НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

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

МАТЕРІАЛИ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ «РЕЗИЛЬЄНТНІСТЬ ДИНАМІЧНИХ СИСТЕМ»

27 грудня 2024 року

Київ – 2024

УДК 620.9::[517.938::(519.718+004.056)]
ББК 31
Р-34

Рекомендовано до друку Вченою радою Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України (протокол № 12 від 28 листопада 2024 р.)

Р-34 **Резильєнтність динамічних** систем, науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України : матеріали (Київ, 27 грудня 2024 р.). Київ : ІПМЕ ім. Г.Є.Пухова НАН України, 2024. 237 с.

R-34 **Resilience of** dynamic systems, scientific-practical conference of the G.E. Pukhov Institute for Modeling in Energy Engineering National Academy of Sciences of Ukraine : materials (Kyiv, December 27, 2024). Kyiv: PIMEE NAS of Ukraine, 2024. 237 p.

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

МАТЕРІАЛИ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«РЕЗИЛЬЄНТНІСТЬ ДИНАМІЧНИХ СИСТЕМ»

27 грудня 2024 року

м. Київ

2024

ОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ

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

ПРОГРАМНИЙ КОМІТЕТ

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

Чемерис Олександр Анатолійович
доктор технічних наук, професор,
заступник директора з наукової роботи

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

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

ОРГАНІЗАЦІЙНИЙКОМІТЕТ

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

Клименко Тетяна Михайлівна
завідувачка науково-організаційного відділу

Цуркан Оксана Володимирівна
молодший наковий співробітник

S. Saukh

DEGRADATION AND COLLAPSE OF DYNAMIC SYSTEMS

BIOLOGICAL SYSTEM

Degradation of a biological system is a gradual deterioration of the functioning of an organism or ecosystem under the influence of internal or external factors. It is characterized by the loss of biological functions, a decrease in resistance to stress and the inability to restore the previous state [1-3].

The collapse of a biological system is the final stage of degradation, when the system can no longer maintain its basic functions and disintegrates or undergoes a drastic change. Collapse leads to the loss of system structure, its functionality and, in ecosystems, can cause the disappearance of species and the destruction of ecosystem balance.

Stages of biological system degradation:

1. *Initial stage:*

At the initial stage, the system can maintain functionality, but minor disturbances in its work begin to appear, for example, a decrease in productivity or an increase in sensitivity to stress.

2. *Progressive degradation:*

Gradual increase of negative effects from external or internal factors. The functions of the system are increasingly disturbed, and it loses the ability to regenerate or adapt.

3. *Approaching collapse:*

At this stage, the system is no longer able to perform its main functions. Negative processes become irreversible, and restoration of system functions becomes impossible without external intervention.

4. *Collapse:*

The last stage, when the system collapses. This can manifest as the death of an organism, the extinction of a species, or the complete destruction of an ecosystem.

SOCIAL SYSTEM

Degradation of the social system is a process of gradual deterioration of the functioning of social institutions, norms and interactions between people in society. It manifests itself through a decrease in social cohesion, trust between citizens and the efficiency of state institutions. Degradation can occur under the influence of internal and external factors, such as economic crisis, political instability or environmental disasters [4-6].

The collapse of the social system is a more radical and drastic process when the social system loses its ability to function normally, which leads to massive social upheavals, chaos, the destruction of social order and the disruption of the basic functions of the state and society.

Stages of degradation of the social system:

1. *Initial violations*:

At this stage, signs of ineffectiveness of state institutions, growing inequality and social tension appear. Society is still functioning, but crises of confidence in the government and other institutions are beginning.

2. *Deepening of the crisis*:

Internal conflicts and social contradictions are intensifying. You can see the increase in economic inequality, the rise in crime, the decline in living standards and mass protests.

3. *Instability and decline*:

Social institutions become unable to maintain order and provide basic needs of citizens. This can lead to destabilization, weakening of state power and outbreaks of violence.

4. *Collapse*:

The social system is completely destroyed: institutions lose their effectiveness, chaos is observed, social control is lost, mass riots or even civil wars are possible.

ECONOMIC SYSTEM

Degradation of the economic system is a process of gradual deterioration of the functioning of the economy, which is manifested in a decrease in growth rates, a drop in productivity, deepening of inequality, unemployment, and an increase in poverty. Economic degradation is often accompanied by crises in various sectors of the economy, financial instability and lack of investment in development [7-9].

The collapse of the economic system is a sharper and deeper deterioration of the economic condition of a country or region, when the main economic mechanisms fail. The collapse leads to mass bankruptcy of enterprises, a sharp drop in the incomes of the population, hyperinflation, a crisis in the banking system and a decrease in the state's ability to fulfill its obligations.

Stages of degradation of the economic system:

1. *Initial degradation*:

Declining economic growth, falling investment and increasing unemployment. At this stage, the first signs of inflation or budget deficit can be observed.

2. *Progressive degradation*:

Aggravation of economic problems: a decline in production, an increase in the debt burden, a shortage of goods, and an increase in social inequality. At this stage, it becomes more difficult to provide the basic economic needs of the population.

3. *Economic crisis*:

A sharp drop in economic indicators, bankruptcies of enterprises, an increase in unemployment, a drop in the standard of living. The economy is becoming unstable and needs immediate measures to avoid collapse.

4. *Collapse of the economic system*:

Complete collapse of economic infrastructure, loss of control over financial institutions, hyperinflation, mass unemployment and shortage of goods. The state loses the ability to perform its social and economic functions.

ENERGY SYSTEM

Degradation of the energy system is a gradual deterioration of the functioning of the energy infrastructure, which leads to a decrease in the efficiency of energy production, distribution and consumption. This process can be accompanied by disruptions in the work of energy enterprises, wear and tear of equipment, insufficient investments in modernization and an increase in the frequency of accidents. Degradation can seriously affect the stability of energy supply and economic development of the region [10-13].

The collapse of the energy system is a sudden and abrupt shutdown of a significant part of the energy infrastructure, which leads to massive power outages, stopping production processes and disrupting the life of the population. Collapse is often the result of systemic problems that have accumulated over time and can be caused by technical, natural or human factors.

Stages of energy system degradation:

1. *Initial degradation*:

In the initial stages, there may be minor disruptions in the operation of the energy infrastructure, an increase in the frequency of accidents and a reduction in the amount of investment in maintenance.

2. *Progressive degradation*:

At this stage, the problems become systemic: more frequent accidents, problems with energy supply in remote regions, rising costs for repairs and maintenance of old infrastructure.

3. *Energy crisis*:

There are massive power outages, a shortage of capacity to meet the energy needs of the population and industry. The number of accidents is increasing, the efficiency of energy production and transportation is decreasing.

4. *Energy system collapse*:

Collapse can occur as a result of large-scale technical accidents, natural disasters or military operations. It leads to the termination of energy supply to large regions, the shutdown of industrial enterprises and vital infrastructure facilities.

INFORMATION SYSTEM

Information system degradation is a process of gradual reduction of its functionality, efficiency and reliability. Degradation is manifested in a decrease in the speed of data processing, more frequent errors in work, a decrease in security and resistance of the system to external threats. Degradation can occur due to wear

and tear of technical resources, outdated software, or improper system management [14-16].

The collapse of an information system is a critical moment when the system completely loses its ability to perform its functions. Collapse is accompanied by failure of key components, loss of data, inability to process information or access it.

Stages of information system degradation:

1. *Initial degradation*:

Slow system performance, more frequent crashes or delays due to technical issues or outdated software. At this stage, the system is still functional, but its reliability and performance are gradually decreasing.

2. *Progressive degradation*:

The system begins to fail more often, serious problems with access to information or its processing appear. The number of errors in the software increases, and users begin to experience significant inconvenience in working with the system.

3. *Information crisis*:

There are mass failures in the work of key components of the system, which leads to interruptions in the work of enterprises or institutions that depend on this information system. Without immediate intervention, the system may fail completely.

4. *Collapse of the information system*:

Complete system failure due to technical or software problems, cyber attacks or catastrophic events. Loss of the ability to access data, process information and maintain communication between system elements.

CONCLUSION.

Dynamic systems degradation and collapse refer to the process by which complex systems deteriorate over time and eventually fail. This can happen due to various factors such as wear and tear, environmental conditions, and operational stresses.

Degradation involves the gradual decline in system performance and reliability. It can be caused by factors like aging components, material fatigue, and external environmental conditions.

Dynamic Systems often operate under changing conditions, which can accelerate degradation. These dynamic environments include variations in temperature, humidity, load conditions, and other external factors.

Collapse is the final stage where the system fails completely. Collapse can be sudden or progressive, depending on the system's resilience and the severity of the degradation.

To predict and manage degradation, reliability models are used. These models help in understanding how systems degrade over time and in developing strategies to mitigate failure.

Building resilience into systems can help them withstand degradation and avoid collapse. This involves designing systems to be flexible and robust against various stressors.

1. Brockett C., Woolaston K., Deane F., et al., “Best practice mechanisms for biodiversity conservation law and policy,” Cambridge Prisms: Extinction, 2023. https://doi:10.1017/ext.2023.14.
2. Garcia-Pichel F., Sala O., “Expanding the Pulse–Reserve Paradigm to Microorganisms on the Basis of Differential Reserve Management Strategies,” BioScience, Volume 72, Issue 7, 2022, pp. 638–650, https://doi.org/10.1093/biosci/biac036.
3. Ferreira A.F., Zimmermann H., Santos R., von Wehrden H., “Biosphere Reserves’ Management Effectiveness—A Systematic Literature Review and a Research Agenda,” Sustainability, 2020, Vol. 12, 5497. https://doi.org/10.3390/su12145497.
4. Ferreira A.F., Zimmermann H., Santos R., Von Wehrden H., “A Social–Ecological Systems Framework as a Tool for Understanding the Effectiveness of Biosphere Reserve Management,” Sustainability, 2018, Vol. 10, 3608. https://doi.org/10.3390/su10103608.
5. Saja A.M.A., Teo M., Goonetilleke A. et al., “A Critical Review of Social Resilience Properties and Pathways in Disaster Management,” Int J Disaster Risk Sci, 2021, Vol. 12, pp. 790–804. https://doi.org/10.1007/s13753-021-00378-y.
6. Pathak P., Persad G., Sönmez T., Ünver M.U., “Reserve system design for allocation of scarce medical resources in a pandemic: some perspectives from the field,” Oxford Review of Economic Policy, Vol. 38, Issue 4, Winter 2022, pp. 924–940, https://doi.org/10.1093/oxrep/grac034.
7. Schanz, Jochen F., “Reserve Management in Emerging Market Economies: Trends and Challenges,” (October 31, 2019). BIS Paper No. 104. https://ssrn.com/abstract=3497866.
8. Corsetti G. and Maeng F., ‘DP18644 The Theory of Reserve Accumulation, Revisited,” CEPR, 2023, Discussion Paper No. 18644. CEPR Press & London. https://cepr.org/publications/dp18644.
9. Barbosa-Alves M., Bianchi J., Sosa-Padilla C., “International Reserve Management Under Rollover Crises,” May 2024, NBER Working Paper No. w32393, Available at SSRN: https://ssrn.com/abstract=4825978.
10. Narayanan A., Welburn J.W., Miller B.M., Li S.T., Clark-Ginsberg A., “Deterring Attacks Against the Power Grid. Two Approaches for the U.S. Department of Defense,” RAND Corporation, 2020. https://www.rand.org/pubs/research_reports/RR3187.html.
11. Lei S., Wang C., Hou Y., “Power Grid Resilience against Natural Disasters: Preparedness, Response, and Recovery,” Wiley-IEEE Press, 2023. 10.1002/9781119801504.
12. Yao X., Wei H.-H., Shohet I., Skibniewski M. 2020. “Assessment of Terrorism Risk to Critical Infrastructures: The Case of a Power-Supply Substation,” Applied Sciences, 2020. 7162. https://doi.org/10.3390/app10207162.
13. Narayanan A. et al., 2020. “Deterring Attacks Against the Power Grid: Two Approaches for the U.S. Department of Defense,” RAND Corporation, 2020, United States. Retrieved from https://coilink.org/20.500.12592/1qrw1h.

14. Thunes J., Ulshagen A., Utvik V.A. 2023. “Information Systems Resilience: The Role of Flexibility and Stability,” In Proceedings of the 2022 International Conference on Information and Communication Technologies and Development (ICTD '22). 2023, Association for Computing Machinery, New York, Article 15, 1–4. https://doi.org/10.1145/3572334.3572382.
15. Andersson J., Grassi V., Mirandola R., Perez-Palacin D.. 2021. “A conceptual framework for resilience: fundamental definitions, strategies and metrics,” Computing, 2021, Vol. 4, pp. 559–588. https://doi.org/10.1007/s00607-020-00874-x
16. Goel L., Russell D., Williamson S., Zhang J.Z. (2023), “Information systems security resilience as a dynamic capability,” Journal of Enterprise Information Management, 2023, Vol. 36 No. 4, pp. 906-924. https://doi.org/10.1108/JEIM-07-2022-0228.

Л.В. Ковальчук, Р.В. Олійников, Г.В. Неласа, Т.М. Клименко

МЕТОД ПІДВИЩЕННЯ НАДІЙНОСТІ ФУНКЦІОНУВАННЯ ГВП/ГПВП

Тестування апаратних генераторів випадкових послідовностей вимагає набагато більш складного підходу, ніж тестування інших класів цифрових пристроїв. На відміну від традиційного підходу до перевірки функціональності, для апаратних генераторів випадкових послідовностей неможливо організувати перевірку в моделі чорної скриньки, з використанням еталонних вхідних значень, відповідних шляхів активізації внутрішніх схем і заздалегідь відомого фіксованого виходу обробки вхідної активації.

Більш того, поява відмови у процесі поточного функціонування апаратної реалізації звичайного скінченого автомату, як правило, одразу виявляється через очевидні некоректні вихідні послідовності. І така властивість також непритаманна апаратним генераторам випадкових послідовностей, що додатково ускладнює побудову і експлуатацію апаратних засобів для генерації випадкових послідовностей із заданим рівнем надійності.

Таким чином, для засобів апаратної генерації випадкових послідовностей із заданим рівнем надійності потрібно мати щонайменше три набора тестів різного призначення.

1. Після виробництва і на етапі налаштування.

Цей набір тестів повинний виявляти можливі дефекти окремих компонентів, процесу виробництва, некоректне налаштування та інші можливі причини некоректного функціонування після виробництва.

2. Періодичні діагностичні перевірки.

Ці тести повинні запускатися із заданою періодичністю (обумовленою рівнем прийнятного ризику) для виявлення потенційних збоїв і відмов, пов'язаних із зміною характеристик електронних компонентів з часом і в умовах експлуатації в різних режимах. Ці тести також повинні зменшувати ризики, пов'язані зі зникаючими збоями, коли пристрій знаходиться у неналежному стані деякий час і самостійно, без будь-якого зовнішнього впливу, повертається до нормального робочого стану.

З одного боку, ці тести дозволяють виявити достатньо велику кількість дефектів, з іншого боку, вимагають періодичне виведення пристрою генерації з режиму нормальної експлуатації.

Крім того, такі тести не зможуть виявити дефекти пристрою, що з'явилися вже після проведення перевірки, що є потенційною загрозою для використання дефектних послідовностей для генерації ключових даних у криптографічних застосунках.

3. Оперативне тестування в нормальному режимі роботи.

Такі тести запускаються під час штатної експлуатації пристрою і дозволяють у реальному режимі часу контролювати якість вихідних випадкових послідовностей.

На ці тести накладаються суворі вимоги щодо їхньої ефективності. З одного боку, вони повинні мати прийнятний рівень обчислювальної і просторової складності, щоб мати можливість проводити тестування у реальному режимі часу. З іншого боку, при всіх таких обмеженнях вони повинні максимізувати ймовірність виявлення всіх критичних дефектів, що можуть з'явитися в процесі експлуатації пристрою генерації.

Ці тести є критичними для кардинального зниження ризику використання дефектної послідовності для генерації ключових даних у криптографічних застосунках.

4. Post mortem дослідження.

Після виведення із експлуатації пристрій детально тестується, в тому числі із незворотньою зміною функціональності (наприклад, руйнуванням окремих компонентів при дослідженні властивостей) для отримання максимального обсягу інформації про компоненти пристрою і зміну їхніх властивостей під час життєвого циклу пристрою.

Такі тести проводяться як для вдосконалення процесу експлуатації подібних пристроїв, що ще залишаються в роботі, так і для створення вдосконаленого наступного покоління апаратних генераторів випадкових послідовностей.

Спираючись на попереднє обґрунтування, було визначено чотири основних типи тестування, які потрібно застосовувати для перевірки криптографічних якостей генераторів псевдовипадкових/випадкових послідовностей (ГПВП), а також їх окремих послідовностей. Для кожного з цих типів тестування необхідно створити свій набір тестів, що виконує певну задачу. Ці чотири типи тестування є наступними:

(i) – всебічне тестування ГПВП, яке виконується як при першому допуску засобу до експлуатації, так і при наступних допусках після ремонтів або проведення профілактичних процедур; також, за необхідності, такі дослідження можуть виконуватись або через фіксовані достатньо великі проміжки часу (1-5 років), якщо є ризик погіршення криптографічних якостей засобу за певний період часу, або в усіх випадках, коли результати регулярного (пункт (ii)) або постійного (пункт (iii)) тестування показали погіршення криптографічних якостей засобу;

(ii) – регулярне тестування ГПВП, що виконується через певні, достатньо невеликі проміжки часу (кожен день, кожен тиждень, тощо – в залежності від статистичних характеристик надійності роботи засобу), або в усіх випадках, коли результати постійного (пункт (iii)) тестування показали погіршення криптографічних якостей засобу;

(iii) – постійне тестування ГПВП, що виконується на постійній основі і в режимі реального часу повідомить про виникнення збоїв у роботі пристрою;

(iv) – тестування окремих послідовностей вихідної гами, отриманої з генератора, які для перевірки їх криптографічних якостей і прийняття рішення стосовно того, чи може окрема послідовність бути використана в якості ключових даних (ключів, початкових заповнень, векторів ініціалізації, синхропосилок, тощо).

В роботі також надано детальне обґрунтування вибору типів тестування ГПВП, яке суттєво спирається на особливості його роботи і застосування.

Для кожного набору тестів, відповідно до його призначення, визначено певні вимоги.

Вимогами, які є спільними для всіх наборів тестів з пунктів (i) - (iv), є наступні:

- тести повинні бути незалежними, щоб не дублювати роботу один одного і не збільшувати час тестування;

- тести повинні бути підібрані таким чином, щоб перевірка, яку вони виконують, охоплювала різні типи відхилень послідовності від суто випадкової послідовності, такі як: відхилення від рівноімовірного розподілу символів та груп символів; наявність міжсимвольних залежностей; наявність залежності від місця у послідовності, тощо.

Характеристиками, які є різними для різних наборів тестів, є наступні:

- час виконання тестування: від найбільшого (пункт (i)) до найменшого (пункт (iii));

- загальна помилка першого роду: від найбільшої (пункт (i)) до найменшої (пункт (iii));

- кількість тестів, спрямованих на перевірку одного типу відхилення: від найбільшої (пункт (i)) до найменшої (пункт (iii)).

