечує адаптивність і практичну застосовність підходу в умовах реального планування.

Вторинні батареї електротранспорту мають розглядатися не лише як комерційний продукт, а передусім як елемент системного управління енергетичним переходом. Їх повторне використання виходить за межі простої утилізації: це інструмент, який може суттєво впливати на конфігурацію енергетичного ландшафту. У такому контексті моделювання виконує функцію політичного інструмента — воно допомагає перетворювати складні технічні та економічні дані на аргументовані рішення, формувати сценарії, які можуть бути безпосередньо застосовані в енергетичній політиці.

З огляду на це, SLB доцільно розглядати як адаптивний ресурс у сфері циркулярної енергетики. Важливо, щоб національна політика включала індикатори ефективності повторного використання батарей, а також створювала умови для залучення SLB до систем управління попитом і гнучкістю. Підтримка досліджень і пілотних проєктів, які поєднують моделювання з розробкою політичних рішень, є необхідною умовою для успішного впровадження цієї практики. Крім того, підходи циркулярної економіки мають бути інтегровані до нормативно-правової бази енергетичного сектору. Особливу увагу слід приділяти застосуванню індексу деградації SLB як інструмента для диференційованого регулювання та стратегічного планування заміни.

Таким чином, моделювання повторного використання SLB має потенціал стати повноцінним інструментом формування політики — здатним забезпечити перехід від реактивного реагування на екологічні та технологічні виклики до проактивного, адаптивного та відповідального управління ресурсами.

[1] Kostenko, G., & Zaporozhets, A. (2024). World experience of legislative regulation for lithium-ion electric vehicle batteries considering their second-life application in power sector. System Research in Energy, 2(77), 97–114. https://doi.org/10.15407/srenergy2024.02.097

[2] Костенко, Г., & Запорожець, А. (2024). Інтегральний показник деградації вторинних батарей електромобілів в системах зберігання енергії: урахування календарного та циклічного старіння. Системні дослідження в енергетиці, (2a (78), 31-33. вилучено із https://systemre.org/index.php/journal/article/view/848

[3] 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

[4] 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

[5] Костенко, Г. (2025). Кластерний підхід до використання вторинних батарей електротранспорту для надійного та сталого резервного живлення в енергосистемах. Системні дослідження в енергетиці, (1 (81), 40-60. https://doi.org/10.15407/srenergy2025.01.040

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

ГЕНЕРАТОР ЗОНДУВАЛЬНИХ СИГНАЛІВ ТРУБОПРОВОДІВ І ЙОГО ПРОГРАМА КЕРУВАННЯ

ВСТУП. Умови технічного діагностування систем тепло- та водопостачання міст України потребують розвитку відповідного приладового забезпечення. Це спричинено сукупністю ускладнень, які вносять загальний знос систем, військові умови та їх наслідки у діагностування. У першу чергу це стосується оперативного визначення місць частих витоків у підземних трубопроводах [1]. Бо ці об'єкти забезпечують стале тепло- та водопостачання населення і є критичними.

Найбільш чутливим до витоків та поширеним методом їхнього акустичного визначення є кореляційний метод (КМ). Для збільшення його можливостей та ефективності застосування розроблена система РАСТР-2В [2]. Важливою складовою цієї системи є підсистема акустичного зондування трубопроводу. Ця активна підсистема додає до звичайного, пасивного КМ нових, витребуваних на сьогодні можливостей [3]:

- При розрахунку просторової координати витоку за допомогою КМ використовувати не приблизне теоретичне значення швидкості акустичних сигналів витоку, а виміряне, фактичне значення. Спосіб цього вимірювання пристосований до наявних умов і не потребує втручання в гідравлічний режим роботи зношених систем тепло- та водопостачання. Значення швидкості вимірюється саме на пошкодженій підземній ділянці трубопроводу і саме на частотах сигналів від зареєстрованого за КМ витоку. Це дозволяє зручно враховувати вплив на точність визначення місць витоків корозійного пошкодження ділянок трубопроводів та їх акустичних особливостей.
- Перед застосуванням КМ контролювати повноту заповнення пошкодженої ділянки трубопроводу водою, бо заповнення є умовою застосування КМ. Контроль потрібний при пошуку витоків на пошкоджених і тому відключених перед заповненням для діагностування відгалуженнях.
- Контролювати загасання та прохідність акустичних хвиль по ділянці трубопроводу, що діагностується. Це важливо у важких випадках застосування КМ, коли виток не реєструється і потрібно з'ясувати причину відсутності очікуваної кореляції зареєстрованих по кінцях трубопроводу акустичних сигналів.

Активним елементом підсистеми, який генерує потужні зондувальні сигнали, є Генератор. Генератор створено на базі однокристального мікроконтролера та керується його програмою.

ПРИЗНАЧЕННЯ. Генератор призначений для створення у трубопроводі акустичних зондувальних сигналів заданого виду з встановленими параметрами. Генератор складається з блоку генератора, акустичних

випромінювачів та сигнальних кабелів. Генератор є складовою частиною РАСТР-2В, в яку також входять три багатоканальні реєстратори акустичних сигналів трубопроводів з вібродатчиками, генератор радіо сигналів синхронізації вимірювань, мобільний комп'ютер для обробки даних [2].

Функціонально РАСТР-2В поділяється на активну та пасивну підсистеми. Застосування генератора разом з реєстраторами та їхніми датчиками утворюють підсистему активного зондування трубопроводів. Окреме застосування реєстраторів з датчиками утворюють пасивну підсистему визначення координат витоків трубопроводів. Для забезпечення синхронізованих вимірювань між рознесеними у просторі реєстраторами у обох підсистемах застосовується окремий генератор радіосигналів синхронізації. Для обробки даних використовується ноутбук зі спеціальним програмним забезпеченням.

Програма забезпечує введення оператором у генератор витребуваних у конкретних умовах параметрів та виду зондувального сигналу, відображення поточного режиму та стану зондування на цифровому екрані генератора, керування його роботою.

ХАРАКТЕРИСТИКИ. Генератор (Рис.1.) містить керуючий контролер, акумулятори, МП3 програвач треків зондувальних сигналів з SD карти, підсилювач класу АВ потужністю 100 Вт та інші супутні елементи. На рис.2 більш детально вказано призначення індикаторів генератора.

Рис.1. Фото генератора з підключеним акустичним випромінювачем.

Рис.2 Панель керування генератора.

РОБОТА ПРОГРАМИ**.** Програму створено у системі програмування Arduino. Програма міститься у флеш-пам'яті контролера керування генератором, працює у двох режимах - зондування та зупинки.

Параметрами, що задаються в режимі зупинки, є:

- номер тесту - звукового треку на SD-карточці МП3 програвача, змінюється від 1 до 9;
- рівень звуку на виході генератора, задається від 1 до 9;
- тривалість звучання, задається від 1 до 11 хвилин;

Параметр, доступний до зміни в режимі зондування - рівень звуку. Зміна номеру тесту та тривалості зондування (звучання) заблоковано.

Параметр, що змінюється автоматично в режимі зондування – поточна тривалість зондування. Відображення напруги акумуляторів при натисканні відповідної кнопки, рис.2, не залежить від режиму роботи генератора.

Даний випробувальний зразок автономного генератора з програмою керування створено для відпрацювання нових підходів, схем та приладових режимів визначення витоків підземних трубопроводів в умовах їхньої експлуатації.

Автори висловлюють щиру подяку Національному фонду досліджень України за грантову підтримку, завдяки якій була виконана дана розробка в рамках проєкту №2023.04/0022 «Розроблення апаратно-програмного

комплексу та методики оперативного виявлення пошкоджень систем тепло- та водопостачання з врахуванням їх зношеності та мілітарних впливів».

[1] Владимирський О.А, Владимирський І.А., Артемчук В.О., Криворучко І.П., Семенюк Д.М. Особливості і розвиток технологій виявлення витоків трубопроводів тепло- та водопостачання в умовах зношеності та мілітарних впливів. Електронне моделювання. 2024, 46(5), С. 64-73. URL: https://doi.org/10.15407/emodel.46.05.064.

[2] Владимирський О.А, Владимирський І.А., Артемчук В.О. Комп'ютерна програма «Багатоканальний реєстратор «Вібрологгер - 3.02» системи виявлення витоків підземних трубопроводів «РАСТР-2В» Свідоцтво про реєстрацію авторського права на службовий твір № 132954 від 03.02.2025р. ІПМЕ ім. Г.Е. Пухова НАН України. URL: https://sis.nipo.gov.ua/uk/search/detail/1848332/.

[3] Vladimirsky A.A., Vladimirsky I.A. Correlation parametric method for determining the velocity of acoustic wave propagation in a pipeline. Electronic Modeling, 2024, 46(6). P.55-63. URL: https://doi.org/10.15407/emodel.46.06.055.

С.Ф. Гончар, В.В. Ткаченко

УДОСКОНАЛЕНА СТРУКТУРНА МОДЕЛЬ ВЗАЄМОДІЇ ЕЛЕМЕНТІВ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОБ'ЄКТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Дослідження показують [1, 2], що на об'єктах критичної інфраструктури можуть виникати аварійні ситуації, при яких вплив вражаючих факторів початкової (ініціюючої) події на сусіднє обладнання призводить до появи інших руйнівних подій, наслідки яких можуть бути важчими, ніж викликані тільки однією ініціюючою подією – каскадні аварії. Такі аварії можуть призвести до серйозних техногенних катастроф на об'єктах критичної інфраструктури із заподіянням великого збитку, у тому числі екологічного. Наприклад, в ході аварії на АЕС Фукусіма-1, відмова насосів подавання морської води і системи аварійного енергозабезпечення призвели до аварії реактора з втратою теплоносія, до часткового розплавлення реактора, нагрівання сховища відпрацьованого палива, пожежі, викидання радіації в атмосферу [3]. Також, техногенні аварії каскадного характеру сталися на заводах з виробництва зрідженого природного газу в 1972 році у Монреалі (Канада), у 1983 році в місті Бонтанг (Індонезія) та у 2004 році в Алжирі [4].

Таким чином, актуальною задачею являється розробка методів оцінювання ризиків виникнення таких аварій. Для цього, використовуючи структурну модель взаємодії елементів інформаційної системи об'єкту критичної інфраструктури [5, 6], розглянемо удосконалену структурну модель взаємодії елементів інформаційної системи об'єкту критичної інфраструктури, рис. 1.

Рисунок 1 – Удосконалена структурна модель взаємодії елементів інформаційної системи об'єкту критичної інфраструктури

[1] Бєлов П.Г. Управління ризиками, системний аналіз і моделювання: навчальний посібник і практикум / П.Г. Бєлов. – М.: Видавництво Юрайт, 2016. - 272 с.
[2] Гончар С. Ф. Методологія оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури: дис. на здобуття наукового ступеня доктора техн. наук: 05.13.21, Київ, 2020. 326 с.
[3] Брежнєв Є.В. Метод оцінювання ризиків каскадних відмов (аварій) з використанням динамічних матриць критичності / Є.В. Брежнєв // Наука і техніка Повітряних Сил Збройних Сил України. 2015, № 1 (18), С. 187-190.
[4] Бєлов П.Г. Управління ризиками, системний аналіз і моделювання: навчальний посібник і практикум / П.Г. Бєлов. – М.: Видавництво Юрайт, 2016. - 272 с.
[5] С. Гончар, Г. Леоненко, «Аналіз факторів впливу на стан кібербезпеки інформаційної системи об'єкту критичної інфраструктури», InformationTechnologyandSecurity, Vol. 4, Iss.2 (7), С. 262-268, 2016.
[6] Гончар С.Ф. Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури. Монографія. Київ: «Альфа реклама», 2019, 176 с.

Д.П. Сінько, К.Д. Сінько

ЗАСТОСУВАННЯ МАШИННОГО НАВЧАННЯ У ВИЯВЛЕННІ ПЕРЕДУМОВ ДО ПОТЕНЦІЙНОГО ПОДІЛУ КЛАСТЕРА

Анотація. У тезах представлено реалізацію авторського підходу, запропонованого в попередній роботі «Аналіз застосовності методів машинного навчання при вирішенні задачі прогнозу реалізації чинників партиціювання кластеру», засобами мови програмування Python та спеціалізованих бібліотек. На основі чисельного моделювання встановлено, що моделі Gradient Boosting та CatBoost забезпечують найвищу ефективність у прогнозуванні факторів, що можуть свідчити про потенційне партиціювання кластеру та виникненню проблеми розщеплення кластера. Отриманий застосунок може бути використаний як практичний інструмент для фахівців, що проектують складні кластерні кібернетичні системи, а також як приклад для створення власних інструментів.

Вступ. У попередніх тезах [1] було запропоновано використання методів машинного навчання для прогнозування проблеми розщеплення кластера (далі ПРК) - критичного стану кластерних систем, пов'язаного з їх партиціюванням, у англомовній літературі цей термін відомий як split brain problem [2]. Було розглянуто підхід до підтримки консистентності у кластерах із реплікацією типу single leader [3], де одна з нод виконує роль лідера, а в разі розпаду інші частини кластера орієнтуються на її рішення.

У даній роботі здійснено подальший розвиток цього підходу шляхом чисельного експерименту, спрямованого на виявлення найбільш ефективного алгоритму прогнозування ПРК. Для реалізації моделі обрано мову Python, що має розвинуту екосистему та потужні засоби для побудови моделей машинного навчання. Окрему увагу приділено візуалізації результатів моделювання та забезпеченню їх повторюваності. Було створено відкритий репозиторій з вихідним кодом і матеріалами, достатніми для самостійного відтворення результатів.

Виклад основного матеріалу

У рамках дослідження розглянуто розробку програмного засобу для виявлення та візуалізації ситуацій типу ПРК у кластерних системах. Як основний інструмент реалізації було використано мову Python завдяки її широким можливостям для чисельного моделювання, наявності бібліотек для машинного навчання, а також зручності створення вебсервісів через Django, що значно пришвидшило процес розробки.