Вимоги до набору тестів для за пунктом (iv) відрізняються від інших, оскільки вони призначені для перевірки якостей послідовностей, отриманих з генератора із заздалегідь високими криптографічними характеристиками. Тому ці вимоги більше направлені не на перевірку якості самого генератора, а на запобігання атакам направленого перебору, що мають на меті відновлення ключа шифрування. Тому до набору тестів, що відповідають задачі (iv), повинна входити невелика кількість тестів, що перевіряють відсутність у послідовності тих особливостей, які можуть бути використані для розробки алгоритму направленого перебору (відхилення від імовірного розподілу, залежність між символами, залежність від місця, тощо).

Оскільки одною з основних вимог до набору тестів є поняття їх незалежності, то для перевірки незалежності тестів було запропоновано кілька методів (та розроблено відповідні методики), що базуються на строгому визначенні незалежності статистичних тестів і також є строго обґрунтованими. Деякі із цих методів були розроблені раніше, деякі є новими і розроблені в рамках виконання цієї роботи. Проведено порівняльний аналіз всіх цих методів, в результаті чого показано, в яких саме випадках який метод має певні переваги.

Розроблені методи перевірки незалежності статистичних тестів дозволяють не тільки визначити, чи є тести залежними, але і вилучити надлишкові тести з набору, що дозволяє оптимізувати процес тестування (за швидкодією, без втрати якості тестування).

На базі розроблених та обґрунтованих вимог до кожного з набору тестів (незалежність, величина помилки 1 роду, перевірка за різними типами відхилень від випадковості), було сформовано відповідні набори тестів, а також реалізовано їх прототипи. При цьому, для повноти перевірки, було окремо розроблено тести перевірки незалежності окремих послідовностей та додано їх до відповідних наборів.

Звичайно, набори тестів для однієї і тієї ж задачі, які задовольняють визначеним властивостям, можна вибрати по-різному. За нашими експериментальними результатами, ми зупинились на наступних варіантах наборів тестів:

(i) – оновлений набір тестів NIST [1];

(ii) – набір тестів OPTIMA-6 [2, 3];

(iii) – набір miniOPTUMA-3, який містить 3 тести з попереднього набору: частотний бітовий тест, тест серій, тест місць знаків; як альтернативний варіант, можна використати набір тестів, описаний у FIPS 140-2 (2002 року) [4].

(iv) – набір OPTIMA-6.

Висновки. В результаті досліджень розроблено Метод статистичної перевірки криптографічних властивостей ГВП/ГПВП, що дозволяє перевіряти коректність і контролювати якість роботи протягом всього часу функціонування генератора. Цей Метод створює підґрунтя для розробки Національного стандарту перевірки статистичної якості генераторів.

Автори вдячні НФДУ за підтримку цього дослідження в рамках проекту № 2023.04/0020 «Розроблення методик та макету АРМ «ДЕМЕТРА» для постійного та періодичного контролю функціонування криптографічних застосунків з використанням статистичних методів» конкурсу Національного фонду досліджень України «Наука для зміцнення обороноздатності України».

1. Bassham III, L.E., Rukhin, A.L., Soto, J., Nechvatal, J.R., Smid, M.E., Barker E.B. Leigh S., Levenson M., Vangel M., Banks D., Heckert A., Dray J., &Vo S. (2010). A statistical test suite for random and pseudorandom number generators for cryptographic applications. *NIST Special Publication 800-22, Revision 1a.* https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf.
2. Rodinko, M., Kovalchuk, L., Nelasa, H., Bespalov, O. (2024) A New Extended Strategy of Processing of Statistical Testing Results. *Materials of the XI International Conference IT&I Information Technology and Implementation,* Kyiv.
3. Kovalchuk, L., Rodinko, M., Oliynykov, R., Klymenko, T. (2024) Using Chernoff Bound to Statistical Tests Independence Checking. *Materials of the XI International Conference IT&I Information Technology and Implementation,* Kyiv.
4. FIPS PUB 140-2 CHANGE NOTICES (12-03-2002): Security Requirements for Cryptographic Modules. National Institute of Standards and Technology, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf.

S.S. Shevchenko

ENSURING THE RESILIENCE OF ENERGY PUMPS BY INCREASING THEIR VIBRATION RELIABILITY

The rotor sealing system of a high-speed centrifugal pump is one of the most complex and critical units that determine the reliability of the entire unit. This is due to the harsh operating conditions of the seals in combination with high requirements for tightness in all operating modes [1]. In addition to the sealing function, non-contact seals perform an equally important function - they improve the vibration state of the centrifugal machine [2]. Dynamic indicators are especially important for seals of high-speed pumps. When designing sealing systems, it is necessary to coordinate their tightness and reliability, on the one hand, and resource indicators, on the other [3].

The creation of highly loaded pumping equipment with sealing systems for non-standard operating conditions is impossible without taking into account the above factors. Examples of such non-standard products are pumping units for nuclear power plants [4] (Fig. 1).

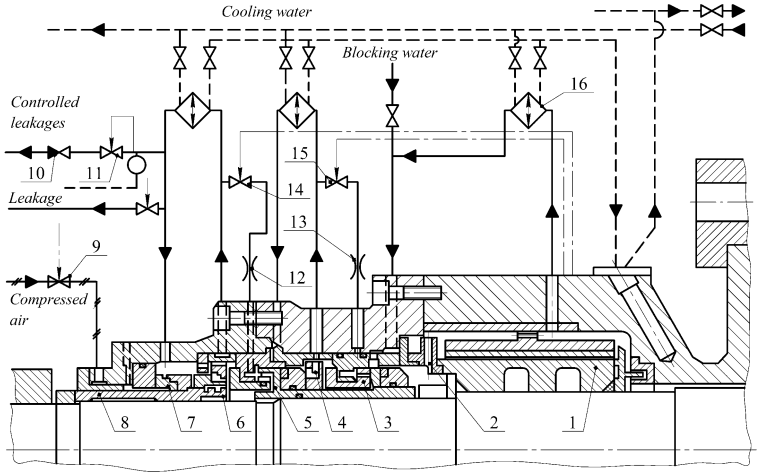


Figure 1 – Diagram of RCP shaft seal

As indicated in [5], the energy of volumetric losses can be converted into useful energy if, simultaneously, gap seals are used as hydrostatic supports, which are capable of not only having high radial rigidity, but also effectively damping rotor oscillations to acceptable values even in the presence of significant imbalance. This effect is especially significant in the presence of steep velocity and pressure gradients inherent in small gaps of gap seals, on which high pressure drops are throttled, and one of the surfaces belongs to the rotor, which simultaneously rotates and vibrates [6]. In [7], the dynamic characteristics of gap

seals as intermediate supports were investigated. The results of the conducted studies show that when creating sealing systems for modern centrifugal machines, it is necessary to take into account the effect of contactless seals on the dynamic characteristics of the rotor.

Forced joint radial-angular oscillations of the rotor at a constant pressure drop across slotted seals are described by the equations [6]

$$\begin{aligned} &a_1\ddot{u}+a_2\dot{u}+a_3u\mp i\left(a'_4\dot{u}+a'_5u\right)\omega-\left(\alpha'_2\dot{\theta}+\alpha'_3\theta\right)\omega\mp\\ &\mp i\left(\alpha_4\dot{\theta}+\alpha_5\theta-\alpha_0\theta\right)=\omega^2a^*=\omega^2\left|a^*\right|e^{\pm i\omega t},\\ &b_1\ddot{\theta}+b_2\dot{\theta}+b_3\theta\mp i\left(b'_4\dot{\theta}+b'_5\theta\right)\omega+\left(\beta'_2\dot{u}-\beta'_3u\right)\omega\mp\\ &\mp i\left(\beta_4\dot{u}+\beta_5u+\beta_0u\right)=\left(1-j_0\right)\omega^2\gamma^*=\left(1-j_0\right)\omega^2\left|\gamma^*\right|e^{\pm i\omega t}. \end{aligned} \quad (1)$$

Substituting the solution of equations (1) in the form

$$u=u_ae^{i(\omega t+\varphi_u)}=\tilde{u}e^{i\omega t},\ \theta=\theta_ae^{i(\omega t+\varphi_\vartheta)}=\tilde{\theta}e^{i\omega t},$$

we obtain a system of algebraic equations for the complex amplitudes A and

$$\Gamma\begin{bmatrix}-a_1\omega^2+a_3+a_4\omega^2+i\left(a_2-a_5\right)\omega\end{bmatrix}\tilde{u}-\begin{bmatrix}\left(\alpha_3-\alpha_4\right)\omega+i\left(\alpha_2\omega^2+\alpha_5-\alpha_0\right)\end{bmatrix}\tilde{\theta}=A\omega^2\\ \begin{bmatrix}-\left(\beta_3-\beta_4\right)\omega+i\left(\beta_2\omega^2-\beta_5-\beta_0\right)\end{bmatrix}\tilde{u}+\begin{bmatrix}-b_1\omega^2+b_3+b_4\omega^2+i\left(b_2-b_5\right)\omega\end{bmatrix}\tilde{\theta}=\Gamma\omega^2. \quad (2)$$

From the system of inhomogeneous algebraic equations (2), after a series of transformations, we obtain the amplitudes and phases expressed in terms of external perturbations:

$$\begin{aligned} u_a&=\overline{\omega}^2\sqrt{\frac{\left(AU_{22}-\Gamma U_{12}\right)^2+\left(AV_{22}-\Gamma V_{12}\right)^2}{U_0^2+V_0^2}},\\ \theta_a&=\overline{\omega}^2\sqrt{\frac{\left(\Gamma U_{11}-AU_{21}\right)^2+\left(\Gamma V_{11}-AV_{21}\right)^2}{U_0^2+V_0^2}},\\ \varphi_u&=-\operatorname{arctg}\frac{\left(AU_{22}-\Gamma U_{12}\right)V_0-\left(AV_{22}-\Gamma V_{12}\right)U_0}{\left(AU_{22}-\Gamma U_{12}\right)U_0+\left(AV_{22}-\Gamma V_{12}\right)V_0},\\ \varphi_\vartheta&=-\operatorname{arctg}\frac{\left(\Gamma U_{11}-AU_{21}\right)V_0-\left(\Gamma V_{11}-AV_{21}\right)U_0}{\left(\Gamma U_{11}-AU_{21}\right)U_0+\left(\Gamma V_{11}-AV_{21}\right)V_0}. \end{aligned} \quad (3)$$

Using a similar algorithm, it is possible to obtain expressions for amplitudes and phases for other types of non-contact seals.

For impulse seals [14]:

$$A\left(\omega\right)=\sqrt{\frac{b_1^2+\omega^2b_0^2}{U^2+\omega^2V^2}},\varphi=-\operatorname{arctg}\omega\frac{b_0U-b_1V}{b_1U+\omega^2b_0V}. \quad (4)$$

The amplitude and phase frequency characteristics of the auto-balancing system according to the corresponding external influences have the form:

$$A_\tau\left(\omega\right)=\sqrt{U_\tau^2+\omega^2V_\tau^2}=\sqrt{\frac{U_p^2+\omega^2V_p^2}{U^2+\omega^2V^2}},\ \varphi=\operatorname{arctg}\omega\frac{UV_p-VU_p}{UU_p+\omega^2VV_p} \quad (5)$$

and for shaftless pump:

$$A(\omega)=\sqrt{\frac{U_e^2+\omega^2V_e^2}{U_0^2+\omega^2V_0^2}},\qquad \varphi(\omega)=\operatorname{arctg}\omega\frac{U_0V_e-U_eV_0}{U_0U_e+\omega^2V_0V_e};\qquad (6)$$

As can be seen, expressions (3-6) for the amplitudes and phases of various non-contact sealing systems have a similar form.

An analysis of the gap seals' dynamic characteristics showed that the force coefficients of slotted seals are determined by geometric (clearance, radius, length, taper, shape of the leading edges) and operational (pressure drop, operating speed range, physical properties of the pumped medium) parameters. With a purposeful choice of these parameters, it is possible to influence the vibrational state of the rotor and the machine itself.

An important feature of centrifugal machines is that the pressure drops throttled at the gap seals are proportional to the rotor speed. This is due to the self-tightening effect of the rotor, which leads to a positive shift of the critical frequencies.

The operation of non-contact mechanical seals is accompanied by complex non-stationary, high-frequency hydrodynamic processes determined by micron end gaps. For the analytical description of the processes, a model for a sealing in the form of an automatic control system is proposed.

Automatic compensation systems for axial forces acting on the rotor of a multi-stage centrifugal pump simultaneously perform the functions of a self-adjusting non-contact mechanical seal and a heavily loaded radial-axial hydrostatic bearing. Such systems largely determine the oscillatory state of the rotor.

Axial and radial hydrodynamic forces arising in the throttling gaps of the balancing device are interconnected. As a result, the "rotor-auto-offloading" system, under the influence of the inevitable radial static imbalance, discharge pressure pulsations and harmonic changes in the axial force acting on the rotor perform interconnected forced radial-axial oscillations. At rotational frequencies coinciding with any natural frequency, the resonant amplitudes of these oscillations can exceed the permissible limits, therefore, the determination of resonant rotational frequencies and detuning from them is of great practical importance.

The wheel of a shaftless pump performs independent axial oscillations under the action of kinematic excitation in the form of given radial oscillations due to the static imbalance of the impeller. In this case, the adjustable end throttle creates negative feedback, so the impeller with the support-seal assembly is an automatic control of the end clearance system.

When designing a shaftless pump, it is necessary to compute the axial and angular vibrations of the impeller freely floating in the slotted seals. This will allow to ensure self-tightening of the rotor relative to its oscillations and avoid destabilizing factors by selection of design parameters.

Similar support-balancing devices can also be successfully used in multistage centrifugal pumps.

Using the proposed general approach to the analysis of non-contact seals as automatic control systems, and the algorithm for constructing their dynamic characteristics at the design stage, it is possible, by changing the geometric parameters of the seals, to ensure their vibration resistance margin.

The studies carried out have shown that all sealing units with throttling gaps or sealing paths filled with a high-pressure medium to be sealed should be considered as dynamic systems. The medium to be sealed, acting on the walls of the sealing paths, affects the dynamic state of the rotor.

It is shown that the purposeful choice of the design parameters of the seals makes it possible to improve the vibrational state of the rotor. In this case, the initially "flexible" dynamically rotor, in combination with properly designed seals, becomes "rigid". The proposed general technique makes it possible to evaluate this effect depending on the design characteristics of the seals and, by changing them at the design stage, to rebuild the “rotor-seals-auto-unloading” system from resonant operating modes.

1. Martsinkovsky, V. A., Shevchenko, S. S. (2018). Pumps of nuclear power plants: calculation, design, operation (S. Shevchenko (ed.)). Private Fund “University Book Publishing House.” 472 p. ISBN 978-966-680-866-3.
2. Martsynovskyi, V.A. Groove Seals: Theory and Practice; Sumy State University: Sumy, Ukraine, 2005. 416 p.
3. Shevchenko, S.S.; Shevchenko, O.S.; Vynnychuk, S. Mathematical Modelling of Dynamic System Rotor-Groove Seals for the Purposes of Increasing the Vibration Reliability of NPP Pumps. Nuclear and Radiation Safety. 2021, 1(89) 80–87. https://doi.org/10.32918/NRS.2021.1(89).09.
4. Shevchenko S., Shevchenko O. Improvement of Reliability and Ecological Safety of NPP Reactor Coolant Pump Seals. Nuclear and Radiation Safety. 2020. 4(88). 47—55. https://doi.org/10.32918/nrs.2020.4(88).06.
5. Shevchenko S. Mathematical modeling of centrifugal machines rotors seals for the purpose of assessing their influence on dynamic characteristics. Mathematical Modeling and Computing. 2021. 8(3).422—431. https://doi.org/10.23939/mmc2021.03.422.
6. Martsynovskyi, V.A. Dynamics of the Centrifugal Machine Rotors: Monograph; Sumy State University: Sumy, Ukraine, 2012. 562 p.
7. Shevchenko, S. S., Shevchenko, O. S. Mathematical Model and Calculation Method of a Shaftless Pump with Seals-Bearings. Electronic modeling, 2021, 43(1), 03–16. https://doi.org/10.15407/emodel.43.01.003.

Г.П. Дубинський, В.Ю. Зубок

КІБЕРСТІЙКІСТЬ КРИТИЧНИХ ІНФОРМАЦІЙНИХ АКТИВІВ В ОБ'ЄКТАХ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Наявність взаємодії з кіберпростором докорінно змінює ландшафт загроз для автоматизованих систем керування технологічними процесами (АСКТП). Це ставить нові вимоги до здатності передбачати, виявляти, реагувати на кіберінциденти та готуватися до них, забезпечуючи швидке відновлення як під час інцидентів, так і після їх завершення. Ці властивості можна окреслити одним терміном - кіберстійкість (cyber resilience, кіберрезилєнтність) [1]. Згідно затвердженого рішення Ради національної безпеки і оборони України "Про Стратегію кібербезпеки України" від 14 травня 2021 кіберстійкість визначається як набуття здатності швидко адаптуватися до внутрішніх і зовнішніх загроз у кіберпросторі, підтримувати та відновлювати стале функціонування національної інформаційної інфраструктури, насамперед об'єктів критичної інформаційної інфраструктури (ОКІІ). Багато з АСКТП мають відношення до функціонування об'єктів критичної інфраструктури.

Критичний інформаційний актив (КІА) – компонент ОКІІ, порушення цілісності якого або незабезпечення (авторизованого) доступу до якого безпосередньо вплине на стале функціонування ОКІ. Одним з найважливіших чинників, що впливає на топологію ОКІІ, є вибір базового архітектурного рішення – розгортання системи або на власному програмно-апаратному обладнанні підприємства, або в орендованій «хмарі». Через російські атаки на критичну інфраструктуру забезпечення доступу до КІА потребує використання найбільш витривалих комунікаційних технологій в умовах переривань електропостачання. Багато підприємств переглянули ставлення до конфіденційності чутливих даних в рамках завдань забезпечення безперервності бізнес-процесів на користь їх доступності, оскільки таким чином вони більше відповідають завданням безперервності бізнесу. Втім, хмарне рішення означає фактично передавання логічного доступу до даних ще одному учасникові ланцюжка постачання. Альтернативою рішенню on-premises та орендованої хмари є послуга *colocation* - розгортання КІА в спеціалізованому приміщенні центру обробки даних (ЦОД), але на обладнанні власника КІА. Розміщення власних апаратних серверів в ЦОД усуває загрози, пов'язані з конфіденційністю в хмарній інфраструктурі [2].

Сучасним підходом також є використання гібридної хмарної інфраструктури - комбінації приватного середовища (on-premises, приватна хмара або colocation), з публічною хмарою. Гібридна інфраструктура дозволяє зберігати конфіденційні дані локально в приватному середовищі,

тоді як програмні засоби та віртуальні машини можна розгорнути в публічній хмарі, серед переваг якої – швидке масштабування. Сучасні АСКТП мають гібридну архітектуру, в якій задіяні on-premises активи сумісно із приватними чи публічними хмарами, що є невід'ємними частинами певної платформи (це типово для промислового інтернету речей). Організаційні та технічні ризики, пов'язані з хмарними обчисленнями, детально викладено в рекомендаціях ENISA [3].

Основними елементами, що підтримують цілісну стратегію кіберстійкості є: кіберзахист (Cybersecurity), управління ризиками (Risk management), безперервність бізнесу (Business continuity), аварійне відновлення (Disaster recovery).

В ІКС в основі аварійного відновлення лежить відновлення цілісності та доступності даних за допомогою ***резервного копіювання*** — процесу створення копій критичних даних інформаційних систем для їх відновлення у разі втрати або пошкодження. Цей процес забезпечує безперебійність критичних операцій при технічних збоях, атаках чи фізичних пошкодженнях. Резервні копії включають дані операційних систем, баз даних, конфігурацій та образи віртуальних машин, конфігурацію мережевих пристроїв тощо [4]. Один із важливих етапів реалізації системи резервного копіювання — визначення ключових параметрів для оцінки її ефективності, надійності та внеску в кіберстійкість організації. Основні часові метрики включають RTO (Recovery Time Objective), що вказує на цільовий час відновлення після аварії, який залежить від апаратних параметрів та швидкості реакції персоналу, і RPO (Recovery Point Objective), що визначає максимальний час, протягом якого можуть бути втрачені дані без критичних наслідків для системи. Ці показники мають відмінності: RTO оцінює доступність сервісів, а RPO — частоту резервного копіювання та допустимі втрати даних.

Крім того, для можливості виконання ОКІІ своїх критичних функцій має бути забезпечений доступ до КІА для відповідних суб'єктів доступу ($СД_{КІА}$). Через російські атаки на критичну інфраструктуру забезпечення доступу до КІА потребує використання найбільш витривалих комунікаційних технологій в умовах переривань електропостачання. Критерієм витривалості може служити кількість активних точок ретрансляції, що потребують електроживлення. Обрання певного рішення з підвищення доступності залежить від пріоритетів власника системи. Три критерії є вхідними даними для оцінювання:

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

Окрім топології КІА, на кіберстійкість ОКІІ впливають різні комунікаційні технології так званої «останньої милі», що типово використовуються для підключення кінцевих споживачів: Ethernet, DOCSIS, ADSL, FTTB або FTTH, PON, різні супутникові системи широкосмугового

доступу (VSAT, Starlink, OneWeb). Ефективне обрання комбінацій з цих варіантів може потребувати ще більшої деталізації, яка має привести до розуміння переваги того чи іншого рішення по сукупності метрик *m*:

- можливість впровадження (m_1);
- швидкість впровадження (m_2);
- низька вартість впровадження (m_3);
- результативність впровадження (m_4).

Оскільки йдеться про критичну інфраструктуру, скоріше відновлення є найвищим пріоритетом. *Результативність* впровадження може бути відображена або в зменшенні часу на відновлення, або в зменшенні вартості відновлення в межах визначеного часу (recovery point objective, RPO).

Приклад: технологія побудови широкосмугових мереж доступу PON вважається найбільш стійкою до дефіциту електроенергії за умови забезпечення автономного живлення лише кінцевих точок. Таким чином, ця технологія забезпечить високу доступність даних при обміні між КІА та $СД_{КІА}$ в разі масштабних відключень електроенергії. Це має високу цінність, оскільки для ОКІ безперервність роботи (тобто швидше відновлення) є найвищим пріоритетом.

Важливим фактором є принципова можливість використання певних рішень для підвищення доступності доступу до мережі в конкретному приміщенні або на конкретній території. Спробуємо подати оцінку в числовій формі. Для цього ми присвоюємо кожному параметру деякі коефіцієнти (ваги). Приклади «зважування» заходів з підвищення кіберстійкості наведено в табл. 1 та табл.2.

Таблиця 1. Підхід до вимірювання кіберстійкості розташування КІА

Спосіб розташування	m_1	m_2	m_3	m_4	**Сума метрик** $m_2 - m_4$
on-premises	так	3	1	9	13
colocation	так	4	5	8	18
публічна хмара	ні	-	-	-	-
гібридне	так	2	3	6	14

Таблиця 2. Підхід до вимірювання кіберстійкості «останньої милі» доступу до КІА

Технологія	m_1	m_2	m_3	m_4	**Сума метрик** $m_2 - m_4$
ADSL	так	3	1	3	7
FTTB	так	3	3	1	7
PON	так	4	3	5	12
Starlink	так	2	1	5	8
LTE	так	1	2	2	5

Пелюсткова ідаграма на рис.1 дозволить візуально оцінити якість кожного рішення з точки зору запропонованих метрик.

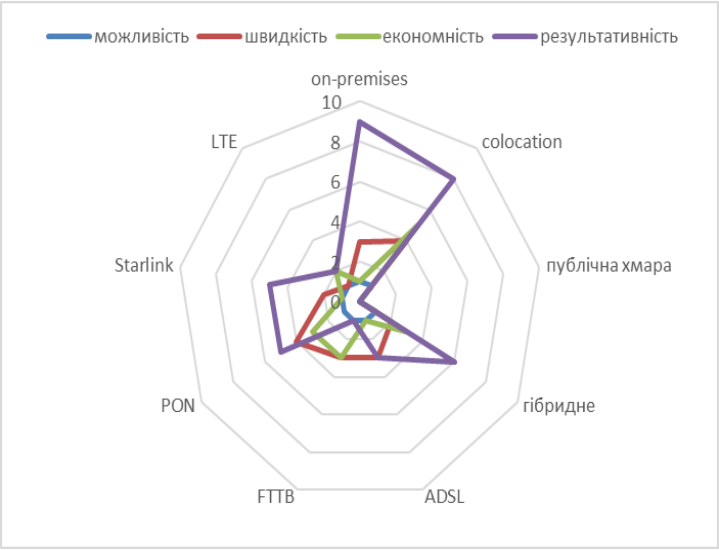


Рисунок 1 – Діаграма порівняння заходів підвищення кіберстійкості на прикладі запропонованих метрик

1. Swanson, M., Bowen, P., Wohl Phillips, A., Gallup, D., & Lynes, D. (2010, травень). Contingency Planning Guide for Federal Information Systems. nvlpubs.nist.gov. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf.
2. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України", Указ Президента України № 447/2021 (2021) (Україна). https://zakon.rada.gov.ua/laws/show/447/2021#Text.
3. Cloud Computing. Benefits, risks and recommendations for information security. URL: http://www.enisa.europa.eu/media/news-items/cloud-computing-speech (accessed: 11.11.2024).
4. What is Storage Area Network (SAN)? | VMware Glossary. (б. д.). VMware by Broadcom - Cloud Computing for the Enterprise. https://www.vmware.com/topics/storage-area-network-san.

С.Є. Саух

РЕЗИЛЬЄНТНІСТЬ ЕЛЕКТРОЕНЕРГЕТИЧНОЇ СИСТЕМИ В УМОВАХ МИРНОГО ЧАСУ ТА ВІЙСЬКОВИХ ЗАГРОЗ

Система — це набір взаємопов'язаних модулів або елементів, які працюють разом як єдине ціле для досягнення конкретної мети чи функції.

Функціональна стійкість системи підтримується шляхом управління її резервними механізмами та ресурсами, які використовуються для відповідного впливу на структурну організацію системи та процеси, що в ній відбуваються.

За умов недостатності резервних механізмів і ресурсів для управління структурою і процесами в системі поступово або повністю втрачається її здатність досягати певної мети чи функції, тобто система деградує до стану колапсу.

Нижче аналізуються особливості управління резервними механізмами та ресурсами в енергетичних та інформаційних системах. Також описано етапи деградації таких систем до стану колапсу.

ЕНЕРГЕТИЧНА СИСТЕМА

Деградація енергетичної системи – це поступове погіршення функціонування енергетичної інфраструктури, що призводить до зниження ефективності виробництва, розподілу та споживання енергії. Цей процес може супроводжуватися збоями в роботі енергетичних підприємств, зношеністю обладнання, недостатніми інвестиціями в модернізацію та збільшенням аварійності. Деградація може серйозно вплинути на стабільність енергопостачання та економічний розвиток регіону [1-6].

Колапс енергетичної системи – це раптова і різка зупинка значної частини енергетичної інфраструктури, що призводить до масових відключень електроенергії, зупинки виробничих процесів і порушення життєдіяльності населення. Колапс часто є результатом системних проблем, які накопичилися з часом і можуть бути спричинені технічними, природними чи людськими факторами.

Етапи деградації енергосистеми:

1. Початкова деградація:

На початкових етапах можливі незначні збої в роботі енергетичної інфраструктури, збільшення частоти аварій і зменшення обсягу інвестицій в обслуговування.

2. Прогресуюча деградація:

На цьому етапі проблеми набувають системного характеру: частішають аварії, проблеми з енергопостачанням у віддалених регіонах, подорожчають ремонти та обслуговування старої інфраструктури.

3. Енергетична криза:

Мають місце масові відключення електроенергії, брак потужностей для забезпечення енергетичних потреб населення та промисловості. Збільшується кількість аварій, падає ефективність виробництва та транспортування енергії.

4. Колапс енергетичної системи:

Обвал може статися в результаті масштабних технічних аварій, стихійних лих або військових дій. Це призводить до припинення енергопостачання великих регіонів, зупинки промислових підприємств і життєво важливих об'єктів інфраструктури.

ІНФОРМАЦІЙНА СИСТЕМА

Деградація інформаційної системи – це процес поступового зниження її функціональності, ефективності та надійності. Деградація проявляється у зниженні швидкості обробки даних, частіших помилках у роботі, зниженні безпеки та стійкості системи до зовнішніх загроз. Деградація може статися через знос технічних ресурсів, застаріле програмне забезпечення або неправильне керування системою.

Колапс інформаційної системи – критичний момент, коли система повністю втрачає здатність виконувати свої функції. Колапс супроводжується відмовою ключових компонентів, втратою даних, неможливістю обробки інформації або доступу до неї.

Етапи деградації інформаційної системи:

1. Початкова деградація:

Повільна продуктивність системи, частіші збої або затримки через технічні проблеми або застаріле програмне забезпечення. На цьому етапі система все ще працює, але її надійність і продуктивність поступово знижуються.

2. Прогресуюча деградація:

Система починає частіше давати збої, з'являються серйозні проблеми з доступом до інформації або її обробкою. Збільшується кількість помилок в програмному забезпеченні, і користувачі починають відчувати значні незручності в роботі з системою.

3. Інформаційна криза:

Відбуваються масові збої в роботі ключових компонентів системи, що призводить до перебоїв у роботі підприємств чи установ, які залежать від цієї інформаційної системи. Без негайного втручання система може повністю вийти з ладу.

4. Колапс інформаційної системи:

Повний збій системи через технічні чи програмні проблеми, кібератаки чи катастрофічні події. Втрата можливості доступу до даних, обробки інформації та підтримки зв'язку між елементами системи.

З аналізу процесів деградації та колапсу систем різної природи стає зрозумілою важлива роль управління резервними механізмами та ресурсами, наявними в таких системах.

Обмежена дія резервних механізмів і обсяг резервних ресурсів, а також обмежена швидкість їх активного використання для локалізації та усунення негативних зовнішніх і внутрішніх впливів на систему призводять до тимчасової часткової або повної втрати функціональних властивостей системи.

Наявність достатнього резерву механізмів і ресурсів для швидкого відновлення функціональних властивостей системи свідчить про її резильєнтність. Зазначимо, що важливою характеристикою резильєнтності є тривалість процесів адаптації та відновлення системи. Якщо тривалість таких процесів менша від періодичності негативних впливів на систему, що порушують її функціональну спроможність, то така система не є резильєнтною.

Для ілюстрації на рис. 1 та 2 наведено графіки готовності електроенергетичної системи (ЕЕС) до виконання своїх функцій у мирний та у воєнний час відповідно.

При плануванні енергетичної системи враховувалися різноманітні фактори негативного впливу на її функціонування лише в умовах мирного часу, такі як техногенні аварії, стихійні лиха, антропогенний вплив та інші. Для забезпечення резильєнтності ЕЕС передбачені резервні механізми та ресурси, достатні для своєчасного реагування на негативні впливи [1-2, 4-6].

Проте наявність таких резервних механізмів і ресурсів недостатня для підтримки готовності ЕЕС до виконання своїх функцій в умовах воєнної загрози. Якщо частота ракетних атак менша за тривалість процесів адаптації та відновлення системи, то така ЕЕС втрачає свою резильєнтність.

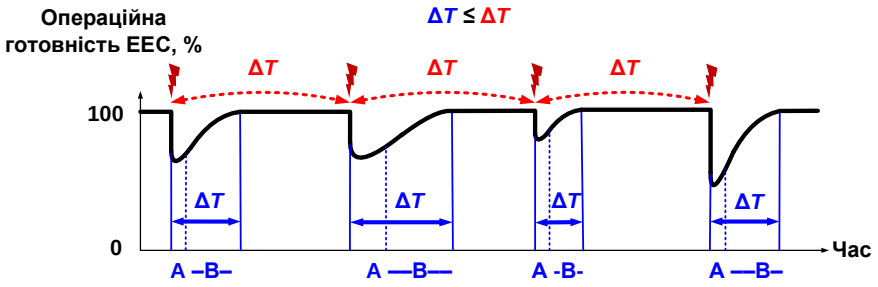


Рисунок 1 – Наявні в ЕЕС резервні механізми управління та ресурси достатні для швидкого реагування на негативні зовнішні чи внутрішні деструктивні впливи. Тривалість процесів адаптації (А) та відновлення (В) системи менша за періодичність деструктивних впливів

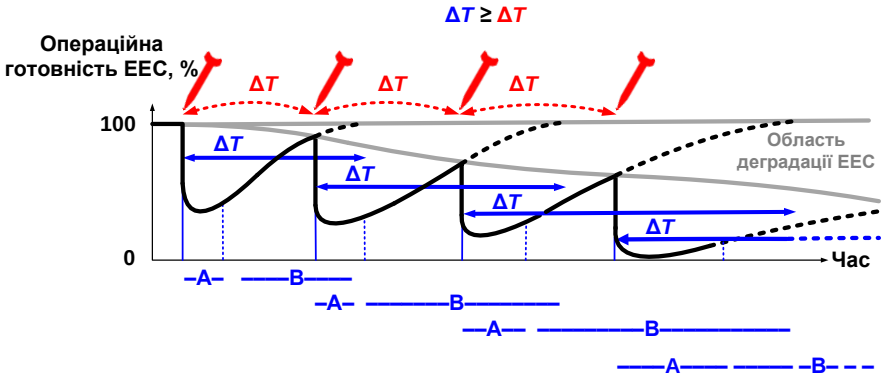


Рисунок 2 – Управління резервними механізмами та ресурсами, наявними в ЕЕС, недостатнє для швидкого реагування на руйнівні наслідки ракетних ударів. Тривалість процесів адаптації (А) та відновлення (В) системи є меншою за частоту ракетних ударів, що призводить до деградації системи і, в кінцевому підсумку, до її колапсу

Забезпечення надійного, безпечного та доступного постачання електроенергії має важливе значення для економічного зростання та розвитку. Як правило, електроенергетична система знаходиться під постійною загрозою низки природних, техногенних та антропогенних впливів, які можуть спричинити будь-яке: від перебоїв з електроенергією до хронічної нестачі електроенергії. Для розробників енергетичної політики, проектувальників та системних операторів надзвичайно важливою є проблема захисту електроенергетичної системи, яка вирішується шляхом планування та інвестування у підвищення резильєнтності її функціонування та розвитку.

Комплексне планування сталого розвитку енергетичного сектору передбачає визначення майбутніх загроз і критичних навантажень на ЕЕС, а також можливостей підготовки та адаптації до них. Планування сталого розвитку електроенергетики передбачає розробку стратегії пом'якшення наслідків реалізації таких загроз, тобто стратегії розвитку резильєнтності ЕЕС [7-9].

1. Stout S., Lee N., Cox S., Elsworth J. and Leisch J., “Power sector resilience planning guidebook,” U.S. Department of Energy’s NREL and USAID, 2019.
2. Lei S., Wang C. and Hou Y., “Power Grid Resilience against Natural Disasters: Preparedness, Response, and Recovery,” Wiley-IEEE Press, 2023.
3. Narayanan A., Welburn J. W., Miller B. M., li S. T., Clark-Ginsberg A., “Deterring Attacks Against the Power Grid. Two Approaches for the U.S. Department of Defense,’ RAND Corporation, Santa Monica, Calif., 2020.

4. Yao X., Wei H. H., Shohet I. M. and Skibniewski M. J., “Assessment of Terrorism Risk to Critical Infrastructures: The Case of a Power-Supply Substation,” Applied Sciences, vol. 10 (20), 2020, 7162.
5. Bhusal N., Gautam M., Abdelmalak M. and Benidris M., "Modeling of Natural Disasters and Extreme Events for Power System Resilience Enhancement and Evaluation Methods," 2020 International Conference on Probabilistic Methods Applied to Power Systems (PMAPS), Liege, Belgium, 2020, pp. 1-6.
6. Bhusal,N., Abdelmalak M., Kamruzzaman M. and Benidris M., "Power System Resilience: Current Practices, Challenges, and Future Directions," in IEEE Access, vol. 8, 2020, pp. 18064-18086.
7. Саух С.Є., "Концепція побудови структурно мінливої електроенергетичної системи України" // Технічна електродинаміка, – 2023. – N 5. – С. 48 – 54. – DOI: https://doi.org/10.15407/techned2023.05.048.
8. Saukh S, "A Structurally Variable Electric Power System Resistant to Terrorist and Military Threats," 2023 IEEE 13th International Conference on Dependable Systems, Services and Technologies (DESSERT), Athens, Greece, 2023, pp. 1-5, DOI: 10.1109/DESSERT61349.2023.10416549.
9. Саух С.Є. Концепція забезпечення жорсткої стійкості електроенергетики України в умовах терористичних та мілітарних загроз // Електронне моделювання. – 2023. – N 3. – С. 3 – 10. – DOI: https://doi.org/10.15407/emodel.45.03.003.

РЕЗИЛЬЄНТНІСТЬ СИСТЕМ ЗА ДАНИМИ ІНДИКАТОРІВ

Хоча природа даних відрізняється від природи фізичних товарів, перенесення практик загального менеджменту якості (Total Quality Management, TQM) та ощадливого менеджменту (Lean Management) на ресурси даних є корисним і вигідним для промислового підприємства [1].