Було створено веб-інтерфейс, що дає змогу користувачам у інтерактивній формі будувати кластер, вводити ноди, формувати між ними одно- або двосторонні зв'язки, які автоматично відображаються у вигляді матриці доступності, де цифра 0 - відсутність зв'язку, 1 - наявність зв'язку між нодами. Побудований кластер надсилається на сервер, де обчислюється ймовірність виникнення ПРК за допомогою заздалегідь навчених моделей.

Сервіс також перевіряє чи не є кластер мертвим, адже в такому випадку ситуація ПРК є неможливою. Живим кластер вважається, якщо він має хоча б один повністю функціонуючий острів, тобто містить хоча б по одній ноді кожного типу. Стан ПРК фіксується у випадку, якщо є 2 та більше повністю функціонуючих островів. Для пошуку островів використовується пошук у глибину.

При вирішенні задачі робиться декілька припущень. Перше це те, що кластер не може розділитися так, аби хоча б два острови були функціональними, якщо не існує хоча б два екземпляри певного типу ноди. Всі типи ноди вважаються рівно важливими для повноцінного функціонування кластеру. Також вважається, що єдиним повноцінним зв'язком є двосторонній, коли обидві ноди можуть комунікувати між собою, в інакшому випадку зв'язок є втраченим.

Після відправлення кластеру до сервера постає проблема розмірності. Програма працює з кластерами розміром від 4 нод до 20. Розміри менше 4 майже не мають практичного сенсу — ймовірність split brain у таких випадках надзвичайно низька, і вони скоріше заважають навчанню, ніж допомагають. З іншого боку, розміри понад 20 є надто важкими для обробки в поточних технічних умовах. Тому виникає ньюанс з тим, аби модель завжди отримувала дані однакового розміру. До того ж, модель має розуміти де в матриці є певний тип, тому був створений метод preprocess. Він отримує на вході список нод, матрицю доступності та перетворює це на матрицю розмірністю 21x20 вигляду, де цифри від 2 до ∞ позначають тип ноди, 0 - відсутність зв'язку, 1 - наявність зв'язку між нодами, -1 - відсутність ноди.

Для тренування моделі використовувалися синтетичні дані, що містили ноди зі списку A, B, C, та мали розмір від 4 до 20 нод. Так само вони проходили через функцію preprocess, що робила єдиний розмір та формат даних для навчання. Для кожного кластеру визначалася мітка, чи є ситуація ПРК чи ні і зберігалася в масив. Також додатково у тренувальний масив додавалось 500 тисяч екземплярів, де була ситуація ПРК. Таке рішення дозволило значно покращити результати моделі, адже під час тренування вона мала більше прикладів.

Було проведено експеримент із трьома методами для виявлення та прогнозування ситуацій партиціювання в розподілених системах. Результати можуть бути використані для створення проактивної адміністративної ноди, що в реальному часі моніторить стан системи та надає рекомендації у разі критичних подій.

Random Forest [4] демонструє високу точність за рахунок ансамблю незалежних дерев рішень, що знижує ризик перенавчання. Модель була побудована з використанням 400 дерев глибиною до 20 рівнів, параметри max_features="sqrt" і class_weight="balanced" дозволили досягти балансу між ознаками та класами. Для навчання використовувалися 500 тисяч випадкових кластерів та додаткові 50 тисяч із підтвердженим станом ПРК. Через обмеження пам'яті модель не масштабувалася до більших обсягів, оскільки

займала до 5.5 ГБ. Навчання проводилося із використанням Gini-критерію, а серіалізація моделі здійснювалася за допомогою pickle

Алгоритм Gradient Boosting [5] був обраний завдяки здатності моделювати складні залежності між ознаками. Модель складалася з 200 дерев з максимальною глибиною 7 рівнів і темпом навчання 0.1. Кожне дерево навчалося на помилках попереднього, оптимізуючи прогнозування за допомогою градієнтного спуску. Навчання виконувалося на більшій виборці - 900 тисяч звичайних кластерів і 500 тисяч із ПРК. Такий підхід забезпечив високу точність і узагальнюючу здатність моделі в реалістичних сценаріях.

CatBoost [6] був використаний для ефективної роботи з числовими та категоріальними ознаками без необхідності попередньої обробки. Було побудовано модель з 1000 дерев, глибиною 10 рівнів, з темпом навчання 0.1 та логарифмічною функцією втрат. Для тренування використано 1.4 мільйона прикладів, зокрема 500 тисяч з ПРК, як і в попередньому випадку. Завдяки своїй стійкості до перенавчання, CatBoost продемонстрував стабільну роботу з великими та незбалансованими наборами даних. Навчена модель зберігалася за допомогою pickle для подальшого використання без повторного тренування.

Окрім зазначених вище завдань, автор також прагнув забезпечити відтворюваність експерименту. Вихідний код розміщено у відкритому доступі в репозиторії https://github.com/PSnik-Kostiantyn/SplitBrainDetector на GitHub. Щоб розпочати роботу, необхідно клонувати репозиторій, наприклад, за допомогою GitHub CLI командою: gh repo clone PSnik-Kostiantyn/SplitBrainDetector. Далі слід відкрити проєкт у зручному середовищі розробки, перейти до його директорії та у терміналі виконати команду python manage.py runserver. Після цього застосунок буде запущено локально, і його можна відкрити у браузері за адресою: http://127.0.0.1:8000/.

Репозиторій вже містить натреновані моделі. Однак, якщо ви бажаєте провести навчання самостійно, достатньо видалити або перейменувати відповідні файли моделей, а потім надіслати запит на прогнозування. У разі відсутності збереженої моделі програма автоматично розпочне навчання нової моделі та збереже її для подальшого використання.

Детальніші інструкції щодо запуску та використання застосунку можна знайти у файлі README.md, що входить до складу репозиторію.

Висновок

У ході дослідження було розглянуто три методи машинного навчання для вирішення задачі прогнозування проблеми розщеплення кластера у розподілених кластерних системах: Random Forest, Gradient Boosting та CatBoost. Незважаючи на обмеження апаратного забезпечення, усі моделі продемонстрували здатність ефективно аналізувати складні зв’язки між компонентами системи, особливо у кластерах з більшою кількістю нод.

Random Forest виявився найбільш ефективним при роботі з малим обсягом даних та невеликими кластерами, однак обмежена масштабованість і високе споживання пам’яті знижують його придатність для роботи з великими системами. Gradient Boosting продемонстрував найстабільніші

результати, особливо при роботі з великими кластерами (понад 8 нод), завдяки здатності виявляти якісні відмінності у структурі з'єднань. CatBoost, у свою чергу, проявив високу чутливість у критичних ситуаціях і продемонстрував конкурентну точність на менших вибірках, однак виявився менш стійким до незначних змін у структурі графа.

Варто зауважити, що наданий код є лише однією з можливих реалізацій, і існує багато інших підходів, які можуть бути використані для покращення результатів. Найперспективнішим напрямком є комбіноване використання Gradient Boosting та CatBoost, що дозволяє поєднати їх сильні сторони для побудови проактивної системи моніторингу стану кластеру. У майбутньому доцільно дослідити гібридні ансамблеві підходи, оптимізацію гіперпараметрів, а також застосування глибоких нейронних мереж. Крім того, розширення набору даних за рахунок реальних сценаріїв дозволить підвищити надійність та узагальнюючу здатність моделей.

[1] Сінько, Д. П., & Сінько, К. Д. (2024). Аналіз застосованості методів машинного навчання при вирішенні задачі прогнозу реалізації чинників партиціювання кластеру. У МАТЕРІАЛИ XXIV міжнародної науково-технічної конференції«Штучний інтелект та інтелектуальні системи- AIIS'2024» (с. 170–173). Інститут проблем штучного інтелекту МОН та НАН України. https://www.ipai.net.ua/docs/AIIS-2024.pdf

[2] Bhuiyan, S., & Zheludkov, M. (2019). Apache ignite book. Lulu Press, Inc.

[3] Shang, Y. (2024). Resilient leaderless and leader-follower consensus over random networks through ℓ-hop communication. European Journal of Control, 101075. https://doi.org/10.1016/j.ejcon.2024.101075

[4] Louppe, G. (2014). Understanding random forests: From theory to practice. Choice Reviews Online, 45(02), 45–0602. https://doi.org/10.5860/choice.45-0602

[5] Brownlee, J. (2023). A gentle introduction to the gradient boosting algorithm for machine learning. https://machinelearningmastery.com/gentle-introduction-gradientboosting-algorithm-machine-learning/

[6] Hancock, J. T., & Khoshgoftaar, T. M. (2020). CatBoost for big data: an interdisciplinary review. Journal of Big Data, 7(1). https://doi.org/10.1186/s40537-020-00369-8

Є.В. Парус, І.В. Блінов

ІМІТАЦІЙНА МОДЕЛЬ ПЛАНУВАННЯ УЧАСТІ АКТИВНОГО СПОЖИВАЧА НА РИНКУ ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ

Децентралізація процесів управління електроенергетикою зумовлює потребу в розвитку децентралізованих платформ торгівлі електричною енергією. При цьому розробка нормативно-правової бази щодо впровадження і функціонування децентралізованих сегментів ринку електричної енергії має базуватися на результатах досліджень поведінкових моделей учасників таких платформ, передусім – активних споживачів [1]. Модель поведінки активного споживача, у свою чергу, має враховувати його технічні можливості та економічні інтереси в частинах забезпечення власного електроспоживання та продажу надлишків електроенергії власного виробництва. Таким чином, стратегія участі активного споживача на ринку електроенергії базується на економічно обґрунтованих планах закупівлі та продажу електроенергії, якими враховуються його економічні інтереси та технічні можливості реалізації таких планів.

Процедура визначення активним споживачем оптимальних графіків закупівлі та продажу електричної енергії є однією із основних задач планування, які реалізує система енергоменеджменту. Вимоги до архітектури та функцій системи енергоменеджменту визначені у [2]. Для розв'язання поставленої задачі виконується імітація режимів енергетичного устаткування з метою пошуку оптимальних графіків отримання електроенергії з мережі розподілу та відпуску електроенергії у мережу розподілу. Основними критеріями для оцінки оптимальності при цьому виступають економічні витрати на забезпечення власних потреб в електроенергії та вигода від продажу електроенергії. Оптимальні графіки закупівлі та продажу активним споживачем електроенергії є основою для формування відповідних ставок на децентралізованій торговій платформі.

Таким чином, цільова функція задачі формування оптимальних графіків закупівлі та продажу активним споживачем електроенергії поєднує дві задачі оптимізації: мінімізацію вартості закупівлі електроенергії та максимізацію вигоди від продажу електроенергії протягом розрахункового періоду, наприклад розрахункової доби:

$$Max\left(\mathrm{Prof}_D^{\mathrm{AC}}\right) \cup Min\left(\mathrm{Cost}_D^{\mathrm{AC}}\right), \qquad (1)$$

де: $\mathrm{Cost}_D^{\mathrm{AC}}$ – витрати на закупівлю електроенергії протягом розрахункової доби; $\mathrm{Prof}_D^{\mathrm{AC}}$ – вигода від продажу електроенергії протягом розрахункової доби.

Обсяги купівлі та продажу активним споживачем електроенергії відповідають обсягам отримання із системи розподілу та відпуску у систему розподілу електричної енергії як складові балансів електроенергії між

електричною мережею активного споживача та системою розподілу. Зважаючи на єдину фізичну сутність отриманої і відпущеної електроенергії, цільову функцію можливо подати як задачу однокритеріальної оптимізації, тобто як задачу мінімізації витрат чи максимізації вигоди за розрахункову добу. Приймаючи одну годину за базовий період незмінних цін купівлі чи продажу електроенергії, отримуємо цільову функцію:

$$Max\left(\sum_{h=1}^{24} C_h^{\text{sell}} \cdot V_h^{\text{out}} - \sum_{h=1}^{24} C_h^{\text{buy}} \cdot V_h^{\text{in}}\right) \equiv Min\left(\sum_{h=1}^{24} C_h^{\text{buy}} \cdot V_h^{\text{in}} - \sum_{h=1}^{24} C_h^{\text{sell}} \cdot V_h^{\text{out}}\right), \qquad (2)$$

де: V_h^{in}, V_h^{out} – погодинні обсяги відповідно закупівлі електричної енергії у постачальника та відпуску електричної енергії; C_h^{buy}, C_h^{sell} – погодинні ціни відповідно купівлі та продажу електричної енергії.

Цільова функція (2) здійснює оцінку балансів споживання/відпуску електроенергії за економічними критеріями. Загальний баланс виробництва/споживання електроенергії енергетичним устаткуванням активного споживача визначається системою рівнянь погодинних балансів у системі обмежень для (2). Крім того, система обмежень для цільової функції (2) містить математичні моделі імітації функцій енергетичного устаткування активного споживача. Зокрема визначаються технічні обмеження енергетичного устаткування різних режимах, імітуються функції управління режимами енергетичного устаткування, а також розраховуються технологічні втрати електроенергії.

Система обмежень для задачі побудови оптимального графіка закупівлі електроенергії формується на основі математичного апарату, наведеного у [3]. У публікації наводиться математична модель для імітації процесів узгодженого функціонування нерегульованого джерела електроенергії на прикладі сонячної електростанції та установки зберігання енергії (УЗЕ) згідно із сценарієм оптимізації використання локальних ресурсів для підвищення надійності та ефективності електропостачання споживачів мікромережі [4]. Для пошуку оптимального графіка закупівлі електроенергії математична модель в [3] здійснює імітацію функцій управління режимами УЗЕ за викладеними у [5] принципами. Система обмежень для задачі побудови оптимального графіка продажу електроенергії формується на основі математичних моделей для вирішення аналогічних задач оптимізації графіків роботи учасників ринку електричної енергії України, наведених, наприклад, у [6 – 10].

Визначені складові побудови імітаційної моделі є основою для створення ефективного інструментарію планування участі активного споживача у на роздрібному ринку електроенергії та створення функції планування режимів роботи енергетичного устаткування у складі системи енергоменеджменту [11] активного споживача.

Публікацію підготовлено в межах виконання наукової роботи «Розвиток розподіленої енергетики в умовах ринку електричної енергії України з використанням технологій та систем цифровізації. Розділ 1.