Уможливлювані зміни в менеджменті ресурсів даних (Data Resource Management, DRM) потребують постійного обгрунтування засобів реалізації для досягнення інвестиційних цілей. Витрати є досить прозорими, оскільки можуть безпосередньо розподілятися на окремі діяльності, інструменти і системи такого менеджменту. Водночас виграші від такого менеджменту не є помітними, оскільки матеріалізуються в різноманітті різних процесів і продуктів. Можна застосувати підхід Золотого кола (Golden Circle) [2], щоб проілюструвати, чому DRM потрібний промисловому підприємству (через ринкові зміни, вимоги клієнтів, регуляторні положення), як DRM впливає на його стратегічне положення (спроможність менеджменту даних підприємства (Enterprise Data Management, EDM)), що треба робити для управління ресурсами даних (керовані даними (data-driven) процеси, продукти та послуги, товари). Цей підхід, що запровадив бізнес-консультант Саймон Сінек, часто використовується в управлінському консалтингу (Management Consulting) і стартап-компаніях.

Можливості EDM досліджували 5 експертів Німеччини від Fraunhofer ISST та Robert Bosch GmbH [3]. Щоб максимізувати ділові виграші від ресурсу даних, ним слід управляти так само, як будь-яким іншим ресурсом на промисловому підприємстві.

EDM − це організаційна спроможність, яка забезпечує управління ресурсом даних відповідно до стратегічної мети підприємства. За підходом Золотого кола, EDM відповідає на питання, що слід встановлювати на підприємстві для того, щоб скористатися діловими перевагами даних.

Отже, створення EDM − це завдання організаційного проектування, яке вимагає розгляду з перспектив і) спроможності, іі) врядування, ііі) динаміки.

і) Перспектива спроможності (у вужчому сенсі) пов’язана з ідентифікуванням і встановленням організаційних можливостей, необхідних для ефективного й дієвого менеджменту ресурсом даних. Перші еталонні моделі для менеджменту даних на рівні підприємства були розроблені у 1990-х роках, зокрема Органом знань з менеджменту даних (Data Management Body of Knowledge) від DAMA [4]. Науково обгрунтовані моделі були надані Центром компетенції з якості корпоративних даних (Competence Center Corporate Data Quality) [5].

іі) Перспектива врядування пов’язана з тим, які рішення кому і де слід приймати на промисловому підприємстві. Тому врядування даних − це

фреймворк прийняття рішень для найкращого використання ресурсу даних [6, 7]. Наявність даних уможливлює застосування ШІ.

iii) Перспектива динаміки виходить з динамічного середовища, в якому мають встановлюватися організаційні спроможності. Тому надзвичайно важливо неперервно переглядати й запроваджувати EDM у термінах індивідуальних спроможностей та налаштування врядування.

Підхід ділової інженерії (Business Engineering), який розробив Інститут менеджменту інформації (Institute for Information Management) при Університеті Санкт-Галлена (Швейцарія), є функціональним засобом для організації різних спроможностей EDM [8]. Слід зазначити увагу цього університету до сучасних практик менеджменту, зокрема до практики Володимира Кличка. Виділяють 3 рівні ділової інженерії:

1. стратегічний менеджмент даних;

2. менеджмент ланцюгів створення вартості даних;

3. менеджмент основ даних.

Кожний такий рівень містить відповідні спроможності EDM, важливі для всього підприємства:

1.1. стратегія даних;

1.2. культура даних;

1.3. врядування даних;

1.4. облік і менеджмент вартості даних;

1.5. менеджмент продуктів даних;

1.6. відповідність даних (data compliance);

2.1. збір, створення, придбання даних;

2.2. каталогізація даних;

2.3. зберігання даних;

2.4. розподіл даних;

2.5. використання даних (аналітика даних і ШІ; керовані даними продукти, послуги, процеси; продукти даних);

2.6. обмін даними;

2.7. посилання на дані (data referencing);

2.8. технічне обслуговування та курація (curation) даних;

3.1. менеджмент архітектури даних;

3.2. менеджмент майстер-даних (довідкових даних);

3.3. безпека даних і захист даних;

3.4. менеджмент якості даних;

3.5. менеджмент платформ даних і просторів даних.

Таким чином, промислове підприємство має створювати ці спроможності, щоб скористатися потенціалом конкурентних переваг ресурсів даних. Врядування даних (1.3.) − це не стільки інструмент керування, скільки інструмент координації. Таке врядування потрібне для

врегулювання порушень функціональності, властивих будь-якому організаційному дизайну (організаційній структурі, організації процесів, міждисциплінарній взаємодії). Знаходження найкращої домовленості про врядування є складним завданням, зокрема в багатонаціональних промислових підприємствах.

Погляд врядування на EDM стосується прав прийняття рішень, підзвітності, відповідальності та їх розподілу в організації. Знаходження правильної домовленості про врядування даних має балансувати такі виміри:

дизайн (наприклад, встановлення стандартів даних, стандартів API тощо) відносно операцій (наприклад, виконання завдань обслуговування даних);

централізовані підрозділи відносно децентралізованих;

ділові аспекти відносно юридичних та IT-аспектів.

EDM − це організаційна спроможність, що стосується оптимального менеджменту і використання ресурсу даних. Окремі спроможності EDM і домовленості про врядування даних необхідно неперервно оцінювати і вдосконалювати, щоб адекватно реагувати на внутрішні та зовнішні зміни.

У той час як EDM (разом з усіма організаційними спроможностями) необхідно постійно адаптувати до внутрішньої та зовнішньої динаміки, у новому тисячолітті можна виділити такі рушійні сили змін: I) дані є ресурсом для ШІ; II) дані вважаються економічним товаром; III) дані формують екосистеми; IV) внутрішній та зовнішній EDM інтегруються; V) культура даних поліпшується; VI) ланцюг створення вартості даних стає замкнутим циклом (closed-loop cycle).

У новому тисячолітті майстерність і зрілість спроможностей EDM на промислових підприємствах невпинно зростають. Дослідження важливості даних для ділового успіху ведуть до більшої уваги для управління ресурсом даних на рівнях прийняття рішень компаній. Запропоновано поняття менеджменту даних атаки й оборони, щоб наголошувати на зміненій ролі даних для ділового успіху [9]. Докладніші дослідження підтверджують твердження, що дані розвиваються від побічного продукту інтеграції ділових процесів до стратегічного ділового ресурсу [10].

Проте загальна зрілість EDM в ЄС загалом і Німеччині зокрема характеризується значним простором для вдосконалення. Федеральне міністерство економіки Німеччини фінансувало проект DEMAND [11], який проводили принаймні 25 експертів від 7 організацій Німеччини (консорціум) – Fraunhofer-Institut für Software und Systemtechnik ISST, Institut der deutschen Wirtschaft, thyssenkrupp Industrial Solutions AG, thyssenkrupp Steel Europe AG, BREUER Nachrichtentechnik GmbH, IW Consult, Advaneo GmbH. Цей проект запровадив підхід Data Readiness, за яким близько 80% компаній Німеччини перебували на одному з двох найнижчих рівнів готовності до даних. Цей підхід для моделювання використовує 6 кроків готовності [12]: (0) аналогова компанія; (1) оцифрована компанія; (2) цифровізована (digital-enabled)

компанія; (3) цифрова компанія; (4) цифрова мережа; (5) цифрова екосистема. Модель готовності надає рекомендації для переходу на вищий рівень зрілості, а тому є функціональним засобом компаній для подальшого вдосконалення своїх спроможностей EDM.

Промислові підприємства мають постійно оцінювати зрілість своїх спроможностей EDM, щоб просувати вміння управління даними як стратегічним ресурсом і максимізувати внесок даних у досягнення цілей компанії, зокрема цілей керованості, стійкості, надійності та резильєнтності. [13−15]. Дані індикаторів пов'язують керованість і резильєнтність системи.

1. Otto B. Quality and value of the data resource in large enterprises. *Information Systems Management*. 2015. 32 (3). P. 234–251.
2. https://simonsinek.com/golden-circle/.
3. Otto B., Grafen D., Krammer L., Gröger C., Lutsc A. *Enterprise Data Management. Building core competencies to unlock data-driven business opportunities and the potential for competitive advantage. White Paper.* Dortmund, Germany: Fraunhofer-Institut für Software und Systemtechnik ISST, 2024. 8 p.
4. https://www.dama.org/cpages/body-of-knowledge.
5. https://www.cdq.com/about/competence-center-corporate-data-quality.
6. Khatri V., Brown C.V. Designing data governance. *Communications of the ACM*. 2010. 53 (1). P. 148−152.
2. Otto B. A morphology of the organisation of data governance. *Proceedings of the European Conference in Information Systems (ECIS) 2011*. Paper 272. 12 p. https://aisel.aisnet.org/ecis2011/272/.
3. *Business Engineering: Auf dem Weg zum Unternehmen des Informationszeitalters*. H.Österle, R.Winter (eds.). 2nd ed. Springer, 2003. 415 p. (In German)
4. DalleMulle L., Davenport T.H. What's your data strategy?. *Harvard Business Review*. 2017, May−June. P. 112−121.
5. Legner C., Pentek T., Otto B. Accumulating design knowledge with reference models: insights from 12 years' research into Data Management. *Journal of the Association for Information Systems*. 2020. 21 (3). P. 735−770.
6. Otto B., Korte T., Azkan C., Spiekermann M., Lis D., Gelhaar J., Iggena L., Meisel L., Trautmann B., Fiedler J., Bresser P., Müller N., Goecke H., Demary V., Engels B., Fritsch M., Krotova A., Rusche C., Scheufen M., Thiele C., Lichtblau K., Schmitz E., Aliu O., Bretfeld J., Mihailidis E. *DEMAND. Data Economics and MANagement of Data-driven business. White Paper. Data Economy Status Quo der Deutschen Wirtschaft & Handlungsfelder in der Data Economy*. Dortmund, Germany: Fraunhofer-Institut für Software und Systemtechnik ISST, 2019. 53 p.
7. https://www.demand-projekt.de/paper/Gutachten_Readiness_Data_Economy.pdf.
8. Gorbachuk V.M., Suleimanov S.-B., Batih L.O. Integrated resilient strategies of renewable power generation and distribution. *Наука і техніка сьогодні*. 2022. № 4 (4). P. 113−125.
9. Горбачук В.М., Лупей М.І., Дунаєвський М.С. Підходи до резильєнтності критичних інфраструктур. Science and education for sustainable development. A.Ostenda, V.Smachylo (eds.) Katowice, Poland: University of Technology, Katowice, 2022. P. 87−95.
10. Gorbachuk V., Dunaievskyi M., Lupey M. Innovative approaches to measuring system resilience. *Contemporary technologies and society: innovations, artificial intelligence, and challenges*. V. Yuskovych-Zhukovska, O. Bogut (eds.). Katowice, Poland: Academy of Silesia, 2023. P. 476−482.

С.Д. Винничук, Л.О. Митько

ПРО ОДИН ПІДХІД ДО РЕЗИЛЬЄНТНОСТІ СИЛОВИХ ЕНЕРГЕТИЧНИХ УСТАНОВОК

Аналізуючи сучасний стан виробництва, призначень, застосування та перспектив розвитку галузі силових енергетичних установок (СЕУ), можна констатувати залежність вимог до засобів управління та спостереження від технологічних вимог та енергетичних параметрів силової частини СЕУ. Урахування особливостей комп'ютерно-інтегрованих систем приводить до необхідності надання методам і засобам моделювання адаптуючих можливостей, що в свою чергу породило створення адаптивних методів і засобів математичного та комп'ютерного моделювання процесів їх функціонування для дослідження і забезпечення якісних показників вказаного класу систем, ефективного розв'язання задач аналізу, синтезу та побудови засобів керування і діагностики з урахуванням обмежень до інформаційних ресурсів.

Сучасний рівень комп'ютеризації СЕУ визначається поточними завданнями і можливостями комп'ютерної техніки. До найпоширеніших завдань належать: проектування установок (при цьому широко відомий важливий недолік дорогих автоматизованих систем проектування – відсутність достатнього набору засобів модельної підтримки); обробка результатів випробувань (виконується автономними засобами); супровід результатів профілактики; реєстрація результатів вимірювань у контрольних точках при діагностиці та контролі; забезпечення процесів управління (використовуються регулятори, які досить часто не здатні враховувати властивості об'єкта).

Насичення СЕУ вбудованими комп'ютерними засобами дозволить вирішувати комплекс визначених завдань та забезпечення інтелектуальних функцій. Поява можливості вирішення складних та специфічних завдань вимагає розробки ефективних математичних та комп'ютерних моделей даного класу об'єктів. Ця обставина породжує таку вимогу до комп'ютерних моделей, як здатність роботи в реальному часі за обмеженими обчислювальними ресурсами.

Розробка адаптивних методів математичного забезпечення систем управління, контролю та діагностики комп'ютерно-інтегрованих автономних СЕУ на основі розвитку та застосування нових, перспективних підходів до побудови якісних та економічних моделей процесів у СЕУ, організації структур та алгоритмічно-програмного забезпечення систем управління та спостереження за станом функціонування СЕУ, передбачає покращення якісних показників функціонування комп'ютерно-інтегрованих СЕУ[1]. Розглядаючи побудову сучасних СЕУ у вигляді комп'ютерно-інтегрованих систем, у тому числі із вбудованим виконанням комп'ютерної частини, запропоновано використовувати наступні принципи.

1) Принцип альтернативності форм моделей динаміки об'єкта керування (лінійного або нелінійного), що забезпечує отримання оптимальних за складом і адекватних математичних описів; надає можливості широкого вибору однієї із форм можливих математичних представлень, які не дивлячись на аналітичну еквівалентність, можуть суттєво розрізнятись за критерієм обчислювальної складності, оскільки реалізуються за допомогою різних за своєю якістю обчислювальних схем.

2) Принцип керування за еталонною моделлю, що допомагає побудувати структури системи керування з урахуванням властивостей об'єкта. При цьому використовується метод побудови керуючого каналу зворотного зв'язку на основі еталонної моделі, що формує керуючий вплив за принципом неперервного відслідковування поведінки моделі без застосування оптимізаційних обчислень.

3) Модельно-орієнтований підхід до побудови систем контролю і діагностики, згідно з яким стан об'єкта спостереження порівнюється, а потім оцінюється розходженням між поточними і номінальними його параметрами, що відображаються відповідними моделями. Тобто відбувається діагностування неперервних систем за принципом виявлення несправності шляхом побудови (ідентифікації) моделі поточного стану несправного фрагменту системи і порівняння значень її параметрів з їх номінальними значеннями, який забезпечує виявлення широкого класу можливих несправностей при обмеженому доступі до внутрішніх елементів системи.

4) Принцип оптимізації алгоритмів, згідно якого створені обчислювальні процеси реалізації математичних моделей отримання керуючих сигналів чи впливів, що сприяє розробці алгоритмів та відповідних програмних засобів необхідної точності і мінімальної складності.

Розроблені адаптаційні методи формування динамічних моделей комп'ютерно-інтегрованих систем з урахуванням альтернативностей їх можливих форм, що сприяють адаптаційній побудові необхідної моделі за принципом мінімальної складності при заданих вимогах до показників якості (точності). В результаті проведеного аналізу виділено клас адаптивних систем з еталонною моделлю як такий, що забезпечує високу адекватність синтезованого управління (з точністю до відтворення моделлю динаміки реального об'єкта), високу швидкодію (управління формується в реальному масштабі часу) та просту апаратну реалізацію. Досліджено також можливість застосування програмних засобів (програмної платформи Matlab) для розв'язання задачі синтезу адаптивного управління об'єкту.

Створення таких систем із застосуванням адаптаційних методів із використанням процесів оптимізації сприяють резильєнтності СЕУ.

1. Верлань А.Ф. Инновационный подход к организации процессов функционирования силовых энергетических установок Сборник научных статей XXV Международной научно-практической конференции "Инновация – 2021", Ташкент, "Инновацион ривожланиш нашриет-матбаа уйи", 2021, с. 46-49.

I. Furtat, Yu. Furtat

ADAPTATION OF INFORMATION INTERACTION «USER-SYSTEM» AS A WAY TO INCREASE THE RESILIENCE OF AUTOMATED CONTROL SYSTEMS

Modern automated control systems (ACS) are human-machine systems with a complex structure, focused on performing a wide range of functions. This determines certain features of working with information in such systems, its storage and processing. Due to the significant amount of information with which operators of automated systems must interact in the process of work, often in conditions of limited time for decision-making, information overload of operators occurs, which negatively affects the quality of their work and the resilience of the ACS [1]. To solve the problem of reducing the efficiency of information interaction of the user with the system, the possibility of creating a model of the information interaction process, algorithmization and implementation of the process of adapting the characteristics of information flows coming from the system to the operator to the individual characteristics of the operator and the workflow is considered.

A number of models are proposed [2-4] to algorithmize and implement the process of adapting the user's information interaction with the system. The adaptation process is implemented as management of interconnected parameters of entity models participating in the process of information interaction.

Information flow I from the system can be described as a set of parameters:

$$I = \langle T, F, C, D \rangle, \quad (1)$$

where T is the rate of information delivery, F is the data presentation format, C is the complexity of the information, its connection with other data blocks, D is the data being transmitted.

The pace of information presentation in the ACS can be controlled in non-critical situations by changing the intensity of information presentation to the user depending on the permissible level of information load. The desired pace for the user is determined by his ability to quickly respond to data from the system, as well as the current level of fatigue and concentration. The format of information presentation can be text, graphic, tabular, audio, combined. In general, the format of data presentation is determined by a set of user interface output elements, but provided that this set can be changed in accordance with the needs and requirements of the user, the presentation format can also be adapted to the features of the user's perception of information (his cognitive portrait). Information complexity is a complex characteristic that takes into account the connections between data blocks in the subject area model, the number of connections and blocks involved in a given episode of data presentation, as well as their overlap with the user's knowledge model. Parameter D – a fragment of information transmitted to the user in a given episode of the workflow. This fragment may correspond to one block of data in the subject area,

or may represent a set of blocks or part of a separate block, depending on the scenario of user interaction with the system.

The user interface in automated systems is considered as a collection of output elements, $UI = \langle E_i \rangle$, $i = \overline{1,n}$, each output element

$$E_i = \left\langle \langle x, y \rangle_i^j, T_i, c_i \right\rangle, \; j = \overline{1,m} \qquad (2)$$

where $\langle x, y \rangle_i^j$ – coordinates of the vertex of the boundary of the output element in the user interface window, T_i – type of output element, c_i – criticality of *the i* -th output element for user work.

The set of values of the parameter T_i in model (2) coincides with the set of values of the parameter F model (1), and it is the type of output elements available in the user interface window that determines the desired data format when forming the information flow.

The criticality of an output element is determined by the specifics of the workflow. Critical elements include elements whose loss of information leads to disruption of the workflow or the inability of the user to correctly process information from the system.

Controlling the placement of output elements and their type allows you to create a personalized user interface to adapt the user's information interaction with the ACS. Critical output elements must be present in the working interface window, regardless of its adaptation.

Personalization of the user interface and management of information flow parameters allow you to configure the process of information interaction in the system, taking into account the individual characteristics of the user and the features of the workflow (work scenario in the system, subject area, etc.), reduce the risk of information overload for the ACS operator, which has a positive effect on the resilience of the system.

1. Wickens, C. D. (2000) Imperfect and Unreliable Automation and Its Implications For Attention Allocation, Information Access and Situation Awareness. Technical Report ARL-00-10/NASA-00-2, Aviation Research Lab Institute of Aviation in University of Illinois.
2. Liu, Jiming, & Kuen, Chi, & Ka, Wong, & Hui, Keung. (2003) An Adaptive User Interface Based on Personalized Learning. IEEE Intelligent Systems, 18(2), 52-57.
3. Xue, Qing, & Han, Xuan, & Li, Mingrui, & Liu, Minxia. (2014). A Conceptual Architecture for Adaptive Human-Computer Interface of a PT Operation Platform Based on Context-Awareness. Discrete Dynamics in Nature and Society, 2014(2014), 35-47.
4. Reinecke, K. (2010). Culturally Adaptive User Interfaces: dissertation. Faculty of Economics, Business Administration and Information Technology of the University of Zurich.

F. Korobeynikov

BEYOND RISK PREDICTION: THEORETICAL FOUNDATIONS OF ADAPTIVE RESILIENCE

Traditional approaches to ensuring the security of socio-technical systems, based on risk prediction and threat prevention, demonstrate critical limitations in the context of unprecedented growth in system complexity, emergence of fundamentally new types of threats, increasing rate of environmental changes, and global interconnectedness of information and socio-technical systems, where local incidents can trigger cascade effects with catastrophic consequences.

The purpose of this paper is to provide a concise conceptual and terminological description of a new security paradigm based on the principles of adaptive resilience.

In this context, ***resilience*** is defined as the ability of a complex open, nonlinear, dissipative system to maintain fundamental invariants and perform critical functions under conditions of deterministic chaos and bifurcation phenomena (caused by environmental changes and destructive factors), ensuring directed self-organization, evolution, and selection of optimal development trajectories within the space of permissible states through the enhancement of adaptive potential and entropy dissipation mechanisms.

The invariants of a socio-technical system comprise a set of fundamental structural-functional characteristics and attributive properties that determine the ontological essence of the system and define the boundaries of permissible morphogenesis during adaptation. Changes in these invariants result in either loss of system identity or degradation of the system's target function.

Based on interdisciplinary analysis integrating complex systems theory, the concept of adaptation energy, and the method of correlation adaptometry, we have formulated definitions for the key concepts of the paradigm. The mechanisms for ensuring resilience through adaptive potential management are proposed, encompassing structural plasticity, resource flexibility, and fractal diversity in the implementation of critical functions. This developed approach establishes a theoretical foundation for designing next-generation security systems capable of utilizing uncertainty as a developmental factor.

A key element of the proposed approach to ensuring resilience is the iterative enhancement of adaptive potential, which includes determining critical stability thresholds, assessing the current level of adaptive resources, and forecasting their depletion. Here, ***adaptive potential*** is defined as an emergent characteristic of a complex system that determines its capacity for structural-functional reconfiguration and modification of connection topology in response to exogenous and endogenous stressors. The concept of adaptive potential is grounded in H.Selye's adaptation energy theory, first proposed in 1938 [1].

For quantitative assessment of the adaptive potential level, the correlation adaptometry method [2] is proposed, which is based on analyzing correlations

between system parameters during adaptation and their variances, enabling evaluation of the system's state under external factors. The method builds upon the observation that the degree of complex systems' adaptation is reflected in changes of correlations between their key parameters. Studies of correlation and variance dynamics in systems adapting to environmental factor loads revealed a universal effect in ensembles of systems under similar factor loads: during crisis, typically before the appearance of obvious system destruction symptoms, both correlation and variance (and volatility) increase. However, successful adaptation leads to their reduction.

In light of the aforementioned evidence, it can be posited that the management of correlations and variances in key system parameters facilitates the intentional enhancement of its adaptive capacity, which is a pivotal factor in ensuring the resilience of socio-technical systems in the face of high uncertainty. Rather than allocating resources towards predicting the probability and consequences of risk realisation in conditions of fundamental unpredictability [3], it would be more prudent to direct efforts towards the development of the adaptive potential of socio-technical systems. This entails:

- Development of structural plasticity, defined as the system's ability for rapid dynamic reconfiguration of internal connections and processes. Structural plasticity is characterized by three primary parameters: reconfiguration speed, depth of possible changes, and transformation reversibility. Reconfiguration speed determines the system's ability to respond promptly to environmental changes through restructuring of internal interconnections. The depth of changes characterizes the scope of possible structural transformations without loss of system functionality. Reversibility defines the system's ability to return to its initial configuration after the cessation of stress factors. High levels of structural plasticity ensure system adaptation to a broad spectrum of impacts through optimization of internal organization. A key factor here is maintaining functional integrity during structural transformations, achieved through preservation of critical interconnections while simultaneously modifying auxiliary structures.
- Development of system resource flexibility. This mechanism encompasses two primary components: optimization of existing entropy dissipation resources and development of capability to detect and utilize new resource sources. Resource flexibility involves not only effective management of available resources but also the system's ability to redistribute resource flows in response to changes in external environment and internal system state. Of particular importance is the optimization of entropy dissipation processes, enabling the system to maintain a stable non-equilibrium state with minimal resource expenditure. A critical factor here is the system's ability to identify and engage alternative resource sources before existing ones are depleted, ensuring operational continuity under resource constraints.
- Iterative testing with sub-threshold stressors. This method is based on modeling critical scenarios that could potentially lead to irreversible loss of system functionality. A fundamental feature of the method is not only the assessment of

current resilience levels but also the purposeful stimulation of the system's adaptive mechanisms development. During operation at the boundary of maximum capabilities, activation of latent system resources occurs, along with the formation of alternative pathways for critical functions implementation and enhancement of recovery mechanisms. Each iterative test acts as a catalyst for evolutionary changes in the system, stimulating qualitative development of its adaptive capabilities. A crucial factor in this mechanism's effectiveness is precise calibration of stressor intensity: they must be sufficiently strong to stimulate adaptive processes while not exceeding critical thresholds beyond which irreversible system degradation begins.

A significant aspect is the existence of critical thresholds beyond which the system loses its capacity for recovery and adaptation. This necessitates proper management of adaptation energy expenditure to prevent its depletion. Statistical evidence indicates that system destruction is frequently caused not by a single powerful impact, but by the cumulative effect of a series of less significant stresses that exhaust the adaptive potential.

To overcome critical thresholds, the concept of diversity in critical function implementation is proposed. Diversity represents a system organization principle wherein each critical function is supported by multiple independent implementation pathways. In essence, this represents a fractalization of critical function implementation paths, where each path maintains its own redundancy system. Such organization ensures system resilience to local failures and continuity of critical functions during disruptions in individual components.

The integration of the described mechanisms: structural plasticity, resource flexibility, and diversity - forms a new type of system architecture, capable not only of maintaining stability under uncertainty but also of utilizing stress impacts as a stimulus for development.

1. Selye, H. (1938). Experimental evidence supporting the conception of "adaptation energy". American Journal of Physiology-Legacy Content, 123(3), 758–765. https://doi.org/10.1152/ajplegacy.1938.123.3.
2. Gorban, A. N., Tyukina, T. A., Pokidysheva, L. I., & Smirnova, E. V. (2021). Dynamic and thermodynamic models of adaptation. Physics of Life Reviews, 37, 17–64. https://doi.org/10.1016/j.plrev.2021.03.001.
3. Korobeynikov, F. (2024). Building resilience through risk management: methodology and strategy. International Science Journal of Engineering & Agriculture, 3(4), 78–85. https://doi.org/10.46299/j.isjea.20240304.08.

В.С. Коберник, Д.С. Матушкін

РЕЗИЛЬЄНТНІСТЬ СИСТЕМ ЦЕНТРАЛІЗОВАНОГО ТЕПЛОПОСТАЧАННЯ

Системи централізованого теплопостачання відносяться до критичної інфраструктури України. Централізоване теплопостачання (ЦТ) в Україні потребує термінового підвищення стійкості для усунення пошкоджень внаслідок війни, зменшення все зростаючих витрат на теплопостачання і зменшення втрат теплової енергії. Вибір напрямку розвитку систем теплозабезпечення України потребує врахування досвіду країн ЄС, які значно випереджають нашу країну у розвитку енергетичної сфери. У роботі [1] було частково розглянуто сонячне теплопостачання об'єктів критичної інфраструктури. Розглянемо використання сонячної енергії та теплових насосів для централізованого теплопостачання.

1. Сонячне централізоване теплопостачання.

Системи сонячного опалення застосовують у країнах, де існують мережі ЦТ, часто з холодним кліматом з високим попитом на тепло взимку. У рамках нової Директиви про енергоефективність, яку запропонувала Єврокомісія, всі європейські муніципалітети з населенням понад 50 тис. жителів мають розробити дорожні карти з розвитку систем опалення та охолодження на основі ВДЕ відповідно до законодавства ЄС.

Доцільність використання сонячного опалення в холодних кліматичних умовах доведена багаторічним досвідом використання таких систем. На цей час 282 міста в Європі використовують сонячне ЦТ і демонструють його ефективність. Містам із централізованим опаленням слід ознайомитися з прикладом Данії, яка є лідером серед країн ЄС по впровадженню сонячного ТЦ, де вироблене влітку тепло зберігається в сезонних накопичувачах до зими, а містам, які ще не мають централізованого опалення, слід це врахувати. Також багато систем є в Швеції, Німеччині та Австрії. За даними, наведеними в [2], проаналізовано впровадження сонячних систем у ЦТ в Європі.

Приклади впровадження. У м. Сількеборг (Данія) в системі ЦТ з 2016 р. працює найбільша у світі сонячна теплова станція з 436 великих колекторів, встановлених на сільськогосподарських угіддях. Сонячне тепло покриває повне теплове навантаження влітку, а взимку 20 % потреби, інші 80 % забезпечують газові когенераційні установки, сезонний накопичувач відсутній.

У м. Гронінген (Нідерланди) у 2024 р. до мережі ЦТ були підключені 48 тис. м^2 сонячних колекторів. Сонячне тепло покриває 25 % загальної річної потреби в теплі.

У 2020 р. у Швеції почалось будівництво пілотного проєкту Solar Thermal Park. Це найбільше сонячне поле концентруючих сонячних колекторів, яке сполучене з ЦТ у м. Гернесанд.

Мережа ЦТ м. Нарбонна (Франція) включає сонячну теплоцентраль. У 2022 р. вона виробила 1000 МВт·год тепла для тепломережі, що відповідає питомому виробництву 555 кВт·год/м^2 на рік і оптимізує роботу котла на біомасі взимку.

У м. Женева (Швейцарія) сонячна система ЦТ працює з 2021 р. і виробляє 558 МВт·год тепла на рік, відповідно 712 кВт·год/м^2 на рік.

У 2024 р. запрацювала сонячна теплоцентраль у м. Бад-Раппенау (Німеччина). Вона повністю задовольняє попит на гарячу воду влітку, а також полегшує функціонування фабрики із сушіння кормів для тварин.

Сонячна теплоцентраль у м. Грац (Австрія) є найбільшою у світі для випробування сонячних колекторів. Вона частково забезпечує потреби в ЦТ з піковим навантаженням 550 МВт і потребою 1200 ГВт·год на рік.

Поблизу м. Саласпілс (Латвія) у 2019 р. введені в експлуатацію сонячне поле площею 21672 м² і котел (3 МВт) на деревній тріщі. Вони задовольняють 90 % попиту місцевої тепломережі.

Сонячна опалювальна установка для мережі ЦТ в м. Панчево (Сербія) потужністю 700 кВт була побудована у 2017 р. і розширена у 2020 р. до 1 МВт. Вона задовольняє 15 % потреби міста в гарячій воді. Планується її розширення до 35000 м² та побудова накопичувача тепла об'ємом 150000 м³.

За даними компанії Solar Heat Worldwide у розробці є системи сонячного теплопостачання потужністю від 40 МВт до 50 МВт, які заплановані в м. Лейпциг (45,5 МВт) та м. Косово (40,6 МВт) [2].

Сезонні системи зберігання тепла перевірені для невеликих теплових мереж. Однак для великих теплових мереж потрібні сховища об'ємом не менше 1 млн м^3, для яких необхідні додаткові науково-дослідні роботи.

Установка на даху Британської бібліотеки складається з 950 сонячних колекторів площею 712,5 м^2. Очікується, що це дозволить скоротити викиди CO_2 від будівлі на 55 т/рік і виробляти 216 МВт·год енергії за рік [3]. Компанія Naked Energy, колектори якої використані в даному проєкті, стверджує, що її продукти Virtu – це сонячна технологія з найвищою у світі щільністю енергії. Сонячні колектори також будуть використовуватися для підтримки точної температури та умов вологості, необхідних для збереження національної колекції бібліотеки.

Системи сонячного ЦТ зменшують споживання викопного палива та викиди в навколишнє середовище. Влітку вони можуть повністю замінити викопне паливо, а сезонні накопичувачі дозволяють зберігати тепло для використання взимку.

Перспективним є використання гібридних систем теплопостачання – сонячні колектори разом з іншими джерелами тепла.

2. Теплові насоси для централізованого теплопостачання

Великі теплові насоси (ТН) потужністю кілька мегават все частіше використовують в мережах ЦТ. Великі ТН станом на 2024 р. вже інтегровані в 14 % теплових мереж у Швейцарії. Найважливішими джерелами тепла є підземні води (58 систем), стічні води (46 систем), геотермальна енергія (39

систем), озерна та річкова вода (38 систем), повітря (12 систем). У 2023 р. в німецькому м. Бундорф було введено в експлуатацію наземну фотоелектричну станцію потужністю 125 МВт. 1,5 МВт установки підключено до сусідньої тепломережі. Електричний котел потужністю 400 кВт і повітряний тепловий насос потужністю 200 кВт перетворюють сонячну енергію в тепло. Сонячна енергія генерує приблизно 54 % потреби в теплі для підключених будівель протягом року [2].

Експерти з централізованого теплопостачання з програми IEA SHC обговорили вплив інтеграції ТН у сонячні системи ЦТ з сезонним зберіганням і без нього. Проаналізовано дані теплоцентралі Ørum у Данії. Тепловий насос повітря-вода потужністю 2,5 МВт почав працювати в 2021 р. в системі ЦТ, яка вже включала 6355 м^2 сонячних колекторів та 1000 м^3 накопичувального бака. Тепловий насос збільшив гнучкість системи та зменшив залежність від газового котла. Сонячні колектори та тепловий насос покрили понад 70 % річної потреби в теплі у 2021-2022 рр. Річне тепло, вироблене газовим котлом, зменшилося з 9936 МВт·год (2020 р.) до 2432 МВт·год (2022 р.) [4].

Ці проєкти можуть бути прикладом для інших приєднатися до енергетичного переходу та відмовитися від викопного палива.

Успішні приклади впровадження енергоефективних технологій у централізованому теплопостачанні також демонструють міста України.

Для підвищення стійкості та екологічності ЦТ в м. Полтава планується проєкт з впровадження сонячної енергії та геотермального опалення. Цей проєкт підвищить резильєнтність критичної інфраструктури міста [5].

Проєкт у м. Полтава є частиною загальної тенденції до інтеграції відновлювальних джерел енергії в системи ЦТ України. Подібні ініціативи вже реалізуються в інших містах країни.

У м. Славутич, де в 2020 р. впровадили геотермальні теплові насоси потужністю 1,5 МВт, значно зменшилися витрати на газ для опалення. Це дозволило на 30% знизити залежність від викопних ресурсів, а також підвищити енергоефективність тепломережі міста.

У м. Вінниця в 2021 р. реалізували проєкт із встановлення сонячних колекторів для гарячого водопостачання, потужність яких складає 500 кВт. Це дозволило знизити споживання енергоресурсів на 25% і зменшити витрати на опалення бюджетних установ.

У м. Одеса, в 2022 р., було встановлено сонячні колектори потужністю 300 кВт, які забезпечують гаряче водопостачання для кількох житлових кварталів. В результаті цієї ініціативи вдалося зменшити використання газу для опалення на 15 %.

У м. Жовква в 2021 р. було встановлено теплові насоси потужністю 1,2 МВт для обігріву шкіл та лікарень. Це дозволило значно знизити витрати на енергію та зменшити викиди CO_2, зробивши місто більш екологічно чистим.

А в м. Миргород, завдяки впровадженню сонячних колекторів на 200 кВт у 2022 р., вдалося значно знизити витрати на опалення і зробити систему ЦТ більш стійкою та незалежною від зовнішніх джерел енергії.

Комплексний підхід до застосування передових технологій в централізованому теплопостачанні здатен суттєво вплинути на резильєнтність забезпечення тепловою енергією і гарячим водопостачанням громад в Україні та на тарифи на теплову енергію.

Ключовим фактором для успішної реалізації цих проєктів є тісна співпраця між комунальними підприємствами, місцевою владою та інвесторами, що забезпечить необхідне фінансування та ефективну організацію процесів. Спільна робота над модернізацією інфраструктури допоможе не лише підвищити енергоефективність, а й забезпечити довгострокову стійкість енергетичних систем.

Для досягнення стійкого розвитку централізованого теплопостачання та гарячого водопостачання в Україні варто орієнтуватися на досвід європейських країн, де вже успішно застосовуються сучасні системи з відновлювальними джерелами енергії. Це дозволить не лише зменшити витрати на енергію, але й значно поліпшити екологічну ситуацію, підвищити енергетичну безпеку та знизити викиди парникових газів.

1. Коберник, В. С. (2023). Сонячне теплопостачання об’єктів критичної інфраструктури. У Резильєнтність критичної інфраструктури – 2023: Збірник матеріалів науково-практичної конференції (с. 86–89). Київ: Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України.
2. Solarthermalworld. (н.д.). News. Retrieved from https://solarthermalworld.org/news.
3. Renewable Energy Magazine. (2024). British Library commissions Naked Energy to install the UK's largest solar heat project. Retrieved from https://www.renewableenergymagazine.com/thermal/british-library-commissions-naked-energy-to-install-20241014.
4. Solarthermalworld. (2024). Investigation of the boost effect of heat pumps in solar district heating. Retrieved from https://solarthermalworld.org/news/investigation-of-the-boost-effect-of-heat-pumps-in-solar-district-heating.
5. NEFCO. (2024, November 19). Швеція фінансує проєкт у сфері централізованого теплопостачання з відновлюваних джерел енергії в Полтаві для посилення енергетичної стійкості.

М.С. Дунаєвський

СУЧАСНА ПРОМИСЛОВА АНАЛІТИКА ЯК ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ РЕЗИЛЬЄНТНОСТІ ЕКОНОМІКО-ВИРОБНИЧОЇ СИСТЕМИ ПІДПРИЄМСТВА

Вступ. Промислові підприємства на сьогодні працюють в складних умовах глобальної конкуренції, стрімкого технологічного прогресу та зростаючих викликів ринку, який динамічно змінюється. Сучасна промислова аналітика, на основі великих за обсягом даних (Big Data) та штучного інтелекту (AI), відкриває нові можливості для підтримки стійкості виробничих процесів та економічного розвитку.