Організаційні та математичні моделі взаємодії учасників децентралізованого ринку електроенергії (шифр: Цифровізація))» (КПКВК 6541230).

[1] Закон України «Про ринок електричної енергії» № 2019-VIII (13.04.2017). http://zakon3.rada.gov.ua/laws/show/2019-19

[2] International electrotechnical commission. (2024). Microgrids - Part 3-2: Technical requirements - Energy management systems (IEC TS 62898-3-2:2024).

[3] Блінов, І.В, Парус, Є.В., Шиманюк, П.В. & Ворушило, А.О. (2024). Модель оптимізації функціонування мікромережі з СЕС та установкою зберігання енергії. Технічна електродинаміка, 5, 69 – 78. https://doi.org/10.15407/techned2024.05.069

[4] Блінов, І.В., Палачов, С.О., Парус, Є.В. & Клименко, О.Г. (2025) Сценарії використання мікромереж згідно з міжнародними стандартами. Праці Інституту електродинаміки Національної академії наук України, 70, 14 – 25. https://doi.org/10.15407/publishing2025.70.014

[5] International electrotechnical commission. (2023). Microgrids - Part 3-3: Technical requirements - Self-regulation of dispatchable loads (IEC TS 62898-3-3:2023).

[6] Parus, E., Olefir, D., Kyrylenko, O. & Blinov, I. (2024). Constrained Multi-Criteria Optimization of the Hydroelectric Power Plant Schedule for Participation in the Day-Ahead Market of Ukraine. In: Kyrylenko, O., Denysiuk, S., Strzelecki, R., Blinov, I., Zaitsev, I., Zaporozhets, A. (eds) Power Systems Research and Operation. Studies in Systems, Decision and Control, 512. Springer, Cham. https://doi.org/10.1007/978-3-031-44772-3_3.

[7] Парус, Є.В., Блінов, І.В. & Олефір, Д.О. (2023). Формування графіка пропозиції ГЕС на ринку «на добу наперед» методами умовної оптимізації зі штрафними функціями. Технічна електродинаміка, 6, 71 – 80. https://doi.org/10.15407/techned2023.06.071

[8] Олефір, Д.О., Парус, Є.В., Рибіна, О.Б. & Мірошник, В.О. (2024). Оптимізація добового графіку роботи гідроелектростанції з урахуванням нелінійної функції витрат на власні потреби. Праці Інституту електродинаміки Національної академії наук України, 69, 36 – 45. https://doi.org/10.15407/publishing2024.69.036

[9] Парус, Є.В., Блінов, І.В., Мірошник, В.О., Рибіна, О.Б., Олефір, Д.О. & Сичова, В.В. (2024). Модель оптимального розподілу гідроресурсів ГЕС з резервуванням потужностей для надання допоміжних послуг автоматичного відновлення частоти. Технічна електродинаміка. 3, 73 – 82. https://doi.org/10.15407/techned2024.03.073

[10] Олефір, Д. ., Є. Парус, О. . Рибіна, і В. . Мірошник. (2024). Оптимізація добового графіку роботи гідроелектростанції з урахуванням нелінійної функції витрат на власні потреби. Праці Інституту електродинаміки Національної академії наук України, вип. 69, Листопад 2024, с. 036, DOI: 10.15407/publishing2024.69.036.

[11] Кириленко, О.В., Денисюк, С.П. & Блінов, І.В. (2024). Енергетичний менеджмент: нові пріоритети XXI століття. Енергетика: економіка, технології, екологія, 1, 7 – 27. https://doi.org/10.20535/1813-5420.1.2024.297508

П.В. Шиманюк

ЗАСТОСУВАННЯ НЕЙРОННИХ МЕРЕЖ ДЛЯ ВИЗНАЧЕННЯ ВТРАТ ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ В СИСТЕМАХ РОЗПОДІЛУ

Актуальність дослідження обумовлена сучасними трендами в управлінні режимами роботи розподільних електричних мереж із використанням технологій Smart Grid [1,2], а також необхідністю зниження витрат операторів систем розподілу на закупівлю електроенергії. Для цього потрібні точні результати прогнозування навантажень у вузлах мережі на різних горизонтах прогнозування. Різкі зміни топології мережі можуть збільшувати похибки прогнозу втрат як єдиного часового ряду, що негативно впливає на ефективність керування мережею та підвищує витрати на закупівлю електроенергії для покриття втрат.

Розвиток методів машинного навчання та нейронних мереж для прогнозування втрат в електричних мережах є важливим кроком у вдосконаленні управління сучасними енергосистемами. Традиційні методи розрахунку втрат, засновані на фізичних моделях, мають обмежену точність через складність врахування багатьох змінних, таких як динаміка навантаження, погодні умови, структурні особливості мережі та її стан. Використання машинного навчання дозволяє подолати ці обмеження завдяки здатності алгоритмів виявляти складні нелінійні залежності між параметрами, що важко формалізувати вручну. Нейронні мережі особливо ефективні завдяки їх гнучкості та здатності до навчання на великих масивах даних, що дає можливість прогнозувати втрати з високою точністю навіть у ситуаціях, коли початкові дані містять значну кількість невизначеності [3-5].

Для визначення очікуваних значень втрат запропоновано використати метод прогнозування на основі штучних нейронних мереж. Для оцінки ефективності було розглянуто два підходи: Розрахунок втрат на основі прогнозних значень вузлового навантаження та прогнозування втрат на основі розрахованих значень втрат. В обох випадках використовується одна і таж нейронна мережа з архітектурою на основі рекурентної мережі типу LSTM (Long-short term memory – довго короткострокової пам’яті) дана архітектура описана в [6-7].

В якості даних для дослідження було використано дані тестової моделі мережі IEEE з 14 шинами та 11 вузлами навантаження [8], даний набір використовують для дослідження ринків електроенергії P2P. Набір даних включає в себе дані навантаження споживачів, дені про сонячну та вітрову генерацію з Австралії за період за липня 2012 по червень 2013 з півгодинною дискретністю. Розрахунок втрат проводився на тестовій моделі мережі IEEE яка включала в себе 14 шин, 20 ліній, 8 джерел генерації які включають в себе 3 ВЕС, 2 СЕС, 2 газові електростанції та 1 вугільне електростанція. На рисунку 1 наведено схему тестової мережі IEEE.

В даному дослідженні ми розглядаємо лише прогноз навантаження для визначення втрат та прогнозування втрат електричної енергії, окремо без врахування прогнозних значень генерації. Також розрахунки проводились для усієї схеми, без розділення на окремі об'єднання.

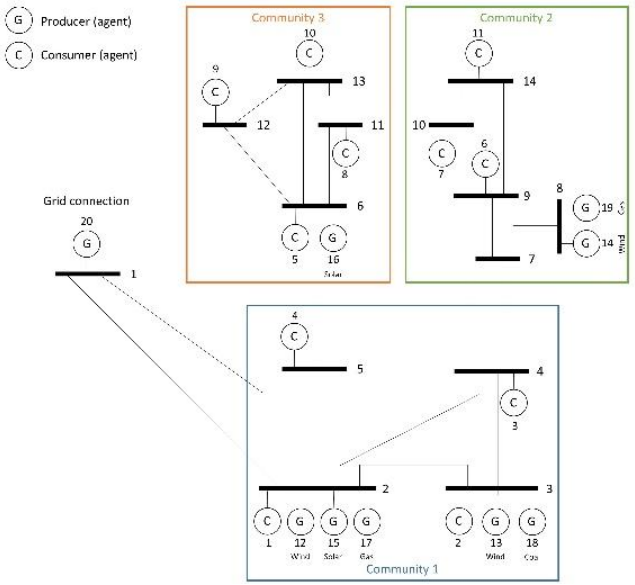


Рисунок 1 - Схема тестової мережі IEEE.

Дані про споживання були розділені на навчальну та тестову вибірки, навчальна вибірка включала в себе 9168 значення (тобто 191 день), а тестова вибірка включала в себе 336 значень (тобто 7 днів).

Для оцінки точності підходів до визначення значення втрат було використано дві функції середня абсолютна відсоткова похибка (MAPE) та середньоквадратична похибка (RMSE). В таблиці 1 наведено похибки прогнозування та розрахунку втрат електричної енергії.

Таблиця 1 – Результати дослідження

Вид прогнозу	MAPE, %	RMSE
Прогноз вузлового споживання (середнє значення)	42,2	0,17-2,95(1,19)
Прогноз втрат	2,47	0,12
Розрахунок втрат на прогнозних значеннях вузлового споживання	13,9	0,46

За результатами прогнозування видно, що прямий прогноз втрат електричної енергії демонструє меншу похибку MAPE та

середньоквадратичне відхилення RMSE у порівнянні із прогнозом вузлового навантаження та подальшого розрахунку втрат. Також з результатів можна зробити висновок що дана архітектура нейронної мережі краще підходить для прогнозування на даних у векторному вигляді.

Дане дослідження є частиною спільного Українсько-Литовського науково-дослідного проєкту «Smart Grid модель для оперативного керування розподільними мережами на основі методів штучного інтелект». В рамках продовження роботи буде покращено архітектуру нейронної мережі для прогнозування вузлового навантаження та генерації відновлювальних джерел енергії. А також дослідження стійкості мережі при роботі окремих об'єднань мережі.

[1] С.П. Денисюк, Р.Стшелецькі Формування складових інтелектуальної платформи керування енергетичними системами та мережами. Енергетика: економіка, технології, екологія. 2019. № 3. с. 7-22. DOI: https://doi.org/10.20535/1813-5420.3.2019.196368

[2] О.В. Кириленко, І.В. Блінов, С.П. Денисюк, Є.А. Зайцев, В.І, Висильченко. Впровадження базових міжнародних стандартів Smart Grid в україні: сучасний стан справ. Енергетика: економіка, технології, екологія. 2022. № 4. с. 44-53. DOI 10.20535/1813-5420.4.2022.273386

[3] Miroshnyk V., Shymaniuk P., Sychova V. Short term renewable energy forecasting with deep learning neural networks. Power Systems Research and Operation: Selected problems. editors: Kyrylenko O., Zharkin A. and other. Springer, 2021. pp. 121–142. DOI: https://doi.org/10.1007/978-3-030-82926-1_6.

[4] F.G.Y. Souhe, C.F. Mbey, A.T. Boum, P. Ele Forecasting of electrical energy consumption of households in a smart grid. Intern. Journ. of En. Econ. and Pol., 11(6), 221-233 (2021). https://doi.org/10.32479/ijeep.11761

[5] Shymaniuk P., Miroshnyk V., Blinov I., Estimation of electrical losses in the distribution network based on nodal electrical load forecasts. 2022 IEEE KhPI Week on Advanced Technology (KhPIWeek). 2022 pp. 1-4. DOI: 10.1109/KhPIWeek57572.2022.9916407.

[6] V. Miroshnyk, P. Chernenko, P. Shymaniuk Univariable short-term forecast of nodal electrical loads of energy systems. Tekhn. elektr., (2), 67-73 (2020). DOI: https://doi.org/10.15407/techned2020.02.067.

[7] Miroshnyk V., Shymaniuk P., Sychova V., Loskutov S. Short-term load forecasting in electrical networks and systems with artificial neural networks and taking into account additional factors. Power Systems Research and Operation: Selected problems II. editors: Kyrylenko O., Denysiuk S. and other. 2022. pp. 87-105. DOI: https://doi.org/10.1007/978-3-031-17554-1_5.

[8] The P2P-IEEE 14 bus system data set / T. Sousa et al. Zenodo. URL: https://zenodo.org/records/1220935 (date of access: 08.05.2025).

С.М. Петрушенко, А.О. Запорожець

ПІДХОДИ ДО ФУНКЦІОНУВАННЯ СИСТЕМИ КОНТРОЛЮ ВИТРАТ ГАЗУ

Метою дослідження є визначення принципів керування системи контролю витрат газу для забезпечення швидкого перекриття ділянок газопроводів у разі аварій та визначення критеріїв для активації системи перекриття газопроводів. З метою вирішення цієї задачі було використано методи статистичного аналізу даних, отриманих на основі даних щодо обсягів та характеристик споживання від декількох промислових підприємств, розташованих у різних містах України. Добові графіки споживання одного із підприємств, дані по споживанню для якого будуть використані у подальшому дослідженні, представлені на рис. 1.

Рисунок 1 – Добові обсяги споживання газу підприємства

З метою статистичного аналізу даних було використано середнє квадратичне відхилення (з метою оцінки рівномірності споживання та подальшого визначення діапазону допустимих значень обсягів споживання).

У наявних даних для цього підприємства прослідковується закономірність 5 через 2, що відповідає робочим та вихідним дням тижня. Як видно з наведеного графіків, починаючи із 02 жовтня починається суттєве збільшення обсягів спожитого газу, що дає підстави стверджувати, що після цієї дати підприємство починає використовувати газ для опалення. Для даних по цьому підприємству визначено: мінімальне, максимальне та середнє значення для двох періодів (до початку опалювального сезону та після його початку), середнє квадратичне відхилення обсягів споживання.

Так як основною функцією розроблюваної системи є перекриття трубопроводу під час аномального споживання, то для пошуку діапазону допустимих значень, при яких обсяги спожитого газу доволі сильно змінюються, взято діапазон з подвійним середнім квадратичним відхиленням (2σ) для виключення можливих нечастих аномалій, але з урахуванням природніх коливань. До початку опалювального сезону нижня межа

допустимих значень рівна нулю (оскільки на вихідних підприємство не споживає газ).

Запропоновано алгоритм ініціювання спрацьовування системи контролю газу, побудований на основі аналізу статистичних даних споживання підприємствами (рис. 2).