Мета та завдання. Метою цієї роботи є дослідити кращі практики використання промислової аналітики задля підвищення ефективності та адаптивності економіко-виробничих систем. Здійснити огляд ключових компонентів сучасних платформ промислової аналітики.

Виклад основного матеріалу. Визначимо резильєнтність економіко-виробничої системи як здатність підтримувати стабільну продуктивну роботу підприємства, реагувати на аномальні внутрішні зміни (події) у виробничих процесах та зміни зовнішнього середовища, відновлювати стабільну роботу після криз [1]. Промислова аналітика допомагає системно відстежувати та вчасно реагувати на такі зміни, сприяє гнучкому управлінню ресурсами та ризиками, підвищує стійкість ланцюгів постачання [2].

Сучасні платформи промислової аналітики охоплюють комплекс технологій та методів збору, обробки, аналізу та інтерпретації даних, що генеруються на підприємстві в процесі його діяльності. Ключовими технологіями є Big Data, глибинний аналіз даних (Data Mining (DM)), інтернет речей (internet of things (IoT)), машинне навчання (Machine Learning (ML)) та хмарні обчислення. Зазначені технології допомагають знаходити приховані закономірності в даних, виявляти та усувати вузькі місця виробничих процесів та відповідно знижувати операційні витрати. Активне впровадження та використання цього аналітичного інструментарію є фундаментом для переходу до «Промисловості 4.0» – еволюційного етапу розвитку виробничих технологій на якому інформаційні технології, та AI технології зокрема, повсюдно інтегруються у промислові процеси, активно впроваджуються кіберфізичні системи, що об’єднують в собі фізичну та інформаційно-комунікаційну інфраструктуру, забезпечуючи автоматизацію практичного повного циклу виробництва з мінімальним втручанням людини, або взагалі без такого [3]. Значною мірою, саме завдяки широкому використанню кіберфізичних систем та IoT сенсорів виконання виробничих процесів стає автоматичним, гнучким та децентралізованим. Промислова аналітика, будучи ядром «Промисловості 4.0», є міждисциплінарною та об’єднує в собі науку про дані (Data Science) та виробничу інженерію (Industrial engineering).

Модернізація підприємств (та інтенсивне впровадження процесів цифровізації зокрема) сприяють генерації та накопиченню великого обсягу різноманітних даних на кожній ланці промислового ланцюга створення доданої вартості [4]. Збираються та зберігаються експериментальні дані згенеровані під час проведення пошукових інженерних досліджень; IoT дані від сенсорів, встановлених на виробничих лініях підприємства; та, що важливо, дані щодо використання продукту кінцевим споживачем. Таким чином накопичені дані відображають замкнену систему «виробництво – споживач», та дозволяють ефективно супроводжувати процеси ітеративного покращення продукції та сервісу. Зазвичай використовують підхід орієнтований саме на процеси (основні виробничі та допоміжні: логістичні, маркетингові та сервісні), або підхід орієнтований на продукт, – точніше на різні фази життєвого циклу продукту, – від розробки до продажу, а також фазу утилізації та переробки чи перевикористання.

Розрізняють наступні 4 типи аналітики даних: описову, діагностичну, прогнозну та рекомендаційну [4]. Описова аналітика забезпечує прозорість виробничих процесів, є основою моніторингового функціоналу, відстежує рівень ключових показників системи (KPI). Діагностична аналітика сприяє виявленню першопричин відхилень від стандартів та неефективної роботи загалом. Прогнозна аналітика оцінює майбутній стан системи та, відповідно, забезпечує функціонал превентивного реагування (наприклад, прогнозуючи необхідність заміни ключових агрегатів найближчим часом). Алгоритми та методи рекомендаційної аналітики допомагають з такими задачами як, пошук оптимальних плану виробництва, позмінного розкладу роботи працівників, маршрутів постачання сировини та готової продукції з врахуванням відповідних обмежень [5].

Відомим та широко застосовуваним прикладом промислової аналітики є прогресивні підходи прогнозного обслуговування устаткування (Predictive Maintenance), які використовують, як історичні дані щодо роботи самого обладнання, так і дані щодо його налаштування та ремонту. Оптимізують виробничі процеси не тільки з метою уникнення незапланованого простою цього обладнання, а й з метою запобігання розбалансування налаштувань устаткування, що може призводити до випуску бракованої продукції (особливо якщо йдеться про формувальне обладнання). Методи глибинного аналізу даних та машинного навчання застосовуються для побудови прогнозної моделі, яка б передбачала залишок часу стабільного операційного функціонування, або ж ймовірність виникнення несправностей впродовж певного визначеного періоду часу, зважаючи на дані щодо проведеного технічного обслуговування та стану обладнання. Для побудови надійної прогнозної моделі потрібні дані щодо несправностей обладнання в минулому. Такі випадки досить поодинокі (зазвичай більшу частину часу обладнання успішно працює), – відповідно дані є незбалансованими щодо прогнозного класу, а побудова високоточних моделей стає досить складним завданням для дослідників даних [6].

Іншим напрямом промислової аналітики є методи прогнозування якості процесу що мають за мету зниження рівня браку та, відповідно, підвищення вихідного рівня придатної продукції з першого підходу (first-pass-yield). Ці методи повинні враховувати складні взаємозв'язки між параметрами обладнання, параметрами процесів, характеристиками інструментів та матеріалів. Згадані методи прогнозують кінцеву якість продукції та визначають першопричину зниження якості на всіх етапах процесу. Робота таких методів в режимі реального часу дозволяє відсіяти браковані компоненти безпосередньо в процесі виробництва, – задовго до того як вони спричинять зниження якості кінцевого продукту та витрати.

Вартий уваги і підхід «Інженерія в циклі» (Engineering in the loop), який має за мету покращення продуктів на основі даних (data-driven) щодо використання готового продукту кінцевими споживачами. Дані від споживачів доповнюються інженерними даними щодо виробництва продукту та утворюють комплексну систему «виробництво – споживач», яка на основі зворотного зв'язку від споживачів дозволяє ітеративно покращувати продукт. Традиційно «Інженерія в циклі» передбачає використання описової аналітики, OLAP (online analytical processing) та попередній дослідницький аналіз даних EDA (Exploratory Data Analysis). Більш прогресивні методи передбачають застосування алгоритмів та методів DM та ML, які, наприклад, дозволяють досить точно віднайти та встановити (часто не очевидні) детальні шаблони використання продукту споживачами та отримати розуміння можливих перспективних напрямів покращення дизайну продукту. Складність застосування цих методологій зазвичай пов'язана з наявністю, збором та якістю отримуваних даних від користувачів.

Багато архітектур, концепцій та технологій промислової аналітики запозичено з вебаналітики. Наприклад, масштабовані послідовності обробки даних (Data Pipelines) з використанням технологій Apache Hadoop та Apache Spark з подальшим збереженням результату в озерах даних (Data Lake). Звичайно ж, запозичення відбувається з відповідною адаптацією під вимоги промислового виробництва. Такі компанії як Amazon, Meta та Google є основними гравцями сфери вебаналітики, – ключовими гравцями в сфері промислової аналітики є такі компанії як Bosch, Airbus та Siemens [4].

Вартою уваги є концепція платформи промислової аналітики запропонована Крістофом Грогером [4]. Вона поєднує в собі переваги широко використовуваних на практиці референтної архітектури Model Industrie 4.0 (RAMI 4.0) та архітектури IIoT. Перша є концептуальною та включає компоненту абстракції даних, рівні ієрархії виробництва та життєвий цикл об'єктів. Зокрема, фокусується на цифрових двійниках (Digital Twins), моделях даних та інтеграції ланцюга вартості, – без деталізації аспектів імплементації. Друга фокусується на інтеграції контролю на виробничих лініях з бізнес процесами та корпоративними IT системами. Визначає ключовими хмарні та крайові обчислення, методи обробки складних подій. Платформа запропонована

в [4] є орієнтованою на дані, оскільки саме наявність якісних даних є необхідною передумовою отримання переваг від застосування методів промислової аналітики. Ключовим компонентом є озеро даних (Data Lake), – технологія, яка з'являється як доповнення до сховищ даних (Data Warehouse), підтримує зберігання та обробку всіх видів даних (структурованих, напівструктурованих та неструктурованих), забезпечує гнучкий аналіз, особливо прогресивними методами ML та аналітики потокових даних. Процеси побудови та розгортання ML моделей автоматизуються та операціоналізуються інструментарієм MLOps. [7]

Висновки. Сучасна промислова аналітика є ключовим елементом забезпечення резильєнтності економіко-виробничої системи підприємства. Зокрема, такі аналітичні технології як прогнозне обслуговування устаткування, методи прогнозування якості процесу, підхід «Інженерія в циклі» дозволяють підвищити ефективність виробничих процесів, мінімізувати ризики та забезпечити стійкий розвиток. Сприяє цій меті й побудова сучасних платформ промислової аналітики, ключовими компонентами якої є такі технології зберігання даних як Data Warehouse та Data Lake, технології обробки великих за обсягом даних (Big Data), прогресивні технології побудови прогнозних моделей та рішень з використанням алгоритмів машинного навчання та технологій штучного інтелекту. Подальша еволюція аналітичних інструментів та платформ відкриває нові можливості для зміцнення стійкості та ефективності сучасного підприємства.

1. Горбачук В.М., Лупей М.І., Дунаєвський М.С. (2022) Підходи до резильєнтності критичних інфраструктур. Science and education for sustainable development. A.Ostenda, V.Smachylo (eds.). Poland: University of Technology, Katowice. 87−95. DOI:10.54264/M005.
2. Горбачук В.М. (2010) Методи індустріальної організації. Кейси та вправи. Економіка та організація виробництва. Економічна кібернетика. Економіка підприємства. К.: АСК.
3. Горбачук В.М. (2016) На порозі четвертої промислової революції. Причорноморські економічні студії. вип. 8. сс. 216–220.
4. Gröger C. (2022) Industrial analytics – An overview. it – Information Technology, 64(1-2), pp. 55–65. DOI: https://doi.org/10.1515/itit-2021-0066
5. Kart L., Linden A., Schutle W. (2013) Extend your portfolio of analytics capabilities. Gartner research note G00254653.
6. Dogan A., Birant D. (2021) Machine learning and data mining in manufacturing. Expert systems with Applications. v. 166. pp. 1–22.
7. Дунаєвський М.С. (2024) MLOps архітектура сучасних інтелектуальних систем, що самонавчаються. Збірник тез XIII Міжнародної науково-практичної конференції «Глушковські читання. Сучасна кібернетика 2024». Київ: Інститут кібернетики імені В.М. Глушкова НАН України.

С.Є. Саух, Т.В. Пучко

ПАРАЛЕЛЬНІ АЛГОРИТМИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ МОДЕЛЮВАННЯ РЕЗИЛЬЄНТНИХ ЕЛЕКТРОЕНЕРГЕТИЧНИХ СИСТЕМ

У сучасних умовах терористичних і воєнних загроз особливо важливим стає пошук ефективних підходів до оптимізації структури генеруючих потужностей енергетичних систем. Атаки на енергетичну інфраструктуру призводять до перебоїв в електропостачанні, що негативно позначається на національній безпеці, економічній стабільності та добробуті суспільства. Одним із можливих рішень є використання розподілених відновлюваних джерел енергії (ВДЕ) та систем накопичення енергії, що здатне підвищити резильєнтність енергосистем.

Задачі оптимізації, пов'язані з плануванням генеруючих потужностей, зазвичай формулюються як задачі змішаного цілочисельного лінійного програмування (MILP). Вони характеризуються великою розмірністю і потребують значних обчислювальних ресурсів, оскільки врахування непередбачуваності та некерованості ВДЕ суттєво ускладнює моделювання енергосистем [1]. Для ефективного розв'язання таких задач необхідно розробляти та впроваджувати паралельні алгоритми, що робить вкрай актуальними дослідження у сфері паралельної оптимізації.

Одним із підходів до розв’язання задач MILP великої розмірності є метод декомпозиції [2]. Завдяки особливостям задачі оптимізації структури генеруючих потужностей, її можливо розділити на підзадачу першого рівня, яка визначає кількість генеруючих блоків і враховує вартість їх встановлення, та множину підзадач другого рівня, які моделюють технологічні умови навантаження блоків і операційні витрати. При цьому:

- кількість генеруючих блоків задається змінними в підзадачі першого рівня та параметрами в підзадачах другого рівня;
- значення цільової функції підзадачі першого рівня для певної кількості генеруючих блоків залежить від значень цільових функцій підзадач другого рівня і є оптимальним значенням усієї задачі оптимізації для цієї кількості блоків;
- підзадача першого рівня має опуклу область допустимих значень змінних, та її цільова функція є опуклою;
- підзадачі другого рівня є задачами MILP.

Виходячи з вищенаведеного, ми пропонуємо розв’язувати підзадачу першого рівня за допомогою алгоритмів, що не потребують обчислення похідної від цільової функції [3]. Їх ще називають алгоритмами «чорної скриньки», бо вони вимагають не математичного формулювання цільової функції, а лише можливості обчислити її значення у будь-якій точці. До них належать метаевристичні алгоритми, що використовують випадковість для пошуку

рішення [4]. Багато з таких алгоритмів, зокрема ті, що засновані на популяції, можуть обчислювати значення цільової функції одночасно у багатьох точках, що сприяє паралелізації обчислень. Таким є, наприклад, алгоритм еволюційних центрів [5].

Під час обчислення значення цільової функції у певній точці необхідно обчислити значення цільової функції кожної з підзадач другого рівня. Оскільки ці підзадачі не залежать одна від одної, їх можливо розв'язувати одночасно за допомогою будь-яких доступних солверів MILP, наприклад, солвера SCIP [6].

Запропонований нами паралельний алгоритм показано на рисунку 1. Він поєднує алгоритм «чорної скриньки» та солвер MILP. Цей гібридний алгоритм здатен досягати високого рівня паралелізації обчислень завдяки як одночасному розв'язуванню підзадач другого рівня, так і здатності багатьох алгоритмів «чорної скриньки» одночасно виконувати кілька обчислень значень цільової функції.

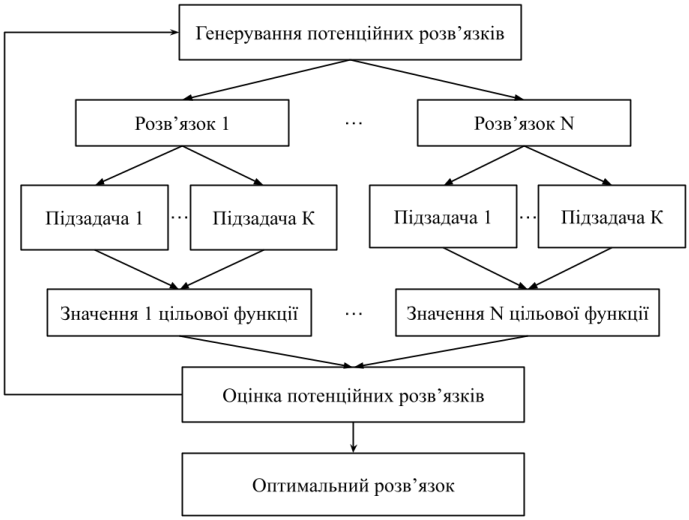


Рисунок 1 – Гібридний паралельний алгоритм

Таким чином, на сьогодні є надзвичайно актуальним підвищення резильєнтності енергетичних систем, яке можливо досягти завдяки розподіленому розміщенню ВДЕ. Щоб моделювати енергосистему зі значною часткою ВДЕ, необхідно ефективно використовувати паралельні обчислювальні ресурси. Ми запропонували узагальнений алгоритм оптимізації структури генеруючих потужностей, що має високий рівень паралелізації обчислень. Метою подальших досліджень буде оцінювання ефективності цього алгоритму в середовищах із розподіленою оперативною пам'яттю, таких, як комп'ютерні кластери.

Наукові дослідження виконані за проєктом, який фінансується МОН в рамках міжнародного наукового білатерального співробітництва відповідно до програми спільних українсько-німецьких науково-дослідних проєктів для реалізації у 2024-2025 рр. Державний реєстраційний номер: 0124U002691.

1. Hong, Y. -Y., & Apolinario, G. F. D. (2021). Uncertainty in unit commitment in power systems: A review of models, methods, and applications. *Energies*, *14*(20), 6658. https://doi.org/10.3390/en14206658.
2. Rahmaniani, R., Crainic, T. G., Gendreau, M., & Rei, W. (2017). The Benders decomposition algorithm: A literature review. *European Journal of Operational Research*, *259*(3), 801-817. https://doi.org/10.1016/j.ejor.2016.12.005.
3. Метод прямого пошуку. (2023, 16 травня). *Вікіпедія.* https://uk.wikipedia.org/wiki/Метод_прямого_пошуку.
4. Метаевристика. (2023, 3 вересня). *Вікіпедія.* https://uk.wikipedia.org/wiki/Метаевристика
5. Mejía-de-Dios, J.-A., & Mezura-Montes, E. (2019). A new evolutionary optimization method based on center of mass. In K. Deep, M. Jain, & S. Salhi (Eds.), *Decision Science in Action* (pp. 65–74). Springer Singapore. https://doi.org/10.1007/978-981-13-0860-4_6.
6. Bolusani, S., Besançon, M., Bestuzheva, K., Chmiela, A., Dionísio, J., Donkiewicz, T., van Doornmalen, J., Eifler, L., Ghannam, M., Gleixner, A., Graczyk, C., Halbig, K., Hedtke, I., Hoen, A., Hojny, C., van der Hulst, R., Kamp, D., Koch, T., Kofler, K., … Xu, L. (2024). *The SCIP optimization suite 9.0*. arXiv. https://doi.org/10.48550/ARXIV.2402.17702.

І.В. Пучко, А.М. Примушко, М.С. Ярошинський, Г.О. Кравцов

ПІДВИЩЕННЯ РЕЗИЛІЄНТНОСТІ ДИНАМІЧНИХ СИСТЕМ ПРИ СИНХРОНІЗАЦІЇ СТАНІВ ЗА ДОПОМОГОЮ CRDT

Резильєнтність (resilience) динамічних програмних систем визначається як їх здатність адаптуватися до змін і протистояти зовнішнім впливам без втрати основної функціональності [1]. На відміну від традиційних підходів до забезпечення стійкості, які акцентуються на попередженні збоїв, резильєнтність спрямована на мінімізацію наслідків таких подій та забезпечення безперервності роботи системи навіть у несприятливих умовах. Тобто системи мають продовжувати функціонувати, відновлюватися після збоїв адаптуючись до нових умов [2].

Особливої актуальності концепція резильєнтності набуває у розподілених системах, які характеризуються високою динамікою, масштабністю та великою кількістю взаємозалежних компонентів. У таких умовах критично важливо забезпечити стабільність і узгодженість роботи навіть за наявності часткових збоїв або втрати зв'язку між вузлами.