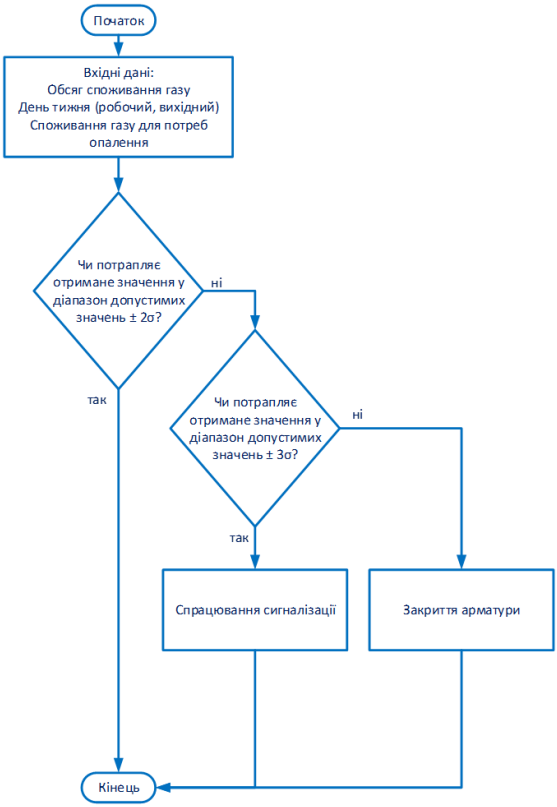


Рисунок 2 – Алгоритм визначення критеріїв для активації системи перекриття газопроводів

I.O. Dubovkina

ENERGY SAVING HYDRODYNAMIC TREATMENT OF LIQUID SOLUTIONS

Growing plants on hydroponics is the most common technology, which involves the rejection (or partial rejection) of the soil as the main environment where the root mass of the plant develops [1].

Aquatic solutions were used for experimentation investigations. Aquatic solutions gave in to processing by physical influence before the technological process of production. Aqua treatment and obtaining process was spent in the condition of the physical influence.

Liquid nutrient solutions such as double distilled water, irrigation water for drip irrigation systems, and solutions with fertilizes were used for processing. Spring barley “Myronivskyi 22” and vigorous triticale “Soncedar kharkivskyi” were used for testing growing crops.

Rotary-pulsed apparatus of the cylindrical type with clearances 120×10^{-6} m was used. The method of testing growing crops and method of optical microscopy were used.

Agriculture occupies 38% of the Earth’s surface and is the largest amount of land dedicated to a sole purpose[2].

For growing of spring barley “Myronivskyi 22” such parameters were selected: processing time - 30 s, processing frequency 5, angular velocity - 315 s^{-1}, impulses of pressure – 390 kPa. For growing of vigorous triticale “Soncedar kharkivskyi” selected parameters were: processing time - 15 s, processing frequency 1, angular velocity - 300 s^{-1}, impulses of pressure – 370 kPa.

The analysis of experimental data showed the effectiveness of using of alternating impulses of pressure for treatment of liquid nutrient solutions and media for hydroponic system.

The productivity of the growing agricultural crop of spring barley “Myronivskyi 22” increased by 32.8% and the productivity agricultural crop of vigorous triticale “Soncedar kharkivskyi” increased by 33.3%. Growth rate for spring barley increase by 20.5%, and for vigorous triticale increased by 22.7%.

A study of growing crops using irrigation water showed that as a result of using alternating pressure impulses for processing liquid nutrient solutions and media for a hydroponic system, the yield of the grown agricultural crop of spring barley "Mironovsky 22" increased by 33.3%, and the yield of the agricultural crop of vigorous triticale "Soncedar Kharkivskyi" increased by 33.5%. The growth rate of spring barley increased by 22.2% and of vigorous triticale by 24.4%.

The highest yield was obtained using a nutrient solution containing fertilizers. The highest growth rate of experimental crops was observed using irrigation water for drip irrigation systems.

The effects of analytical computation and mathematical modeling, statistical experiment have given the possibility to calculate basic design data of devices

which influence on intensification of carrying out of obtaining processes for aquatic mediums, and also processing for the purpose of change of physical and chemical parameters and structural transformations. The research studies demonstrated the increasing of the pH of the water prepared for the technology on the 15%.

The potential of hydrogen is shows concentration of free ions of hydrogen in water and water solutions and it is one of the major operational indicators of quality of water, in many compliments describes nature of chemical and another process which take place in water.

The nature and velocity of many physical and chemical processes which take place in such water systems changes.

The potential of hydrogen can greatly verify the velocity of itinerary of chemical reactions. Throughout processing of aquatic solutions and obtaining process in the conditions of linear speeds of the first rotor is 21,5 m/s and the second rotor is 23,5 m/s. The pressure of shift of a stream for the first rotor is 215 Pa and for the second rotor is 235 Pa.

The speeds of shift of a stream for the first rotor is $2{,}0 \times 10^5\ s^{-1}$ and for the second rotor is $2{,}5 \times 10^5\ s^{-1}$. The speed of rotary motion of the rotors is $n = 50\ sec^{-1}$. Through researches the potential of hydrogen of the aquatic solutions prepared on standard technology has raised on 15%. Employment the method of physical influence in technology of receiving of mediums allows receiving the activated aquatic solutions with the certain physical properties and parameters, assured value of a potential of hydrogen.

Carrying out of obtaining processes for mediums in continuous approach is giving the possibility to decrease reduction-oxidation potential on 25-55%.

The results of the experimental researches is established that using of no reagent methods of physical influence is of current interest and perspective for consciousness of control on physical and chemical parameters, properties and the structural organization for the purpose of an intensification of obtaining process of the aquatic solutions mediums.

Analysis of experimental data showed the effectiveness of using alternating pressure impulses for processing liquid nutrient solutions for hydroponic systems to increase the productivity of cultivated agricultural crops and the yield of green biomass.

[1] Chris Blok, Erik van Os, Raed Daoud, Laith Waked and Ala'a Hasan (2017). Hydroponic Green Farming Initiative: Increasing Water Use Efficiency by Use of Hydroponic Cultivation Methods in Jordan: Final Report, Wageningen University & Research, BU Greenhouse Horticulture, Report GTB-1447, p.26

[2] Foley J.A., Ramankutty N., Brauman K. A. (2011), Solutions for a cultivated planet, Nature, 478(7369), pp. 337–342, https://doi.org/10.1038/nature10452

А.В. Яцишин, С.І. Скуратівський, Є.В. Кочелаб, А.В. Сідельов, М.В. Чимбай

ОСОБЛИВОСТІ ХІМІЧНОГО ЗАБРУДНЕННЯ ДОВКІЛЛЯ В ПРОЦЕСІ ЕКСПЛУАТАЦІЇ АЕС

У процесі експлуатації атомних електростанцій (АЕС) виникає низка хімічних загроз для компонентів навколишнього природного середовища. До основних джерел такого впливу належать нерадіоактивні викиди в атмосферу, скиди у водні об'єкти та осадження забруднюючих речовин на ґрунтову поверхню, що супроводжують як технологічні, так і господарсько-побутові процеси. З огляду на складність виробничого циклу АЕС, ці джерела формують багатокомпонентні потоки забруднення, які включають оксиди азоту, сірки, важкі метали, органічні розчинники та кислотні залишки [1].

Джерелами хімічного впливу на навколишнє природне середовище є періодичні нерадіоактивні викиди і скиди, що виникають в об'єктах і спорудах на проммайданчику АЕС і мають в своєму складі хімічні елементи і речовини, граничний вміст яких регламентується діючими санітарними нормами і правилами.

В атмосферне повітря надходять газо-аерозольні нерадіоактивні викиди від допоміжних споруд і виробничих приміщень. Основні виробничі та технологічні процеси, які призводять до викиду забруднюючих речовин і основні шкідливі компоненти у складі цих викидів наведені в табл. 1 [2, 3 та ін.].

Таблиця 1 – Основні виробничі та технологічні процеси, які призводять до викиду забруднюючих речовин і основні шкідливі компоненти у складі цих викидів

Основні виробничі та технологічні процеси	Режим роботи	Основні шкідливі компоненти викидів
Процеси спалювання в стаціонарних двигунах. (Пуско-резервна котельня)	Знаходження у резерві Аварійний	NO_x, SO_2, CO, CO_2, V_2O_5, метан, сажа
Масломазутогосподарство	Періодично	НМЛОС
Безконтактні технологічні печі. (Дизель-генераторні станції)	Періодично	NO_x, CO, SO_2, вуглеводні, сажа
Зварювання металів	Періодично	NO_x, SO_2, CO, залізо та його сполуки, манган та його сполуки, нікель та його сполуки, фториди, кремнію двоокис аморфний

Основні виробничі та технологічні процеси	Режим роботи	Основні шкідливі компоненти викидів
Механічна обробка металу	Періодично	Пил абразивно-металевий, пил металевий, масло нафтове мінеральне, НМЛОС
Ремонтно-будівельні роботи	Періодично	Пил деревини, кальцію оксид, NO_x, SO_2, CO, сажа
Очистка стічних вод у промисловості. Розміщення осаду стічних вод	Постійно	Аміак, сірководень
Транспортний цех. Ремонт та фарбування автомобілів. Транспортування, зберігання та розподіл рідкого палива	Періодично	NO_x, SO_2, CO, сажа, НМЛОС (толуол, етанол, ацетон, бензин та ін.), кислота сірчана
Будівельно-монтажні роботи	Періодично	CO, NO_x, пил деревини, НМЛОС, залізо та його сполуки, манган та його сполуки, нікель та його сполуки, фториди, кремнію двоокис аморфний, пил неорганічний з вмістом SiO_2
Зберігання неорганічних хімічних продуктів	Постійно	Гідразін гідрат, морфолін, азотна кислота, сірчана кислота, хлор
Виробництво хлору	Постійно	Водню хлорид, хлор

В процесі виробничої діяльності АЕС атмосферне повітря забруднюється також викидами від пересувних джерел: автотранспорт, залізничний транспорт, річковий транспорт та інші механізми.

Більша частина АЕС світу у процесі своєї роботи для охолодження конденсаторів турбін використовує воду спеціально споруджених для цих цілей ставків-охолоджувачів. Інша частина використовує для цього оборотну воду, яка охолоджується градирнями.

В результаті виробничої та господарсько-побутової діяльності на АЕС утворюються стічні води, в яких містяться різні шкідливі речовини (нафтопродукти, сульфати, хлориди, нітрати, фосфати тощо). Після очищення на відповідних очисних спорудах АЕС ці стічні води скидаються у ставок-охолоджувач для повторного використання. Але через недосконаліть очисного обладнання у стічній воді залишаються шкідливі речовини, що спричиняє забруднення ставка-охолоджувача небезпечними хімічними, біологічними та іншими сполуками. Дослідження, проведені на прикладі

Чорнобильської АЕС, показали, що навіть після очищення стічні води можуть містити залишкові концентрації шкідливих речовин, які накопичуються у ставках-охолоджувачах, спричиняючи їх забруднення [4].

Якість води ставка-охолоджувача формується за рахунок скидання у нього стоків: підживлення ставка-охолоджувача. Для підживлення ставка-охолоджувача використовується вода скидного каналу, яка найбільшою мірою впливає на хімічний склад його води. Також в ставок охолоджувач скидаються різні дебалансні води.

Хімічний вплив на ґрунти від експлуатації АЕС здійснюється шляхом осадження та відповідної подальшої міграції забруднюючих речовин, викинутих стаціонарними та пересувними джерелами забруднення в атмосферне повітря, а також шляхом потрапляння забруднених вод на ґрунт.

Таким чином, функціонування АЕС здійснює вплив на навколишнє природне середовище викидами в атмосферу від стаціонарних джерел – пускова резервна котельня, дизель генератори станції та інші допоміжні виробництва та обладнання (масло-мазутне-дизельне господарство, зварювальні дільниці, дільниці механічної обробки металу і т.д.), так і пересувних джерел – автотранспорт, залізничний транспорт та інші механізми; скидами у поверхневі водні об’єкти забруднених вод виробничої та господарсько-побутової діяльності АЕС. Крім того, контроль за нерадіаційними факторами дозволяє виявити ознаки підготовки терористичних актів в зоні, яка прилягає до АЕС.

[1] Soto, G. H., & Martinez-Cobas, X. (2024). Nuclear energy generation’s impact on the CO2 emissions and ecological footprint among European Union countries. Science of The Total Environment, 945, 173844. https://doi.org/10.1016/j.scitotenv.2024.173844

[2] Тарнавський, А. Б., Сукач, Р. Ю., & Сукач, Ю. Г. (2014). Техногенна безпека АЕС: Навчальний посібник (Ч. 1, 371 с.). Державна служба України з надзвичайних ситуацій, Львівський державний університет безпеки життєдіяльності.

[3] Попов, О. О. (2014). Вплив АЕС на екологічну безпеку прилеглих територій. Збірник наукових праць Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України, (70), 11–20.

[4] Sato, H., Gusyev, M., Veremenko, D., Laptev, G., Shibasaki, N., Onda, Y., Zheleznyak, M., Kirieiev, S., & Nanba, K. (2023). Evaluating changes in radionuclide concentrations and groundwater levels before and after the cooling pond drawdown in the Chornobyl Nuclear Power Plant vicinity. Science of The Total Environment, 872, 161997. https://doi.org/10.1016/j.scitotenv.2023.161997

О.О. Попов, М.Л. Миронцов, А.М. Лагойко,
О.О. Вовк, О.В. Фаррахов, Є.В. Пилипчук

ПРО ВИКОРИСТАННЯ ГЕОХІМІЧНИХ МЕТОДІВ ДЛЯ ВИЯВЛЕННЯ СКУПЧЕНЬ ВОДНЮ В ПІДЗЕМНИХ ПОКЛАДАХ

У контексті глобального пошуку екологічно чистих джерел енергії природний водень розглядається як перспективна альтернатива викопному паливу. Завдяки високій енергетичній щільності, відсутності вуглецевого сліду при згорянні та поширеності в надрах планети, водень привертає дедалі більшу увагу вчених. Одним з ключових інструментів його пошуку є геохімічні методи, які дозволяють безпосередньо виявляти і аналізувати наявність водню в приповерхневому середовищі та глибших горизонтах.

Геохімічна розвідка передбачає відбір газів із ґрунтів, свердловин або порід з подальшим аналізом їхнього складу. Основними компонентами для дослідження є водень (H_2), гелій (He), метан (CH_4), вуглекислий газ (CO_2), азот (N_2) та ізотопні співвідношення. Високі концентрації водню в ґрунтовому повітрі або порових водах можуть свідчити про вертикальну міграцію з підземних резервуарів. Наприклад, дослідження в Австралії [1] зафіксували вміст водню до 2,7% у зразках, відібраних у зонах субциркулярних депресій, які, ймовірно, є поверхневими проявами глибоких витоків газу (рис. 1).

Окрім концентраційного аналізу, застосовують вимірювання флюксу – швидкості виділення газу з ґрунту. Для цього використовують камери накопичення та портативні газоаналізатори, які дають змогу фіксувати зміни концентрацій у реальному часі. Цей підхід є ефективним для локалізації активних зон дегазації, особливо в районах тектонічної активності або в зонах розломів.

Надзвичайно важливою складовою є ізотопний аналіз, який дозволяє встановити походження газу – біогенне чи абіогенне. Наприклад, співвідношення $^3He/^4He$ може вказувати на мантійне джерело гелію, тоді як ізотопи водню δ^2H – на його утворення внаслідок серпентинізації, радіолізу або мікробіологічних процесів. Аналіз супутніх газів (CH_4, H_2S) також дозволяє зрозуміти геохімічне середовище утворення водню та виявити можливе мікробне споживання газу в поверхневих шарах.

Геохімічні дослідження активно використовуються в міжнародній практиці (Франція, Канада, Австралія, Малі) і доповнюються геофізичними та ізотопними методами.

Особливо показовим є приклад родовища Буракебугу в Малі, де виявлено промислові концентрації водню і підтверджені як сейсмічними, так і геохімічними методами [2].

Попри високу інформативність, геохімічні методи мають ряд обмежень:

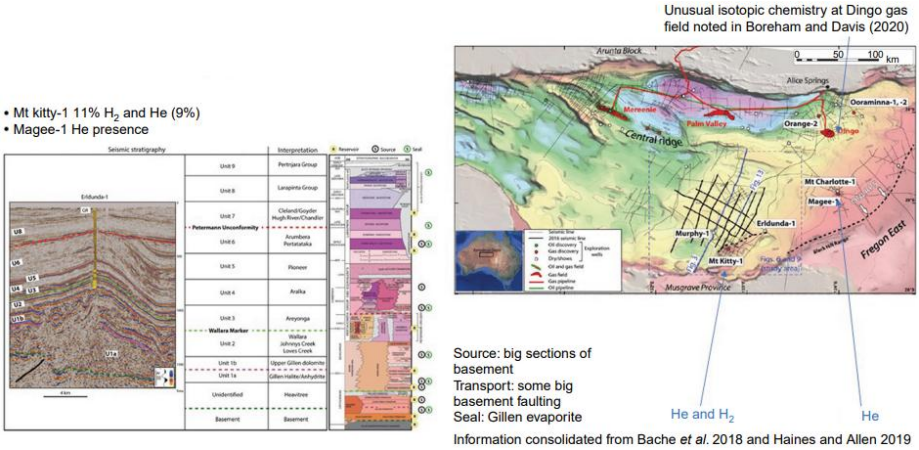


Рисунок 1 – Стратиграфічні, сейсмологічні та геохімічні дані, що підтверджують наявність природного водню (H_2) та гелію (He) в Австралії [1]

– потреба у спеціалізованих протоколах під час відбору та аналізу (зокрема, уникнення використання H_2 або He як газів-носіїв у хроматографії);

– локальність та точковість досліджень, що вимагає множинного буріння для репрезентативного охоплення;

– споживання водню мікроорганізмами (наприклад, сульфатредукуючими бактеріями), що ускладнює інтерпретацію отриманих даних.

Останні дослідження також наголошують на потребі мультидисциплінарного підходу, що передбачає поєднання геохімічних, геофізичних і мікробіологічних даних, а також вдосконалення інструментів відбору, автоматизацію аналізів і довготривалий моніторинг.

У порівнянні з іншими методами геохімічний аналіз: надає прямі підтвердження наявності водню; на відміну від геофізики, орієнтований не на структури, а на газовий склад і хімічні процеси; у порівнянні з мікробіологією – швидший та аналітично точніший щодо концентрації газу.

Таким чином, геохімічний аналіз залишається ключовим методом для первинного виявлення водню, оцінки його походження та визначення активних зон просочування. Для комплексної оцінки ресурсів доцільно інтегрувати його з геофізичними й біогеохімічними дослідженнями.

[1] Maiga, O., Deville, E., Laval, J., Prinzhofer, A., & Diallo, A. B. (2024). Trapping processes of large volumes of natural hydrogen in the subsurface: The emblematic case of the Bourakebougou H2 field in Mali. International Journal of Hydrogen Energy, 50, 640–647. https://doi.org/10.1016/j.ijhydene.2023.10.131

[2] Gluyas, J., Randle, C. H., & Sepulveda, F. (2023). Hydrogen soil gas surveys across Australian sub-circular depressions. International Journal of Hydrogen Energy, 48(15), 5762–5774. https://doi.org/10.1016/j.ijhydene.2022.12.135

К.М. Стародубець, В.О. Ковач, В.О. Куценко, А.М. Лагойко

ПРО НЕОБХІДНІСТЬ РОЗРОБЛЕННЯ ПРОГРАМНО-МЕТОДИЧНОГО ЗАБЕЗПЕЧЕННЯ МОНІТОРИНГУ РАДОНУ В ҐРУНТАХ ДЛЯ МІНІМІЗАЦІЇ РАДІАЦІЙНОГО ВПЛИВУ ПРИ БУДІВНИЦТВІ ІНФРАСТРУКТУРНИХ ОБ'ЄКТІВ

Радон (^{222}Rn) є природним газом, що утворюється в результаті радіоактивного розпаду урану та торію, які містяться в земній корі. Він присутній у всіх регіонах Землі, однак його концентрація змінюється залежно від місцевих геологічних, геоморфологічних, гідрогеологічних і кліматичних умов. Завдяки наявності тріщин, щілин і пор у гірських породах та ґрунтовому покриві, радон має здатність вивільнятися (еманувати) з земної поверхні. Проникаючи через дефекти фундаменту та пористу структуру будівельних матеріалів, він може накопичуватися у внутрішніх просторах інфраструктурних об'єктів, формуючи підвищений радіаційний ризик для здоров'я населення.

За даними Всесвітньої організації охорони здоров'я довготривалий вплив високих концентрацій ^{222}Rn є другою основною причиною раку легень після тютюнопаління. В Україні, з огляду на її геологічну будову та попередньо проведені дослідження, радононебезпечною можна вважати 40 % території країни. Найвищі рівні природного радонового фону спостерігаються в регіонах, розташованих у межах Українського кристалічного щита, де переважають урановмісні породи. За приблизними оцінками сумарний збиток від ^{222}Rn у повітрі приміщень інфраструктурних об'єктів для України щороку сягає 1–1,5 млрд грн на рік, сюди включені: витрати на лікування радон-індукованих захворювань (зокрема раку легенів); економічні збитки від втрати працездатності; вартість впровадження заходів протирадонового захисту на об'єктах після їхнього будівництва. Попри масштаби проблеми, радонове опромінення в Україні фактично не регулюється на законодавчому рівні. Відсутні чітко визначені: критерії оцінки радононебезпечності територій; вимоги до моніторингу, методів вимірювання, інтерпретації результатів; протоколи забезпечення якості та точності вимірювань; єдині бази даних та радіоекологічне картування території. Затверджена наказом МОЗ України від 13.10.2023 № 1786 «Методика проведення моніторингу радону» [1] в значній мірі присвячена обстеженню повітря інфраструктурних об'єктів та визначення їх радононебезпечності. Що стосується моніторингу ^{222}Rn в ґрунтах, то даний нормативний документ містить лише основні принципи вимірювання в ґрунтовому повітрі та має наступні основні недоліки: не враховані фактори, що впливають на геометрію вимірювання; наявна невизначеність у врахуванні геологічних особливостей території; не враховано вплив сезонних та кліматичних змін; не враховується вплив температури та вологості ґрунту при вимірюваннях; наявні обмеження за часом вимірювання, що може

негативно вплинути на точність результатів; відсутнє поняття радонового індексу в ґрунтах; відсутні детальні рекомендації по періодичності моніторингу. Наявність зазначених обмежень не дозволяє забезпечити високу точність, повноту та достовірність інформації про рівні й просторовий розподіл радону в ґрунтах досліджуваних територій. Це, у свою чергу, перешкоджає ефективному управлінню радоновими ризиками та призводить до суттєвих соціально-економічних збитків, зокрема у сфері будівництва інфраструктурних об'єктів. З огляду на це, актуальним завданням для України є розробка сучасного програмно-методичного забезпечення для моніторингу радону в ґрунтах, яке б відповідало європейським стандартам та практикам. Розробка сучасного програмно-методичного забезпечення для моніторингу радону в ґрунтах дозволить реалізувати пріоритетні завдання «Плану заходів щодо зниження рівня опромінення населення радоном та продуктами його розпаду, мінімізувати довгострокові ризики від поширення радону в житлових та нежитлових будівлях, на робочих місцях», затвердженого розпорядженням КМУ від 27.11.2019 № 1417-р [2] з метою імплементації Директиви Ради 2013/59/Євратом.

Програмно-методичне забезпечення моніторингу радону в ґрунтах має відповідати європейським вимогам та стандартам, що дозволить забезпечити своєчасне прийняття рішень стосовно: необхідності запровадження протирадонових заходів на досліджуваній території; зниження рівня опромінення населення радоном; мінімізації довгострокових ризиків від поширення радону в приміщеннях об'єктів житлово-комунального господарства, призначених для тимчасового або постійного перебування населення. Це дасть можливість в подальшому уникнути значних соціально-економічних збитків при будівництві інфраструктурних об'єктів в Україні, що є надзвичайно актуальним з огляду на сучасні світові економічні та екологічні виклики.

[1] Наказ МОЗ України від 13.10.2023 № 1786 «Про затвердження Порядку проведення моніторингу радону в Україні та нотифікації про радіаційні ризики і Методики проведення моніторингу радону». https://zakon.rada.gov.ua/laws/show/z1874-23#Text

[2] Розпорядження КМУ від 27.11.2019 № 1417-р «Про затвердження плану заходів щодо зниження рівня опромінення населення радоном та продуктами його розпаду, мінімізації довгострокових ризиків від поширення радону в житлових та нежитлових будівлях, на робочих місцях на 2020-2024 роки». https://zakon.rada.gov.ua/laws/show/1417-2019-%D1%80#Text

В.О. Ковач, Є.В. Пилипчук, Т.М. Яцишин, В.О. Артемчук, В.О. Куценко

НАТУРАЛЬНА ШКІРА ЯК НОСІЙ РАДІОЗАХИСНИХ КОМПОЗИТНИХ МАТЕРІАЛІВ

Протягом останніх років виріс попит на нетоксичні, економічно конкурентоспроможні та легкі матеріали, які використовуються у радіаційних технологіях різного призначення. Це, в свою чергу, обумовило появу нових полімерних композитів, для створення яких використовують безпечні речовини та екологічно чисті матеріали, тобто такі, що є біосумісними та здійснюють мінімальний вплив на навколишнє природне середовище при використанні та утилізації.

Одним із перспективних рішень у цьому контексті є композити на основі натуральної шкіри, яка поєднує механічну міцність із функціональною здатністю до зв'язування активних радіозахисних компонентів.

Нещодавно появилися наукові роботи, в яких представлені дослідження щодо потенціалу природних композитів на основі шкіри для захисту від радіації. Натуральна шкіра – це полімер, який використовується для виготовлення придатних для носіння виробів для захисту від радіації. Натуральна шкіра містить різні функціональні групи, такі як –OH, − COOH, − CONH2 та –NH2. Натуральна шкіра, завдяки своїй унікальній структурі та хімічним властивостям, слугує ефективною основою для іммобілізації функціональних наповнювачів, що значно підвищують радіозахисні характеристики матеріалу. Крім того, натуральна шкіра має тривимірну волокнисту тканину мережу, яка забезпечує високу пористість, чудову міцність на розрив і розтягування, а також сприяє стабільній інтеграції та рівномірному розподілу наповнювачів. Перелічені властивості роблять матеріал ідеальною матрицею для захисту від радіації [1].

Для досягнення ширшого діапазону захисту від рентгенівського випромінювання авторами [2] продемонстровано новий підхід до виготовлення композиційних матеріалів на основі натуральної шкіри (рис. 1). Це досягалося шляхом імпрегнування наночастинок Bi_2O_3 і La_2O_3 у матриці. Даний підхід дав можливість значно покращити фотоелектричний ефект і підвищити здатність матеріалу до ослаблення рентгенівського випромінювання. Додавання додаткового покриття Bi_2O_3 на нижню частину матеріалу зменшило небажане вторинне випромінювання.

В роботі [3] запропонована нова стратегія "impregnation–desolvation" для легкого приготування композитів, що екранують рентгенівське випромінювання. Також розроблено композити на основі натуральної шкіри, які наповнені йодом і вісмутом для ослаблення рентгенівського випромінювання. Частинки вісмуту та йоду зв'язувалися з різними групами в натуральній шкірі шляхом координації та утворення водневих зв'язків. Завдяки цьому Bi і I можуть залишатися стабільними та однорідно розсіюватися всередині матриці натуральної шкіри.