Ключові характеристики резільєнтних систем [1]:

- Гнучкість (Flexibility): Здатність системи адаптуватися до змін та непередбачених ситуацій, забезпечуючи ефективне реагування на нові виклики.
- Адаптивність (Adaptability): Можливість системи змінювати свої стратегії та структури у відповідь на зміни в навколишньому середовищі або внутрішні збої.
- Інтеграція (Integration): Співпраця та взаємодія між різними компонентами та підсистемами для досягнення загальної стійкості.
- Навчання (Learning): Здатність системи вчитися на попередніх помилках та успіхах, постійно вдосконалюючи свої процеси та процедури.
- Антиципація (Anticipation): Можливість передбачати потенційні ризики та проблеми, що дозволяє вживати превентивні заходи для їх уникнення.

Приклади резильєнтних динамічних систем:

- Енергетичні мережі, здатні до швидкого перерозподілу навантаження.
- Хмарні обчислення з підтримкою автоматичного відновлення вузлів.
- Транспортні системи, що адаптуються до змін у реальному часі.

CRDT (Conflict-Free Replicated Data Types) [3] забезпечує ефективну синхронізацію станів у розподілених системах, що дозволяє уникати конфліктів і підтримувати стабільність навіть за високої динаміки змін. CRDT — це

абстрактний тип даних з визначеним інтерфейсом, який дозволяє розподілену реплікацію (оптимістична реплікація [4]) через кілька вузлів. Кожну репліку можна змінювати на вимогу та незалежно від інших, без необхідності координувати ці зміни між ними. Коли дві репліки отримують однаковий набір оновлень, навіть якщо вони отримані в різному порядку, вони досягають одного й того самого стану детерміністично, застосовуючи математично обґрунтовані правила для забезпечення збіжності станів [5]. Більше того, якщо одночасні оновлення певних даних є комутативними, і всі їхні репліки виконують усі оновлення в причинно-зв'язному порядку, то значення реплік збігаються. Це називається комутативним реплікованим типом даних [5]. Така система спроектована для комутування одночасних операцій. Це усуває потребу в складному контролі за паралельністю, дозволяючи операціям виконуватись у різному порядку при цьому забезпечуючи збіжність реплік до одного й того ж результату. Такий підхід гарантує відсутність конфліктів, тим самим усуваючи потребу в консенсусному контролі паралельних операцій [6,7].

Серед переваг використання CRDT для підвищення резільєнтності динамічних систем можна віднести:

- Структури даних спроектовані таким чином, щоб бути комутативними та збіжними [8]. Це означає, що кілька копій одних і тих самих даних можуть оновлюватися незалежно одна від одної, а потім об'єднуватися без конфліктів [9]. Це дозволяє ефективно і точно аналізувати дані навіть у випадках, коли мережа відключена або має високе навантаження [10, 11].
- Підхід CRDT ґрунтується на заздалегідь визначених правилах вирішення конфліктів, які визначають їхню семантику. Ці правила, як правило, є специфічними для певних структур даних [9]. CRDT забезпечують механізм для виявлення та вирішення конфліктів, що гарантує консистентність усіх копій даних. Це особливо корисно в електричній мережі, де кілька копій інформації про стан можуть зберігатися в різних місцях;
- Вибір структури CRDT, заснованої на стані [8], яка зберігає поточний стан даних замість історії змін, робить їх придатними для моніторингу та аналізу даних в реальному часі в електричній мережі;
- Масштабованість: CRDT дозволяють створювати розподілені системи, які можуть масштабуватися горизонтально [12] без потреби в складних механізмах координації [10];
- Відмовостійкість: CRDT стійкі до відмов, оскільки дозволяють реплікувати дані між вузлами і відновлювати їх у разі відмови одного або кількох вузлів [13].

Синхронізація станів як основа резильєнтності - стан-орієнтовані структури CRDT дозволяють ефективно вирішувати конфлікти при одночасному оновленні вузлів, забезпечуючи детерміновану узгодженість і підтримку загального стану системи.

Внесок у підвищення резильєнтності - використання CRDT дозволяє будувати системи, стійкі до часткових збоїв вузлів і затримок у передачі даних, забезпечуючи ефективне відновлення і адаптацію до змін.

Зважаючи на викладене вище вважаємо, що проблема підвищення резилієнтності динамічних систем при синхронізації станів за допомогою CRDT є актуальною та заслуговує на подальше дослідження.

1. Hollnagel E., Woods D. D. & Leveson N. C. (2006). Resilience Engineering: Concepts and Precepts, Ashgate, Aldershot, UK, 29738211.
2. M. Ouyang (2014). Review on modeling and simulation of interdependent critical infrastructure systems, *Reliability Engineering and System Safety*. 121, 43–60, https://doi.org/10.1016/j.ress.2013.06.040.
3. Nuno Preguiça (2024, 23 грудня). Conflict-free Replicated Data Types: An Overview, *arXiv* https://arxiv.org/abs/1806.10254.
4. Saito, Y. & Shapiro, M. (2005). Optimistic replication. *ACM Computing Surveys*, vol. 37, no. 1, 42-–81, Mar. https://doi.org/10.1145/1057977.1057980.
5. Almeida, P.S (2024, 23 грудня). Approaches to Conflict-free Replicated Data Types. *arXiv* https://arxiv.org/abs/2310.18220.
6. Shapiro, M.(2011). Conflict-Free Replicated Data Types. У Preguiça, N.; Baquero & C.; Zawirski, M. (Ред.) *Lecture Notes in Computer Science*, с 386—400. Grenoble, France: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-24550-3_29.
7. Letia, M.; Preguiça, N.; Shapiro, M. (2024, 23 грудня). CRDTs: Consistency without Concurrency Control. *arXiv* https://doi.org/10.48550/arXiv.0907.0929.
8. Shapiro M., Preguiça N., Baquero C. & Zawirski M. (2011). A comprehensive study of Convergent and Commutative Replicated Data Types, Inria – Centre Paris-Rocquencourt; INRIA. https://hal.inria.fr/file/index/docid/555588/filename/techreport.pdf.
9. Saquib N. (2022). Log-Based CRDT for Edge Applications. У Krintz C. & Wolski R. (ред.) *IEEE International Conference on Cloud Engineering (IC2E)*, с. 126-137, doi.org/10.1109/IC2E55432.2022.00021.
10. Qayyum, O. (2024). Coordination-Free Replicated Datalog Streams with Application-Specific Availability. У Yu, W. *Advances in Databases and Information Systems. Lecture Notes in Computer Science*. с 155–169 Springer, Cham. https://doi.org/10.1007/978-3-031-70626-4_11.
11. Kleppmann M., Mulligan D. P., Gomes V. B. & Beresford A. R. (2022), A Highly-Available Move Operation for Replicated Trees, *IEEE Transactions on Parallel and Distributed Systems*. 33(7), 1711 - 1724, https://doi.org/10.1109/TPDS.2021.3118603.
12. Biletskyy, B.O. (2019). Horizontal and vertical scalability of machine learning methods. Problems in Programming, 2, 69-80. doi: https://doi.org/10.15407/pp2019.02.069.
13. Balazinska, M., Balakrishnan, H., Madden, S.R., Stonebraker, M. (2008) Fault tolerance in the borealis distributed stream processing system. *ACM Trans. Database Syst.* 33(1), 1–44 https://doi.org/10.1145/1331904.1331907.

А.В. Ковилін

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СТВОРЕННІ РЕЗИЛЬЄНТНИХ СИСТЕМ КІБЕРБЕЗПЕКИ: МЕТОДИ ТА ТЕХНОЛОГІЇ

Штучний інтелект (ШІ) стає важливим фактором у створенні резильєнтних систем кібербезпеки, особливо для динамічних систем, таких як критичні інфраструктури. Використання ШІ забезпечує автоматизацію виявлення загроз, прогнозування атак та реагування, що дозволяє мінімізувати ризики та наслідки реалізації кіберзагроз.

З поширенням цифрових технологій кіберзагрози стають дедалі складнішими, а їх вплив може бути руйнівним для критичних інфраструктур, таких як транспорт, зв'язок, а особливо енергетика. Резильєнтність даних систем базується на здатності протистояти атакам, швидко відновлюватись і адаптуватись до нових викликів. ШІ відіграє важливу роль у цьому процесі, пропонуючи передові методи аналізу, моделювання та автоматизації. Резильєнтні системи кібербезпеки орієнтовані на забезпечення стійкості до атак, швидке виявлення загроз і ефективне реагування. Вони використовують штучний інтелект для аналізу аномалій, прогнозування можливих атак і автоматизації процесів відновлення після інцидентів (табл. 1). Інтеграція таких систем сприяє підвищенню захисту критичних інфраструктур та адаптації до нових викликів у сфері кіберзагроз.

Таблиця 1 – Таблиця прикладів резильєнтних систем кібербезпеки

Тип системи	Приклад
Системи аналізу аномалій	Cisco Secure Network Analytics, яка використовує ШІ для моніторингу аномалій у реальному часі
Платформи автоматизації реагування	Splunk Phantom, IBM Resilient, що автоматизують процеси реагування на інциденти безпеки
Системи прогнозування атак	FireEye Helix, що аналізує історичні дані для визначення можливих векторів атак
Цифрові двійники	Моделі для тестування сценаріїв атак, наприклад, у SCADA-системах енергетики
Моделі самовідновлення	Microsoft Azure Sentinel, що інтегрує ШІ для виявлення загроз і ініціації заходів нейтралізації

ШІ дозволяє аналізувати великі обсяги даних для виявлення аномалій у функціонуванні систем. Методи кластеризації, такі як DBSCAN та K-Means,

ефективно групують дані, допомагаючи визначити відхилення [1]. Глибокі нейронні мережі [2] здатні ідентифікувати нормальну поведінку систем і виділяти аномалії, які можуть вказувати на потенційні загрози.

Прогнозування загроз є ще однією важливою складовою резильєнтності. Використання алгоритмів, таких як Random Forest [3] або XGBoost, дозволяє системам передбачати ймовірність атак на основі історичних даних. Це дає змогу спеціалістам з кібербезпеки чи аналітикам даних завчасно повідомляти про потенційні атаки або приймати превентивні заходи.

Автоматизація реагування на інциденти завдяки ШІ значно зменшує час відгуку. Системи на основі reinforcement learning оптимізують дії в реальному часі, дозволяючи мінімізувати вплив атак на критичну інфраструктуру. Такі підходи знижують залежність від людського фактора та підвищують ефективність захисту.

Перспективи використання ШІ у кібербезпеці включають інтеграцію цифрових двійників для моделювання реальних систем і тестування сценаріїв атак. Поєднання традиційних методів аналізу з інструментами ШІ створює ефективні гібридні моделі. Крім того, розробка міжнародних стандартів інтеграції ШІ сприятиме уніфікації підходів і підвищенню довіри до технологій.

Штучний інтелект має величезний потенціал для створення резильєнтних систем кібербезпеки. Особливо в контексті здатності таких систем:

1. Протидіяти загрозам: Системи здатні виявляти та нейтралізувати загрози ще до того, як вони завдадуть шкоди. Це досягається завдяки аналізу аномалій, прогнозуванню атак та використанню сучасних методів безпеки, таких як Zero Trust [4] моделі.

2. Швидкому відновленню: У разі інциденту резильєнтна система має мінімізувати час простою, автоматично відновлювати пошкоджені дані чи компоненти і підтримувати критично важливі функції.

3. Адаптивності: Резильєнтні системи вчаться на минулих інцидентах, удосконалюючи алгоритми захисту і реагування, що дозволяє їм краще справлятися з новими типами атак.

Використання технологій аналізу аномалій, прогнозування загроз і автоматизації реагування дозволяє мінімізувати вплив атак і забезпечити стійкість критичних систем. Проте для досягнення максимального ефекту необхідно подолати виклики, пов’язані з якістю даних, інтерпретованістю моделей, їх інтеграцією в існуючі інфраструктури.

Попри численні переваги, впровадження ШІ у кібербезпеку стикається з викликами (табл. 2). Однією з головних проблем є висока кількість хибних спрацювань, які можуть створювати додаткове навантаження на фахівців. Крім того, обмеженість якісних і різноманітних даних для навчання моделей ШІ є ще одним бар’єром. Складність інтерпретації моделей, особливо глибоких нейронних мереж, також ускладнює їх інтеграцію у критичні системи.

Таблиця 2 – Виклики впровадження ШІ у резильєнтні системи кібербезпеки

Виклик	Опис
Якість даних	Невелика кількість якісних і різноманітних даних для навчання моделей
False positives результати	Велика кількість хибних спрацювань, що створює додаткове навантаження на фахівців
Інтерпретація моделей	Складність пояснення результатів роботи глибоких нейронних мереж
Інтеграція в існуючі системи	Труднощі адаптації до існуючої інфраструктури та сумісність з іншими системами безпеки
Конфіденційність і безпека	Ризики, пов'язані з обробкою чутливих даних у моделях
Високі витрати на впровадження	Необхідність значних ресурсів для розробки, впровадження та обслуговування ШІ-рішень

Висновок. Штучний інтелект є трансформаційною силою у сфері кібербезпеки, сприяючи розробці резильєнтних систем, здатних протистояти, реагувати та відновлюватися після дедалі складніших кіберзагроз. Інтегруючи передові технології, такі як виявлення аномалій, прогнозування загроз та автоматизація реагування, ШІ не лише зміцнює критичну інфраструктуру, але й забезпечує проактивні стратегії захисту. Успішна реалізація рішень на основі ШІ залежить від подолання викликів, пов’язаних із якістю даних, інтерпретованістю моделей та інтеграцією в існуючі інфраструктури. Завдяки постійним інноваціям та впровадженню уніфікованих стандартів, ШІ має потенціал суттєво посилити глобальну резильєнтність у сфері кібербезпеки динамічних систем.

1. Nurnadiah Zamri et al. A comparison of unsupervised and supervised machine learning algorithms to predict water pollutions. Procedia Computer Science 204 (2022) 172–179. https://doi.org/10.1016/j.procs.2022.08.021.
2. Shams Forruque Ahmed, Md. Sakib Bin Alam, Maruf Hassan, Mahtabin Rodela Rozbu, Taoseef Ishtiak, Nazifa Rafa, M. Mofijur, A. B. M. Shawkat Ali & Amir H. Gandomi. Deep learning modelling techniques: current progress, applications, advantages, and challenges. Volume 56, pages 13521–13617, (2023). https://doi.org/10.1007/s10462-023-10466-8.
3. Zhigang Sun, Guotao Wang, Pengfei Li, Hui Wang, Min Zhang, Xiaowen Liang. An improved random forest based on the classification accuracy and correlation measurement of decision trees. https://doi.org/10.1016/j.eswa.2023.121549.
4. Dr. William R. Simpson. Toward a zero trust metric. Institute for Defense Analyses, 730 East Glebe Road, Alexandria, VA 22305, USA. https://doi.org/10.1016/j.procs.2022.08.015.

В.В. Микитенко

ГІБРИДНА РЕГЕНЕРАЦІЯ ТА РЕЗИЛІЄНТНІСТЬ СОЦІО-ЕКОЛОГО-ЕКОНОМІЧНИХ СИСТЕМ МАКРОРЕГІОНІВ УКРАЇНИ: ІННОВАЦІЙНІ ТЕХНОЛОГІЇ УПРАВЛІННЯ

З огляду на нагальність обґрунтування напрямів й об'єктів локалізації зусиль у контексті вирішення проблем постконфліктного відновлення України, забезпечення сталого розвитку економіки вимагає стратегічних підходів, що здатні синхронно враховувати системну взаємодію соціальних, екологічних та економічних чинників. Гібридна регенерація та резилієнтність соціо-еколого-економічних систем за визначеними семи макрорегіональними зонами реконструктивного просторового відновлення і розвитку України [1] формулюють нові парадигми антикризового та відновлювального управління, які є невід'ємною складовою сучасної економічної науки і практики.

З цього, по-перше, маємо акцентувати увагу на необхідності формування інтегрованих підходів до управління національним господарством, де економічний розвиток гармонійно поєднується з відновленням соціальної стабільності та екологічної рівноваги. По-друге, визнати нагальним впровадження інноваційних технологій моніторингу та управління [2], що забезпечить оперативне реагування на динамічні зміни зовнішніх умов, що дозволяє виробляти стратегії макроекономічної політики з урахуванням реального стану і масштабів потенціалу кожного макрорегіону. Нарешті, розв'язання завдань дослідження х гібридної регенерації сприятиме збагаченню теоретико-методологічної бази управління національним господарством, пропонуючи гібридні рішення для підвищення стійкості систем, підсилюючи їх конкурентоспроможність та стратегічну безпеку у контексті глобальних викликів і трансформацій у повоєнному періоді.

За результатами дослідження *організації реконструктивного просторового розвитку господарської системи України* (ОРПРГСУ) визнано пріоритетність реалізації у повоєнному періоді *до 2030 року гібридного сценарію ОРПРГСУ* (ГБС-2030) [3], типовий склад якого розроблено для семи макрорегіональних зон, ідентифікованих в якості Зон повоєнного відновлення і регенерації з урахуванням усіх сценарних соціо-еколого-економічних детермінант за використання при розбудові інвестиційних, технологічних, когнітивно-інформаційних та інноваційних фільтрів [1,4]. Зазначимо, що реалізація ГБС-2030 із акцентом на *когнітивно-інформаційний сценарний драйвер* (КІСД) має складатися з восьми етапів, реалізованих у замкненому циклі виконання організаційно-економічних і економіко-статистичних завдань та процедур з оцінювання, аналізу, моніторингу і стратегування (табл. 1). За пропонованою схемою автором підкреслено унікальність інструментарію, використаного для забезпечення ефективності повоєнної регенерації, реконструкції та резилієнтності соціо-еколого-економічних систем, інкорпорованих до семи

макрорегіональних зон. Тому, відтворюючи поступовий перехід від їх аналізу та оцінки потенціалів до забезпечення *сталого розвитку і господарювання* (СРГ), маємо пояснити окремі взаємозв'язки і процедури, визначені при алгоритмізації процесів ОРПРГСУ. Так, за: а) Етапами I – IV – формується база для розробки цифрових і когнітивних рішень, забезпечуючи необхідну інфраструктурну і нормативну підтримку; б) Етапами V – VI формуються взаємозв'язки, які безпосередньо, впливають на реалізацію інноваційних підходів до управління *природно-ресурсними активами* (ПРА) і економікою макрорегіональних зон, інтегруючи міжнародний досвід і *когнітивно-інформаційні технології* (КІТ); в) за Етапами VII – VIII забезпечується моніторинг і коригування ГБС-2030 (у разі виникнення певних вимірів відхилень), генеруючи ознаки адаптивності та СРГ (а, при суттєвих відхиленнях від визначених орієнтирів, суб'єкти управління мають повернутися до виконання завдань і процедур за Етапами I – IV).