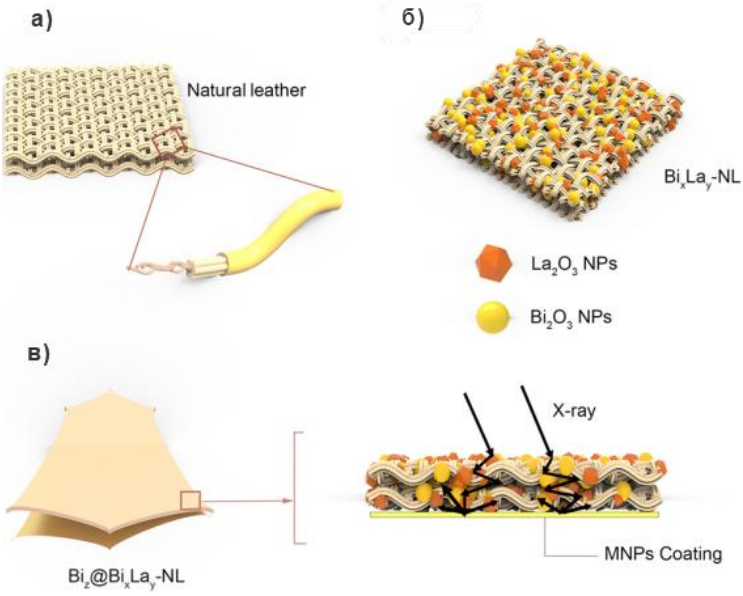


Рисунок 1 – Ієрархічна структурна схема натуральної шкіри (NL) *(а)*; *б)* діаграма Bi_xLa_y–NL; *в)* схема екранування рентгенівського випромінювання $Bi_z@Bi_xLa_y$–NL [2]

Здійснений аналіз показує про високу ефективність використання натуральної шкіри як матриці для створення композитів, здатних екранувати рентгенівське та гамма-випромінювання. Завдяки наявності функціональних груп і тривимірній структурі шкіра забезпечує рівномірний розподіл радіозахисних компонентів, що дозволяє створювати гнучкі, легкі та біосумісні матеріали з підвищеними захисними властивостями.

[1] Chang, Q., Guo, S., & Zhang, X. (2023). Radiation shielding polymer composites: Ray-interaction mechanism, structural design, manufacture and biomedical applications. Materials & Design, 233, 112253. https://doi.org/10.1016/j.matdes.2023.112253

[2] Li, Q., Zhong, R., Xiao, X., Liao, J., Liao, X., & Shi, B. (2020). Lightweight and Flexible Bi@Bi-La Natural Leather Composites with Superb X-ray Radiation Shielding Performance and Low Secondary Radiation. ACS Applied Materials & Interfaces, 12(48), 54117–54126. https://doi.org/10.1021/acsami.0c17008

[3] Wang, Y., Ding, P., Xu, H., Li, Q., Guo, J., Liao, X., & Shi, B. (2020). Advanced X-ray Shielding Materials Enabled by the Coordination of Well-Dispersed High Atomic Number Elements in Natural Leather. ACS Applied Materials & Interfaces, 12(17), 19916–19926. https://doi.org/10.1021/acsami.0c01663

Т.В. Підгаєцький

ПІДВИЩЕННЯ НАДІЙНОСТІ ЕЛЕКТРОГЕНЕРАЦІЇ ЕНЕРГОБЛОКІВ АЕС В УМОВАХ СЕЙСМІЧНИХ ВПЛИВІВ

Ядерна енергетика та атомно-промисловий комплекс України є найвагомішими складовими економічної, енергетичної та екологічної безпеки нашої держави. Надійне функціонування ядерної галузі є основним фактором стабільності роботи об'єднаної української енергосистеми.

Надійність електрогенерації на енергоблоках атомних електростанцій (далі – АЕС) України обумовлена передусім безаварійною та ефективною експлуатацією обладнання та систем, які приймають участь у виробленні електроенергії, як при умовах нормальної експлуатації, так і в умовах екстремальних зовнішніх впливів, до яких зокрема відносяться вібраційні та сейсмічні впливи.

Нормативно-правова база України щодо регулювання ядерної та радіаційної безпеки атомних станцій встановлює вимоги не лише до обладнання важливого для безпеки АЕС, а також і до обладнання, яке не впливає на безпеку, проте відмова якого окремо або в сукупності з іншими системами й елементами може призвести до перерви у виробленні електроенергії. Зокрема, НП 306.2.208-2016 [[1]] для такого обладнання встановлює вимоги щодо стійкості до сейсмічних впливів рівня проектного землетрусу.

Серед усього обладнання АЕС особлива увага приділяється сейсмостійкому проектуванню обладнання та конструкцій, які, крім сейсмічних навантажень під час землетрусу, піддаються також додатковим навантаженням. Надійність експлуатації, наприклад, тонкостінних резервуарів з рідиною обґрунтовується з урахуванням гідродинамічних впливів при сейсмічних коливаннях рідини, оскільки наявність рідини призводить до зміни власних частот та форм коливань конструкцій, додаткового динамічного впливу на їх стінки та днище.

На цей час на АЕС України експлуатується значна кількість обладнання, яке згідно НП 306.2.208-2016 повинно бути стійкім до сейсмічних навантажень, але яке згідно НП 306.2.245-2024 [[2]] визначено як таке, що не впливає на безпеку АЕС, що призвело до відсутності вимог щодо проведення робіт з переоцінки сейсмічної стійкості цього обладнання після зміни сейсмічних характеристик майданчика АЕС, врахованих при проектуванні енергоблоків АЕС, за результатами даних сейсмічного моніторингу.

Основною метою дослідження є підвищення надійності електрогенерації на енергоблоках АЕС України. Зокрема, мова йде про аналіз обладнання, що є найбільш уразливим до проєктних екстремальних зовнішніх впливів [1], з подальшим формуванням рекомендацій і розробкою технічних заходів щодо підвищення його стійкості. Кінцева мета – зменшення тривалості ймовірного недовироблення електроенергії після виникнення таких впливів.

Для досягнення цієї мети було попередньо сформовано перелік обладнання, яке не належить до систем безпеки за [2], але є критично важливим для безперервної генерації електроенергії. Кількість такого обладнання – близько трьох тисяч одиниць, залежно від модифікації енергоблоку. За результатами проведеної оцінки наявності чи відсутності попередніх робіт експлуатуючої організації АТ «НАЕК «Енергоатом» щодо оцінки стійкості зазначеного обладнання до екстремальних зовнішніх впливів, близько 35% одиниць обладнання було вилучено з подальшого аналізу – переважно це нове або модернізоване обладнання, що постачалося з підтвердженою стійкістю.

Для вибору типопредставників обладнання була розроблена адаптована поетапна процедура, яка дозволяє враховувати ключовий аспект — вплив втрати стійкості окремого обладнання на загальне недовироблення електроенергії енергоблоком. Запропонована процедура починається з аналізу масо-габаритних критеріїв. Далі оцінюються вихідні дані та рівні впливів на обране обладнання, а фінальним етапом є врахування економічних критеріїв, зокрема тривалості у виробленні електроенергії. Особлива увага приділяється просторовому позиціонуванню, формі перерізу та наявності внутрішньокорпусних елементів у конструкціях тепломеханічного обладнання, що працює під тиском. Ці параметри є ключовими для визначення модальних характеристик системи «бак + рідина». Геометричні розміри обладнання безпосередньо впливають на рівень напружень у конструкціях. Зокрема, пошкодження великогабаритного обладнання, що працює під тиском, може призвести до тривалих простоїв і затримки відновлення електрогенерації. Додатково враховується тип і параметри робочого середовища, що визначають здатність обладнання витримувати сейсмічні впливи.

Наразі основна увага зосереджена на ідентифікації типопредставників обладнання з найбільшим потенційним часом на відновлення або заміну. Також визначається обладнання, яке не може бути замінене в разі виходу з ладу через відсутність його аналогів на світовому ринку. Особливо це стосується елементів, виготовлених у країні-агресорі, які в умовах війни стали недоступними.

[1] НП 306.2.208-2016 Вимоги до сейсмостійкого проектування та оцінки сейсмічної безпеки енергоблоків атомних станцій НП 306.2.234-2023
[2] НП 306.2.245-2024 Загальні положення безпеки атомних станцій

В.В. Шкарупило, В.В. Душеба, Т.А. Зайко, В.В. Шкарупило

ІЄРАРХІЧНИЙ ПІДХІД ДО ВАРІЮВАННЯ РІВНЯ ДЕТАЛІЗАЦІЇ ФОРМАЛЬНИХ СПЕЦИФІКАЦІЙ

Актуальні праці, у яких висвітлюється предметна область аналізу і дослідження обчислювальних витрат, супутніх проведенню верифікації формальних специфікацій (ФС) в автоматизованому режимі на основі залучення представників сімейства методів перевірки на моделі, є наочними демонстраціями прояву відомого ефекту експоненційного зростання простору станів систем переходів, що при цьому будуються і опрацьовуються [1–4]. Існуючі напрацювання у частині стримування означеного ефекту істотно різняться за концептуальною складовою: це і декомпозиція ФС [5], і залучення бінарних діаграм рішень ROBDDs (Reduced Ordered Binary Decision Diagrams) у межах техніки символьної перевірки на моделі SMC (Symbolic Model Checking) [6]. Відповідний інструментарій NuSMV, що охоплює програмні реалізації діаграм ROBDDs і техніки SMC, вже було успішно застосовано при вирішенні критичних задач, що постають, наприклад, перед енергетикою Фінляндії [7].

Представлений у межах праці ієрархічний підхід базується на альтернативній концепції, що полягає у наступному: проведенні стратифікації на рівні формалізованих конструкцій, з яких формується ФС; залученні математично строгих модульних виразних засобів, що забезпечують однозначність інтерпретації змістового навантаження ФС. Стосовно останньої позиції вибір було зупинено на виразних засобах темпоральної логіки дій TLA (Temporal Logic of Actions) Л. Лемпорта [8]: алгоритмічній мові PlusCal, що дозволяє попередньо формалізувати архітектурну складову (структуру і зв’язки) в основі створюваної ФС [9]; мові TLA+ як засобу формалізації змістового навантаження і безпосередньо подання результуючої ФС [10].

У межах підходу залучено основоположне поняття логіки TLA – поняття «дії». Воно полягає у формалізації переходу між суміжними станами системи переходів, що будується у процесі верифікації ФС методом перевірки на моделі. У якості останнього прийнято рішення застосовувати поширений метод TLC (TLA Checker). Серед показових критичних сценаріїв застосування методу – контроль несуперечливості артефактів, використовуваних при проєктуванні операційної системи реального часу OpenComRTOS [11]. Вказаний метод також було успішно застосовано у частині контролю несуперечливості рольової моделі стосовно процесу оновлення ідентифікаційних кодів учасників європейського ринку електричної енергії [3], що вбачається значимим аспектом у контексті синхронізації об’єднаної енергетичної системи України з європейською інфраструктурою ENTSO-E, яка відбулась 28 листопада 2023 р. [12].

Дослідження проведено у відповідності до задач, вирішуваних у межах НДР 0125U000326 «Розвинення теоретичних засад формалізації подань процесів опрацювання оперативної інформації в енергетиці», виконуваної Інститутом проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України.

[1] Шкарупило, В. В., Душеба, В. В., Зайко, Т. А., Шкарупило, В. В., & Скрупський, С.Ю. (2024). Індуктивний підхід до побудови формалізованих подань програмно-алгоритмічного забезпечення при проєктуванні. Вчені записки Таврійського національного університету імені В.І.Вернадського, серія «Технічні науки», 35(74), 4, 224–229. https://doi.org/10.32782/2663-5941/2024.4/33

[2] Clarke, E. M., Grumberg, O., Kroening, D., Peled, D., & Veith, H. (2018). Model checking (2nd ed.). The MIT Press.

[3] Shkarupylo, V., Blinov, I., Dusheba, V., & Alsayaydeh, J. A. J. (2023). Case driven TLC model checker analysis in energy scenario. CEUR Workshop Proceedings, 3392, 65–75. https://doi.org/10.32782/cmis/3392-6

[4] Шкарупило, В. В., Чемерис, О. А., Душеба, В. В. (2020). Оцінювання просторової складності задачі формальної верифікації, вирішуваної методом перевірки на моделі. Вчені записки Таврійського національного університету імені В.І.Вернадського, серія «Технічні науки», 31(70), 5, 147–151. https://doi.org/10.32838/2663-5941/2020.5/24

[5] Kraibi, K., Ben Ayed, R., Rehm, J., Collart-Dutilleul, S., Bon, P., & Petit, D. (2019). Event-B decomposition analysis for systems behavior modeling. Proc. 14th International Conference on Software Technologies, ICSOFT 2019, Prague, Czech Republic, 1 (P. 278–286). https://doi.org/10.5220/0007929602780286

[6] He, L., Liu, G., & Zhou, M. (2023). Petri-Net-Based Model Checking for Privacy-Critical Multiagent Systems. IEEE Transactions on Computational Social Systems, 10(2), 563–576. http://doi.org/10.1109/TCSS.2022.3164052

[7] Pakonen, A. (2021). Model-checking I&C logics – insights from over a decade of projects in Finland. Proc. 12th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies, NPIC&HMIT 2021. American Nuclear Society (ANS), (P. 792–801). https://doi.org/10.13182/T124-34322

[8] Lamport, L. (2002). Specifying systems: The TLA+ language and tools for hardware and software engineers. Addison-Wesley Longman Publishing Co., Inc.

[9] Lamport, L. (2009). The PlusCal algorithm language / M. Leucker, & C. Morgan (Eds.), Theoretical Aspects of Computing – ICTAC 2009. ICTAC 2009. Lecture Notes in Computer Science (P. 36–60), 5684. Springer. https://doi.org/10.1007/978-3-642-03466-4_2

[10] Kim, Y.-M. & Kang, M. (2020). Formal verification of SDN-based firewalls by using TLA+. IEEE Access, 8, 52100–52112. https://doi.org/10.1109/ACCESS.2020.2979894

[11] Verhulst, E., Boute, R. T., Faria, J. M. S., Sputh, B. H. C., & Mezhuyev, V. (2011). Formal development of a network-centric RTOS: software engineering for reliable embedded systems. Springer Publishing Company, Inc.

[12] USAID. (2023, December 5). The Ukrainian energy system is synchronized with the European network. https://energysecurityua.org/news/the-ukrainian-energy-system-finalized-synchronization-with-the-european-network/

О.С. Потенко

ВПЛИВ ФУНКЦІОНАЛЬНОГО ПРИЗНАЧЕННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ НА ФОРМУВАННЯ ПРОФІЛЮ ЇЇ ЗАХИЩЕНОСТІ У РАМКАХ МУЛЬТИКРИТЕРІАЛЬНОГО ПІДХОДУ

Розробка критеріїв оцінки інформаційної безпеки є важливим етапом у забезпеченні захисту даних та інформаційних систем у сучасному світі, де виникають нові загрози та виклики. Потреба у створенні таких критеріїв обумовлена низкою факторів, серед яких найголовнішими є необхідність впровадження системного підходу до виявлення вразливостей і загроз, аналізу ризиків та оптимального розподілу ресурсів для мінімізації потенційних втрат. Тільки точна оцінка стану безпеки дозволяє виявити слабкі місця в інфраструктурі, правильно вибрати ефективні засоби захисту та оперативно реагувати на можливі інциденти.

Запропонований мультикритеріальний підхід [1] складається з чотирьох взаємозалежних компонентів, що дозволяє точно визначити необхідний рівень захисту інформації. Процес оцінки безпеки починається з оцінки ризиків, яка полягає в аналізі ймовірності виникнення загроз та їх потенційних наслідків для інформаційних ресурсів. Цей етап дозволяє визначити, які загрози є найбільш критичними і потребують особливої уваги для мінімізації їхнього впливу.

Важливим етапом є вибір рівня захищеності, який залежить від призначення автоматизованих систем. Згідно з НД ТЗІ 2.5-005-99 [2] (Рис.1), існує чотири можливі варіанти:

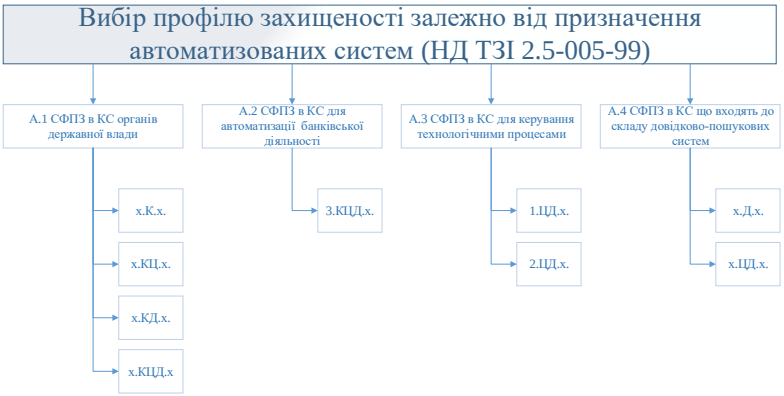


Рисунок 1 – Вибір профілю захищеності залежно від призначення автоматизованих систем

А.1 СФПЗ в КС органів державної влади

А.2 СФПЗ в КС для автоматизації банківської діяльності

А.3 СФПЗ в КС для керування технологічними процесами

А.4 СФПЗ в КС що входять до складу довідково-пошукових систем

У разі використання [2] автоматизованих систем, призначених для автоматизації діяльності органів державної влади, рекомендується вибір профілів х.К.х. Якщо, крім вимоги забезпечення конфіденційності, існують додаткові вимоги до забезпечення цілісності та/або доступності інформації, то доцільно використовувати профілі х.КЦ.х., КД.Х., х.КЦД.х.

Для автоматизованих систем, що входять до складу систем, призначених для автоматизації банківської діяльності, рекомендується вибір профілю 3.КЦД.х.

У разі використання автоматизованих систем для керування технологічними процесами рекомендується застосовувати профілі 1.ЦД.х., 2.ЦД.х.

Для автоматизованих систем, що входять до складу довідково-пошукових систем, рекомендується вибір профілів х.Д.х., х.ЦД.х.

Далі на вимоги НД ТЗІ 2.5-005-99 необхідно накласти вектор виду інформаційної діяльності, що в фіналі дозволить сформувати загальний функціональній профіль захищеності.

Призначення автоматизованих систем (АС) має важливий вплив на вибір профілю захищеності в мультикритеріальному підході, оскільки різні типи систем потребують різних рівнів захисту в залежності від їх функцій та чутливості інформації. Вибір профілю захищеності, визначений на основі аналізу ризиків і характеристик АС, дозволяє адаптувати заходи захисту до специфічних вимог, зокрема для систем органів державної влади, банківської діяльності, керування технологічними процесами. Це забезпечує оптимальний баланс між конфіденційністю, цілісністю та доступністю даних, що є ключовим для ефективного управління інформаційною безпекою.

[1] Потенко О.С. Визначення функціонального профілю захисту автоматизованої системи/ Потенко О.С. - К.: Інститут проблем моделювання в енергетиці ім. Г.Є Пухова НАН України, 2024. 146 с. ISBN 978-617-8579-06-7 (https://ipme.kiev.ua/books/Monog-VFPZ-AS-Potenko-2024.pdf)

[2] НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

V.V. Stanytsina, V.O. Artemchuk

TECHNO-ECONOMIC APPRAISAL OF HEAT-PUMP HEAT-SUPPLY SYSTEMS IN UKRAINE THROUGH LEVELIZED-COST METRICS

Heat pumps (HPs) are widely recognised in Europe as a cornerstone technology for delivering low-carbon space-heating and domestic-hot-water services; more than 24 million units were in operation across 21 countries by the end of 2023, displacing over 59 Mt CO_2 annually. Although Ukraine's market is still nascent and heavily dependent on imported equipment, rising energy-security concerns and EU-alignment targets have stimulated interest in both ground-source (GSHP) and air-source (ASHP) solutions [1, 2].

This study provides a comparative Levelized Cost of Heat (LCOH) analysis for fifteen Ukrainian HP heat-supply systems: eleven real-world installations (private dwellings, public facilities and a commercial building) and four design-stage projects extracted from installers' public offers. Capacities range from 4 kW to 331 kW and Seasonal Coefficients of Performance (SCOP) from 2.8 to 4.1. Capital- and operating-cost data were normalised to August 2024 prices; LCOH values were computed over a 20 – 30 year lifetime under two financing scenarios (0 % and 10 % discount rates) and tariff structures that reflect Ukraine's two-zone residential and commercial electricity pricing.

The results show that CAPEX dominates overall heat cost: GSHPs allocate only 20 – 40 % of investment to the pump itself, with the geothermal field and installation works absorbing the balance, whereas ASHPs devote 60 – 70 % to the unit. A shift from 0 % to 10 % discount rate inflates GSHP LCOH by 2.1 – 2.6 ×, compared with 1.3 – 1.6 × for ASHPs, underscoring the penalty imposed by Ukraine's high-interest environment. Promotional cost estimates published on installers' websites were found to understate total project costs by up to 80 %, leading to unrealistically low LCOH projections. Nevertheless, when interest-free financing and preferential "electric-heating" or night tariffs are assumed, both residential GSHPs and commercial ASHPs can meet or undercut Kyiv's full-cost district-heat tariff (≈ 58 €/Gcal). The analysis confirms that HP systems can deliver economically competitive and carbon-efficient heat in Ukraine provided supportive fiscal instruments are in place—notably subsidised loans, wider two-zone metering and deeper localisation of drilling and balance-of-plant components.

[1] European Heat Pump Association. (2018). Heat pumps integrating technologies to decarbonise heating and cooling (White Paper). https://www.ehpa.org/wp-content/uploads/2022/10/White_Paper_Heat_pumps-1.pdf

[2] Westrig, P., Azau, S., Gibb, D., Vanbecelaere, J., & Uguen, G. (2024). European heat pump market and statistics report 2024 (102 pp.). European Heat Pump Association AISBL.

О.В. Згуровець, В.О. Дерій

ВИЗНАЧЕННЯ ЄМНОСТІ НАКОПИЧУВАЧІВ ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ ДЛЯ ВІТРОВИХ ЕЛЕКТРОСТАНЦІЙ НА ОСНОВІ АНАЛІЗУ ПОГОДИННОЇ ГЕНЕРАЦІЇ

Вступ

Інтеграція вітрових електростанцій до об'єднаної енергосистеми України супроводжується високим рівнем невизначеності у виробітку, що викликає труднощі при балансуванні системи [1–2]. Одним з ефективних підходів до вирішення цієї проблеми є використання систем накопичення енергії (СНЕ), які дозволяють зберігати надлишкову енергію в періоди її перевиробітку та повертати її в мережу у періоди дефіциту [3–4].

Однак встановлення надмірних обсягів накопичення призводить до зростання інвестиційних витрат [5]. Це зумовлює необхідність обґрунтованого вибору розміру СНЕ з урахуванням фактичних режимів генерації та заданого рівня покриття потреб в енергії.

Методика та результати

Проведений аналіз базувався на погодинних даних генерації ВЕС ОЕС України за річний період. У дослідженні була застосована методика, згідно з якою електроенергія, що генерується понад середній рівень добової потужності, вважається такою, що підлягає акумулюванню. Такий підхід дозволив оцінити добові потреби в накопиченні енергії з урахуванням фактичного профілю генерації.

Аналіз розподілу відповідних добових величин показав, що упродовж року виникають як дні з незначною потребою в акумуляції, так і поодинокі випадки значних надлишків генерації. При цьому абсолютні пікові значення спостерігалися вкрай рідко, а значна частина днів характеризувалася відносно помірними рівнями потреби в акумуляції. Це дозволяє зробити висновок, що повне забезпечення покриття добових надлишків у всі дні року вимагає значних обсягів накопичувачів, які будуть затребувані лише у виняткових випадках.

З іншого боку, встановлення обсягу накопичення, що забезпечує покриття більшості ситуацій (наприклад, 90–95% днів), дає змогу значно зменшити необхідну ємність накопичувачів (на 20–30%) без критичної втрати функціональності. Отримані результати свідчать, що компромісні рівні акумуляції можуть бути достатніми для підтримання прогнозованого відпуску електроенергії в мережу за більшістю сценаріїв.

Обговорення

Запропонований підхід дозволяє адаптувати ємність накопичувача під конкретні характеристики вітрової генерації в регіоні. Імовірнісна постановка задачі є доцільною в умовах, коли перевищення потреб трапляються рідко і не потребують 100% покриття.

Модель легко масштабувати на інші типи генерації або гібридні системи. Також методика може бути інтегрована з моделями вартості та тарифного стимулювання для обґрунтування доцільності участі систем накопичення у ринку послуг балансування.

Висновки

Розроблено підхід до визначення оптимальної ємності СНЕ для вітрових електростанцій, що базується на обмеженні відпуску енергії до середнього рівня та акумулюванні надлишків.

Метод дозволяє оцінити потреби в акумуляції з урахуванням статистики генерації та заданого рівня забезпечення генерації. Застосування запропонованого підходу дозволяє знизити встановлену ємність накопичувачів електричної енергії без значної втрати ефективності та покращити економіку проєктів відновлюваних джерел енергії з акумулюванням електричної енергії.

[1] Vergil, H., Mursal, M., Kaplan, M., & Khan, A. U. I. (2024). The Causal Relationship between Public Investment in Renewable Energy and Climate Change Performance Index. International Journal of Energy Economics and Policy, 15(1), 121–130. https://doi.org/10.32479/ijeep.17308

[2] Hassan, Q., Viktor, P., Al-Musawi, T. J., Ali, B. M., Algburi, S., & Alzoubi, H. M. (2024). The renewable energy role in the global energy transformations. Renewable Energy Focus, 48, 100545. https://doi.org/10.1016/j.ref.2024.100545

[3] Володимир Дерій. (2023). Накопичувачі електричної енергії. Системні дослідження в енергетиці, (1 (72), 12-24. https://doi.org/10.15407/srenergy2023.01.012.

[4] Zaporozhets A., Kostenko G., Zgurovets O., Deriy V. Analysis of Global Trends in the Development of Energy Storage Systems and Prospects for Their Implementation in Ukraine. In O. Kyrylenko, S. Denysiuk, R. Strzelecki, I. Blinov, I. Zaitsev, A. Zaporozhets (Eds.). Power Systems Research and Operation. Studies in Systems, Decision and Control. 2024. Vol. 512. P. 69−87. Springer, Cham. https://doi.org/10.1007/978-3-031-44772-3_4

[5] Grid Energy Storage Technology, Cost and Performance Assessment, 2022. 174 p. URL: https://www.pnnl.gov/sites/default/files/media/file/ESGC%20Cost%20Performance%20Report%202022%20PNNL-33283.pdf (дата звернення: 29.04.2025).

S. Matveev, I. Ivchenko

ARTIFICIAL INTELLIGENCE AND HUMAN–MACHINE INTERACTION FOR ENHANCING THE RESILIENCE OF UKRAINE'S ENERGY SYSTEM

Abstract. This article explores the role of artificial intelligence (AI) and human–machine interaction (HMI) in enhancing the resilience of Ukraine's energy system through decentralization. Key challenges facing the Ukrainian energy sector, modern technological solutions, and their potential to ensure energy supply stability are analyzed.

Ukraine is currently facing significant challenges in its energy sector. Energy system resilience is a critical issue, especially amid increasing stress due to physical threats to infrastructure, cybersecurity vulnerabilities, and market instability. To enhance resilience, this paper proposes the adoption of decentralized solutions based on artificial intelligence and human–machine interaction. AI enables optimization and automation of energy management, while HMI allows operators to respond more effectively to unpredictable events.

Ukraine's energy system, which operated under a centralized model until recently, is now encountering multiple threats. Military actions, infrastructure damage, and cybersecurity risks make the traditional centralized management model highly vulnerable. Under such conditions, it is essential to implement new approaches that enable decentralized control and strengthen resilience to external threats. Decentralization allows the system to become less dependent on any single node or source, increasing its overall reliability.

Artificial intelligence has considerable potential to improve the performance of decentralized energy systems. One key application of AI is in forecasting energy demand and optimizing resource distribution. AI systems can analyze large volumes of real-time data, allowing for the management of both energy generation and consumption according to current supply and demand.

The use of AI in smart grid systems enables the integration of renewable energy sources and the automatic balancing of load across the network. The application of smart grid technologies can increase energy system efficiency by 20–30% and reduce the risk of outages.

According to a McKinsey study, integrating AI into energy systems can significantly reduce energy losses and improve resource management efficiency. This is particularly important for Ukraine, which is actively implementing renewable energy sources—such as solar and wind power plants—and pursuing decentralized energy supply models.

Human–machine interaction empowers operators to manage complex systems more efficiently. In the energy context, HMI enables joint operation between human operators and automated systems, reducing the risk of human error and

accelerating decision-making in critical situations. A key component of HMI is real-time monitoring and data analysis systems, which provide operators with up-to-date information on the energy system's status. Thanks to AI, these systems can not only detect problems but also suggest solutions, enabling quicker responses to sudden changes or emergencies.

Decentralizing the energy system facilitates a shift from centralized to distributed management. The main advantage of a decentralized system is its enhanced resilience to external threats. For example, if one node of the network fails, other autonomous subsystems can continue to provide local energy supply, preventing widespread outages.

Because decentralized energy systems rely heavily on automated solutions and AI, cybersecurity threats increase. Using AI to protect systems from cyberattacks is a vital step toward improving their security. AI can detect anomalous activity and respond automatically, significantly reducing the risk of successful attacks.

The use of artificial intelligence and human–machine interaction to improve the resilience of Ukraine's energy system through decentralization is a promising direction for development. It enhances the flexibility and reliability of the system, reduces the risks posed by physical and cyber threats, and supports the integration of renewable energy sources. Successful implementation of these technologies requires active cooperation between academic institutions, government agencies, and the private sector.

[1] McKinsey & Company. (2020). Artificial Intelligence in Energy Systems: New Frontiers and Opportunities. mckinsey.com
[2] OpenAI. (2021). AI and Compute: The Future of Energy Efficiency. openai.com
[3] Microsoft. (2021). Microsoft's Commitment to Renewable Energy. microsoft.com

Є.С. Сметана

ТЕХНОЛОГІЯ РОЗРОБКИ ПРОТИАВАРІЙНИХ ТРЕНУВАНЬ ДИСПЕТЧЕРА ПІДПРИЄМСТВА ЕЛЕКТРИЧНИХ МЕРЕЖ

Однією з основних форм підготовки оперативного персоналу підприємств електричних мереж (операторів систем розподілу (ОСР)) є протиаварійні тренування, надалі тренування.

Протиаварійний програмний тренажер на базі обчислювальної техніки, що використовується для організації тренувань диспетчерського персоналу оперативних диспетчерських служб (ОДС) конкретних ОСР повинен відповідати вимогам [1]:

- система візуалізації (учбова інформаційна модель, далі — УІМ) тренажера має забезпечувати імітацію мнемосхеми (МС) та оперативно-інформаційного комплексу (ОІК), що відповідають реальному об'єкту
- імітація інформаційних каналів (телефонний і радіо зв'язок) і об'єм інформації, що по ним надходить, повинні відповідати специфіці і формам її отримання в реальних умовах;
- діяльність на тренажері не повинні вимагати від тренованого додаткових зусиль на перекодування своїх дій в форму, що відповідає реальній діяльності;
- симуляція режимів обладнання повинні бути максимально наближені до реальних і не викликати в тренованого відчуття дискомфорту. Час реакції тренажера на управління повинен складати 0,5-1С, що відповідає реакції реального об'єкта на управління.

Електрична мережа ОСР є об'єктом унікальним, якому притаманна власна топологія, алгоритми керування, характеристики обладнання, пристроїв, тощо. Враховуючи це, для кожної з них потрібен свій унікальний тренажер, що враховує специфіку управління саме цим об'єктом. Традиційні методи розробки і реалізації комп'ютерних тренажерів фактично потребують створення міждисциплінарних груп розробників для кожного об'єкта рівня ОСР і вище, що на даному етапі ні економічно, ні організаційно виконати неможливо. Забезпечити підприємства галузі необхідною кількістю тренажерів можливо лише з використанням сучасних апаратних і програмних засобів.

Зі сказаного витікає, що інтерактивна програмна платформа тренажера має забезпечувати зручний і інтуїтивно зрозумілий інтерфейс, орієнтований на непрограмуючого користувача, який дозволяв би на місцях експертам-технологам створювати тренажери з врахуванням специфіки функціонування і управління реальним об'єктом, на якому він буде застосовуватись.

Пропонується нова технологія (мал. 1) створення комп'ютерних тренажерів на основі існуючих в ОСР програмах організації і проведення

індивідуальних протиаварійних тренувань диспетчерів ОДС і графічної нотації представлення програм у вигляді алгоритмів [2].

Малюнок 1. - Технологічний ланцюг створення тренування

Існуючі в ОСР програми тренування містять опис схеми до технологічного порушення, причину виникнення порушення, його розвиток, наслідки і карту робочої діяльності персоналу по визначенню, локалізації і ліквідації ситуації що склалась.

Дії персоналу представлені у вигляді карти робочої діяльності будемо називати *лінійною моделлю робочої діяльності (РД)*.

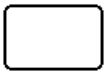
Карта РД не може відобразити реальний процес в його багатогранності. Вона виконує функцію еталонної діяльності, без врахування варіативності поведінки тренованого і прийняття ним рішень при наявності рівноцінних варіантів.

Зважаючи на сказане, модель РД для машинного відтворення потребує чітко структурованої моделі з визначеними потоками даних, логікою обміну інформацією, діями і точками прийняття рішень та взаємодією між учасниками процесу і об'єктом керування.

Для представлення моделі РД вибрана графічна нотація BPMN 2.0 як найбільш розвинена, зрозуміла, така що піддається аналізу і програмній реалізації. В якості елементів нотації BPMN використовуються: дії, логічні оператори розгалуження, події, з'єднувальні елементи і дані [3].

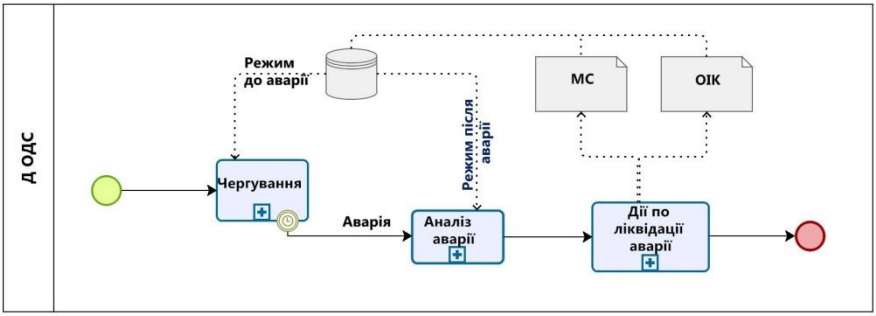
Нотація дозволяє представляти модель РД у вигляді розгалужених алгоритмічних моделей, що адекватно відтворюють реальний робочий процес. Для позначення дій в нотації використовуємо два елементи: проста дія і підпроцес (табл.1).

Таблиця 1. Типи дій.

№ п/п	Позначення	Опис
1		Проста дія. Складається лише з однієї операції.
2		Підпроцес. Позначається маркером (+). Може бути представлений окремим графом. Підпроцес складається з простих дій і з підпроцесів. Глибина вкладень підпроцесів при цьому не обмежується.

Використання підпроцесів забезпечує можливість застосування модульного проектування, за якого алгоритм розбивається на окремі логічно завершені компоненти, що можуть розроблятися та налаштовуватися незалежно.

На першому етапі розробляється алгоритм дій персоналу без деталізації змісту дій. Іншими словами створюємо ескіз алгоритму РД (мал.2). Такий граф будемо називати *аналітичною моделлю* [3] *РД*.



Малюнок 2. – Аналітична модель робочої діяльності.

На основі аналітичної моделі і карти РД розробляємо розгорнуту модель діяльності в реальних умовах технологічного порушення, яка включає алгоритмічний опис власних дій тренованого, його взаємодію з керівництвом, підлеглим персоналом, пристроями дистанційного керування, захисту і сигналізації, МС, ОІК тощо.

Розгорнуту модель, яка представляє направлений граф як сукупність дій, логічних операторів, подій, з'єднувальних елементів, даних і коментарів в нотації BPMN будемо називати *учбовою моделлю діяльності (УМД)*.

Для адекватного відображення учбового процесу тренування УМД має враховувати процедури прийняття рішень і варіативність поведінки реального оператора. Це можливо за умови представлення розгорнутих моделей розгалуженими структурами, у вигляді розгалужених структур, у яких маршрутизація та послідовність дій визначаються логічними операторами й мають інтерактивний характер.

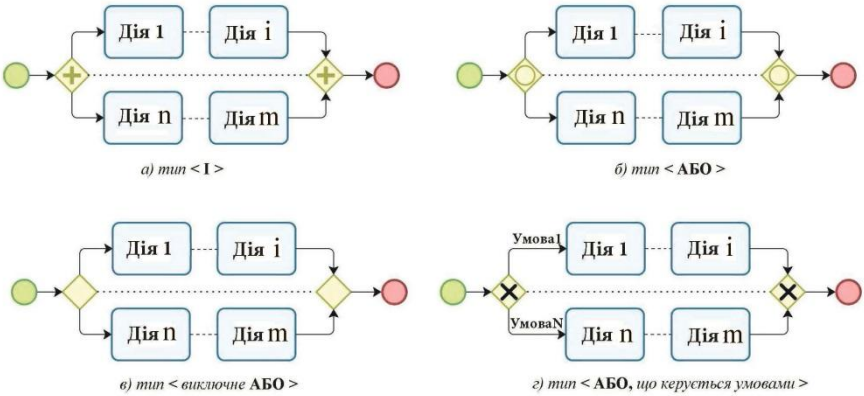
На основі аналізу реальної диспетчерської діяльності в ОДС було виділено чотири типи логічних операторів, що формують алгоритмічну структуру маршрутизації руху. (мал.3).

Логічні оператори кожного типу можуть реалізовувати як функцію розгалуження, так і функцію об'єднання логічних гілок у процесі маршрутизації..

Оператор розгалуження генерує токени [3], які переміщаються гілками моделі активуючи поточні дії і визначаючи порядок їх виконання. Вибір гілки, по якій буде направлений токен є процесом інтерактивним.

Токени активують множину дозволених дій $D_j = \{d_j\}_{j=1}^{n}$.

Тренований виконує дію d_j. Якщо $d_j \in D_j$ відпрацьовується дозволена дія d_j і токен переміщується відповідною гілкою до наступної дії. Вихідна гілка оператора злиття активується лише після того, як виконані передбачені гілки розгалуження.



Малюнок 3. – Типи логічних операторів.

Тип «І». Оператор розгалуження генерує токени по кількості гілок і тим активує дозволені дії $\{d_j\}_{j=1}^{n}$. Виконання дозволеної дії d_j переміщає токен по відповідній гілці до наступної дії формуючи множину $D_{j+1.}$ Вихідна гілка оператора об'єднання активується після того, як в ньому зберуться всі згенеровані токени, що послідовно обійшли всі гілки блоку «І». Даний тип операторів застосовується при моделюванні дій, які виконуються паралельно персоналом різних об'єктів по розпорядженню диспетчера ОДС.

Тип «АБО». Оператор розгалуження активує всі вихідні гілки формуючи D_j, але генерує тільки один токен. Токен переміщується послідовно гілкою, для якої виконується умова $dj \in D_j$. Обхід дій в гілці і гілок виконуються послідовно. Вихідна гілка оператора злиття активується після того, як буде завершено послідовний обхід всіх гілок. Вибір послідовності обходу здійснює тренований. Даний тип застосовується при моделюванні ситуації суб'єктивного вибору послідовності дій..

Тип «виключне **АБО».** Оператор розгалуження генерує один токен і активує всі вихідні гілки, формуючи допустиму множину дій D_j. Виконується дозволена дія $d_j \in D_j$, вибір якої здійснюється тренованим суб'єктивно, на основі власних міркувань або попереднього досвіду. Токен переміщується гілкою, до якої належить d_j. Вихідна гілка оператора злиття активується після того, як токен завершить рух вибраною гілкою. Даний тип застосовується при моделюванні ситуацій коли варіанти дій мають однакову пріоритетність.

Тип «АБО, що керується умовами**».** Те саме, що і «виключне АБО», але вибір визначається зовнішніми умовами, які тренований перевіряє в процесі діяльності (навантаження силового обладнання, стан устаткування тощо).

Дана технологія дозволяє залучити до процесу створення комп'ютерних програмних тренувань найбільш кваліфікований технічний персонал ОСР без посередництва програмістів.

Запропонована графічна специфікація представлення УМД дозволяє адекватно моделювати реальний робочий процес диспетчера ОСР включно з процедурами прийняття рішень і варіативності його поведінки.

[1] Правила проведення протиаварійних тренувань персоналу електричних станцій та мереж. Наказ Міненерго України, №991, від 24.12.2013р.

[2] Інтегрована технологія проектування комп'ютерних засобів сценарного типу підготовки фахівців для енергопідприємств / Р. П. Абрамович, А. О. Бальва, В. Д. Самойлов // Електронне моделювання. - 2018. - Т. 40, № 2. - С. 27-42. - Режим доступу: http://nbuv.gov.ua/UJRN/elmo_2018_40_2_5

[3] Freund, J., & Rücker, B. (2012). Real-Life BPMN: Using BPMN 2.0 to Analyze, Improve, and Automate Processes in Your Company. 3rd ed. Berlin: Books on Demand. – 308 p.

XLIII
НАУКОВО-ТЕХНІЧНА КОНФЕРЕНЦІЯ
МОЛОДИХ ВЧЕНИХ ТА СПЕЦІАЛІСТІВ
ІНСТИТУТУ ПРОБЛЕМ МОДЕЛЮВАННЯ В
ЕНЕРГЕТИЦІ ІМ. Г.Є. ПУХОВА НАН УКРАЇНИ

ПРИСВЯЧЕНА ДНЮ НАУКИ В УКРАЇНІ

Збірник матеріалів конференції
14 травня 2025 р.

Collection of materials of the XLIII Scientific and technical conference of young scientists and specialists of G.E. Pukhov Institute for Modelling in Energy Engineering of National Academy of Sciences of Ukraine, Kyiv, May 14, 2025 / PIMEE of NAS of Ukraine. - 2025. – 144 p.

Збірник матеріалів XLIII Науково-технічної конференції молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, м. Київ, 14 травня 2025 р. / ІПМЕ ім. Г.Є. Пухова НАН України. – 2025. – 144 с.

Інформаційна підтримка:

Сторінка конференції на сайті Інституту

Telegram канал РМВ НАН України