Таблиця 1 – Алгоритм реалізації ГБС-2030 ОРПРГСУ із акцентом на КІДС*

Етап	Опис етапу	Організаційно-економічні заходи	Вимоги щодо впровадження
I. Аналіз поточного стану та ідентифікація ризиків	Оцінка поточного стану економіки, *критичної інфраструктури* (КІ) та ПРА після завершення військових дій.	Проведення комплексного аудиту інфраструктури і ресурсів. Ідентифікація ризиків і загроз (економічних, екологічних, соціальних, тощо).	Залучення фахівців з економіки, екології та соціології. Використання інформаційно-аналітичних систем для збору даних.
II. Визначення пріоритетних напрямків цифрової трансформації	Окреслення ключових напрямів цифровізації та впровадження КІТ задля управління різної природи ресурсами.	Визначення: цифрових платформ та інструментів; застосування фільтрів для коригування; планування і впровадження КІТ та управлінських систем.	Співпраця з технологічними компаніями, фахівцями з ІТ-галузі, експертами, тощо. Забезпечення достатнього рівня кібербезпеки.
III. Модернізація інституційної інфраструктури	Реорганізація державних інституцій для інтеграції нових управлінських механізмів.	Вдосконалення законодавчої бази для цифрового управління. Оптимізація державних органів для підтримки цифрових рішень.	Підготовка державних органів до роботи з новими технологіями. Створення нормат-ивно-правових актів інтеграції цифрових технологій і КІТ.
IV. Розвиток комунікаційного простору взаємодії стейкхолдерів	Створення комунікаційної платформи для прозорої взаємодії між державою, громадськістю і бізнесом.	Впровадження онлайн-платформ для участі громадян у прийнятті рішень. Комунікації між органами влади і громадами.	Відкритість даних для громадськості. Підтримка механізмів електронного уряду.

Закінчення таблиці 1

V. Впровадження КІТ для управління природними ресурсами	Інтеграція інтелектуальних систем управління для ефективного використання ПРА.	Використання ГІС для контролю й управління ПРА. Впровадження інтелектуальних мереж smart grid.	Підготовка кадрів для роботи з інтелектуальними системами, фінансування технолог. Оновлення.
VI. Інтеграція міжнародних стандартів та практик	Залучення міжнародного досвіду і стандартів ефективності регенерації та реконструкції.	Співпраця з міжнародними організаціями. Впровадження кращих світових практик	Підписання угод з міжнародними партнерами. Відповідність міжнародним стандартам (ISO, ЄС).
VII. Оцінка результатів та адаптація стратегії	Моніторинг ефективності реалізації ГБС-2030 та внесення коригувань	Проведення регулярних аудит. перевірок. Оцінка впливу на економіку, екологію та суспільство	Використання показників СРГ для оцінки успіху. Адаптація стратегії на основі зібраних даних.
VIII. Забезпечення сталого розвитку та безперервності	Підтримка безперервності реалізації реконструктивного процесу у контексті забезпечення СРГ.	Розробка довгострокових планів щодо забезпечення СРГ. Залучення інвестицій для підтримки процесів трансформації	Гарантії стабільного фінансування на всіх етапах замкненого алгоритму. Гнучкість реагування на виклики і зміни.

*Джерело * Сформульовано, обґрунтовано, визначено та систематизовано автором*

Визнаємо, що у контексті гібридної регенерації та забезпечення резилієнтності соціо-еколого-економічних систем семи макрорегіональних зон інноваційні технології моніторингу та управління за пропонованим алгоритмом мають володіти достатніми характеристиками і властивостями, деталізованими у [5], що й забезпечать досягнення цілі. А, саме: 1) проактивністю та адаптивністю: технології повинні забезпечувати можливість швидкого реагування на динамічні зміни умов, адаптуватися до нових загроз і викликів, автоматично оновлювати параметри моніторингу і управління залежно від різних факторів; 2) масштабованістю та модульністю: інструментарій має бути здатний до розширення і перебудови під різні обсяги даних та масштаб проблем: від локальних питань до загальнодержавних й макрорегіональних сценаріїв розвитку; 3) інтегрованістю та системністю: технології повинні враховувати взаємозв'язки між соціо-еколого-економічними компонентами, створюючи цілісний комплекс моніторингу й управління, що спирається на міждисциплінарні дані; 4) цифровізацією і аналітикою: інформаційно-аналітичні платформи мають гарантувати оперативний збір, обробку і візуалізацію великих масивів даних, використання ШІ, машинного навчання та прогнозних моделей для формування науково обґрунтованих рекомендацій; 5) прозорістю і підзвітністю: технології повинні забезпечувати відкритий доступ до ключових

індикаторів моніторингу, зрозумілі методи оцінки ефективності прийнятих рішень, гарантувати підзвітність перед суспільством та зацікавленими сторонами; 6) інтероперабельністю та сумісністю: використовувані платформи мають легко інтегруватися з існуючими системами управління, національними і регіональними базами даних, з іншими інструментами прогнозування й прийняття рішень; 7) безпекою і стійкістю до кібератак: має бути передбачено надійний захист інформаційних систем від несанкціонованого доступу, кібератак і деструктивних впливів, що сприятиме підвищенню безпеки та зниженню ризиків і загроз; 8) гнучкістю впровадження й оновлення: технології мають бути простими у впровадженні, зі зручним користувацьким інтерфейсом, легко оновлюватись і модифікуватись із огляду на зміни державних пріоритетів, нормативно-правової бази чи міжнародних стандартів.

Відтак, пропоновані за Алгоритмом реалізації ГБС-2030 організації реконструктивного просторового розвитку (див., табл. 1) інноваційні технології моніторингу та управління у контексті гібридної регенерації і резилієнтності соціо-еколого-економічних систем, визначених для повоєнного періоду, семи макрорегіонів України мають поєднувати в собі аналітичну потужність, інтегральність, прозорість, адаптивність та безпековий аспект, забезпечуючи ефективну взаємодію усіма складовими сталого національного розвитку і господарювання, а також резилієнтністю економіки.

1. Микитенко, В.В. Критеріальний аналіз потенціалів макрорегіональних зон: формування гібридної стратегії реконструктивного відновлення України. Матеріали Міжнародної науково-практичної конференції «Поліські наукові читання - 2024», 27–29 листопада 2024 року. Чернігів: Національний університет «Чернігівський колегіум» імені Т.Г. Шевченка, 2024. С.251-255.
2. Микитенко, В.В., Драчук, Ю.З. Моніторинг результативності управління сталим господарюванням у критичній інфраструктурі: обґрунтування обсягів витрат. Вісник економічної науки України, 2022, № 2(43). С.72–78. DOI: https://doi.org/10.37405/1729-7206.2022.2(43).72-78.
3. Mykytenko, V.V. Hybrid scenario of the organization of reconstructive spatial development of the economic system of Ukraine. Innovations and New Directions in Scientific Research: Proceedings of the International Scientific Conference (2024, October 14). Manchester, UK: Bookmundo, International Education Development Center, Research Europe, 2024. P.23-26.
4. Микитенко, В.В. Гібридний сценарій реконструкції просторового розвитку України у повоєнному періоді: когнітивно-інформаційний драйвер та інвестиційні епюри. Сучасні досягнення та перспективи науки та освіти: матеріали ІІ Міжнародної науково-практичної конференції (Житомир, 4 жовтня 2024 р). Міжнародний гуманітарний дослідницький центр, Research Europe, 2024. С. 233-238.
5. Микитенко, В.В., Чупріна, М.О. Роль інформаційно-комунікаційних технологій в розвитку економіки. Інформаційно-комунікаційні технології управління сталим розвитком економіки України: колективна монографія; за ред. А.В. Череп, І.М. Дашко, Ю.О. Огренич, О.Г. Череп. Запоріжжя: видавець ФОП Мокшанов В.В. 2024. С. 7-70. DOI https://doi.org/10.5281/zenodo.14229515.

Я.Ю. Дорогий, В.В. Цуркан, О.О. Дорога-Іванюк

КРИТЕРІЇ СТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. У роботі аналізуються сучасні підходи до оцінки стійкості критичної інфраструктури, яка є важливою складовою для забезпечення стабільності та безпеки суспільства. На основі аналізу наукових джерел визначено основні критерії оцінки стійкості інфраструктурних об'єктів, зокрема їх функціональність, здатність до відновлення, стійкість до зовнішніх загроз, гнучкість і адаптивність, економічні витрати, інтеграція з іншими системами, а також миттєвий аналіз і прогнозування.

Вступ. Критична інфраструктура відіграє ключову роль у забезпеченні стабільності та функціональності сучасного суспільства. Її стійкість є важливим аспектом для протидії природним, техногенним і соціальним загрозам, що можуть порушити нормальне функціонування систем. Сучасні дослідження присвячені пошуку критеріїв і методів оцінки стійкості інфраструктурних об'єктів, що дозволяють знизити ризики та підвищити ефективність їхньої роботи навіть в умовах криз. Представлений аналіз наукових джерел дозволяє виділити основні критерії оцінки стійкості критичної інфраструктури, які можуть бути використані як база для подальших досліджень і практичних розробок у цій галузі.

Аналіз літературних джерел. Розвиток сучасних методів управління критичною інфраструктурою в умовах зростання загроз є одним із ключових напрямків наукових досліджень. Актуальність теми стійкості критичних систем обумовлена необхідністю забезпечення їх безперебійного функціонування та швидкого відновлення у разі кризових ситуацій. У цьому контексті важливим є аналіз сучасних підходів, які спрямовані на оцінку стійкості інфраструктурних об’єктів та управління ризиками.

У статті [1] представлено інноваційний підхід до оцінки стійкості критичної інфраструктури в умовах багаторівневих загроз, зокрема для транспортних об'єктів, як ключових компонентів критичної інфраструктури. Авторами розроблено адаптивну методологію, яка інтегрує різні параметри ризику, забезпечуючи надійні основи для прийняття рішень у кризових умовах. Цей підхід є основою для подальших досліджень у сфері управління ризиками.

Наступне дослідження [2] фокусується на новій структурі оцінки стійкості багатокомпонентної критичної інфраструктури. Воно демонструє, як використання сучасних підходів у менеджменті інженерних систем може покращити стійкість до комплексних загроз. Особливу увагу приділено математичним моделям для аналізу міжсистемної залежності, що є важливим для забезпечення безперебійного функціонування інфраструктури.

У статті [3] запропоновано кількісний метод оцінки стійкості взаємозалежних інфраструктур. Математична модель, розроблена авторами, дозволяє оцінювати втрати функціональності та швидкість відновлення систем після надзвичайних подій. Цей підхід враховує взаємозв'язки між компонентами інфраструктури, що робить його значущим для практичних рішень.

Дослідження [4] присвячене розробці метрик для оцінки стійкості електроенергетичних систем. Пропонований підхід інтегрує аналіз операційної та структурної стійкості, що дозволяє розробити стратегії мінімізації ризиків і підвищення надійності енергопостачальних систем.

У роботі [5] розглянуто методологію оцінки стійкості мережевих інфраструктур із акцентом на залежності між елементами систем та їх руйнування. Робота закладає фундамент для розробки ефективних стратегій управління ризиками, що сприяють забезпеченню стійкості критичної інфраструктури.

Таким чином, аналіз існуючих досліджень свідчить про широкий спектр методів, спрямованих на оцінку та забезпечення стійкості критичної інфраструктури. Виявлені підходи підкреслюють важливість системного підходу до аналізу ризиків, управління залежностями між компонентами та розробки адаптивних стратегій. На основі цього можна виділити основні критерії стійкості, які будуть розглянуті нижче.

Основні критерії оцінки стійкості. Проведений аналіз останніх досліджень з тематики стійкості критичної інфраструктури дозволяє визначити кілька ключових критеріїв, які забезпечують всебічну оцінку її стану.

Інфраструктурна функціональність. Один із базових критеріїв стійкості інфраструктури – це її здатність виконувати основні функції в умовах стресових ситуацій. Цей критерій включає оцінку можливості забезпечення безперебійної роботи під час і після природних катастроф, техногенних аварій або інших зовнішніх впливів. Функціональність інфраструктури визначає її роль у підтриманні суспільної стабільності та безпеки.

Можливість відновлення. Відновлення після ушкоджень або порушень є критично важливим аспектом стійкості інфраструктури. Цей критерій враховує час, необхідний для повернення до нормального стану, обсяг ресурсів і заходів, що застосовуються для відновлення функціональності. Висока здатність до відновлення знижує негативні наслідки кризових ситуацій і сприяє швидшій стабілізації.

Стійкість до зовнішніх загроз. Інфраструктура повинна бути готовою до впливу екстремальних факторів, таких як стихійні лиха, техногенні катастрофи, економічні та соціальні кризи. Цей критерій акцентує увагу на запобіжних заходах і підвищенні здатності систем протистояти негативним зовнішнім впливам.

Гнучкість і адаптивність. Здатність інфраструктури адаптуватися до нових умов, включаючи кліматичні зміни, розвиток технологій і зміни політичних та економічних обставин, є ключовим аспектом стійкості. Гнучкість забезпечує ефективну реакцію на непередбачувані зміни та дозволяє знижувати негативні наслідки криз.

Оцінка економічних витрат. Важливим елементом стійкості є аналіз витрат, пов'язаних з відновленням інфраструктури після катастроф. Цей критерій включає прямі витрати на ремонт і відновлення, а також непрямі втрати від переривання функціонування системи.

Інтеграція з іншими системами. Оцінка взаємодії інфраструктурних систем дозволяє зрозуміти, як один збій може вплинути на інші компоненти.

Високий рівень інтеграції сприяє кращій координації та зменшенню негативного впливу на загальну систему.

Миттєвий аналіз та прогнозування. Сучасні технології дозволяють оперативно оцінювати стан інфраструктури та прогнозувати можливі проблеми. Використання великих даних і аналітичних інструментів сприяє підвищенню точності оцінки ризиків і швидкості прийняття рішень.

Гнучкість управлінських структур. Організації, відповідальні за управління критичною інфраструктурою, повинні мати здатність швидко адаптуватися до змін. Ефективне управління включає координацію дій, організацію реагування на кризи та забезпечення відновлення функціональності систем.

Безпека і захист даних. У сучасних умовах кіберзагрози становлять серйозний ризик для критичної інфраструктури. Забезпечення надійного захисту інформаційних систем і даних є важливим аспектом для запобігання кібератакам і збереження стабільності систем.

Екологічна стійкість. Інфраструктурні системи повинні відповідати екологічним стандартам і бути адаптованими до змін у навколишньому середовищі. Цей критерій включає оцінку впливу інфраструктури на екологію та можливості її адаптації до нових екологічних викликів.

Висновки. Розвиток і підвищення стійкості критичної інфраструктури є одним із ключових завдань сучасного суспільства. Визначення критеріїв оцінки стійкості дозволяє проводити комплексний аналіз стану інфраструктурних систем і розробляти ефективні стратегії управління ризиками. Представлений аналіз літературних джерел свідчить про багатовимірність проблеми та необхідність інтеграції технічних, економічних, соціальних і екологічних аспектів у процесі оцінки стійкості. Застосування запропонованих критеріїв сприятиме розробці більш стійких і адаптивних систем, здатних витримувати вплив різноманітних загроз і швидко відновлювати функціональність після кризових ситуацій.

1. Argyroudis, S., Mitoulis, S., Hofer, L., Zanini, M., Tubaldi, E., & Frangopol, D. (2020). Resilience assessment framework for critical infrastructure in a multi-hazard environment: Case study on transport assets. The Science of the Total Environment, 714, 136854. https://doi.org/10.1016/j.scitotenv.2020.136854.
2. Wu, B., Tan, Z., Che, A., & Cui, L. (2024). A novel resilience assessment framework for multi-component critical infrastructure. IEEE Transactions on Engineering Management, 71, 14011–14031. https://doi.org/10.1109/TEM.2024.3438157.
3. Nan, C., & Sansavini, G. (2017). A quantitative method for assessing resilience of interdependent infrastructures. Reliability Engineering and System Safety, 157, 35–53. https://doi.org/10.1016/j.ress.2016.08.013.
4. Panteli, M., Mancarella, P., Trakas, D., Kyriakides, E., & Hatziargyriou, N. (2017). Metrics and quantification of operational and infrastructure resilience in power systems. IEEE Transactions on Power Systems, 32, 4732–4742. https://doi.org/10.1109/TPWRS.2017.2664141.
5. Reed, D., Kapur, K., & Christie, R. (2009). Methodology for assessing the resilience of networked infrastructure. IEEE Systems Journal, 3, 174–180. https://doi.org/10.1109/JSYST.2009.2017396.

В.С. Волошин

АЛЬТЕРНАНИВНІ МОДЕЛІ ПОДІЄВИХ РИЗИКІВ ДЛЯ ДИНАМІЧНИХ СИСТЕМ

Час, події, ентропія системи, її ризики, всі ці показники взаємозалежні, і мають свої смислові позиції щодо предмета даної роботи - значення поняття ризику [1].

Те ж саме стосується і такого показника системи, як ризик, пов'язаний з її існуванням і ефективною роботою. Формально в координатах $R = \psi(\Delta S)$ вперше знаходяться взаємозалежні характеристики: ризик і ентропія. Головною їх якістю є крайня невизначеність цієї залежності. До сих пір об'єктивних публікацій на цю тему в літературі не було, а питання про взаємодію ризику і ентропії системи розглядається лише в узагальнених термінах [2, 3, 4, 5, 6]. Необхідно розуміти, що визначальною координатою для них може бути не тільки час, його односпрямована «стріла», як універсальний показник, присутній в такій координатній сітці, але і послідовна шкала передбачуваних, таких що відбуваються і тих, що вже відбулися, подій [1]. Перехідні процеси для таких подій до теперішнього часу можуть відображатися як індикатори системного ризику. Зокрема, поняття біфуркації як області переходу від стабільності до нестійкого стану і навпаки, або точки переходу системи від невизначеності до чітко визначеного стану і навпаки, може бути пов'язано зі зміною параметра ризикового стану системи в образі бінарного коду - «0;1». Тому цілком об'єктивно, що такі властивості системи повинні бути визначальними для самого поняття «ризик події».

У спрощеному варіанті зростання ентропії ΔS системи є кількісною мірою невпорядкованості, яка визначається числом допустимих подій (C), пов'язаних з системою, як $\Delta S \cong k \ln C$. Ентропія системи тим більше, чим більше можливих допустимих варіантів її станів, що передбачаються з майбутнього, і пов'язаних з ними подій з числа тих, що визначають ці стани в передньому сьогоденні. Це означає, що на майбутній час існує ряд невизначених станів подій $C_{\text{Б}} \gg 1$, а на даний час існує тільки один, чітко визначений стан ризикоутворюючої події $C_{\text{Н}} = 1$, що має місце саме в даний момент. Динамічний перехід від ще невизначеного $C_{\text{Б}} \gg 1$ до повністю визначеного $C_{\text{Н}} = 1$ здійснюється в нескінченно малому часовому інтервалі $\delta\tau \to 0$, що передує теперішньому і який описаний в роботі [1]. Отже, завжди виконується умова $\Delta S_{\text{Б}} \gg \Delta S_{\text{Н}}$ (рис. 1). А ризик отримання від майбутнього чітко визначеної події при переході від невизначеності ризику до чітко визначеної ризикоутворюючої події сьогодення завжди відповідає запису $R \cong (\Delta S_{\text{Б}} - \Delta S_{\text{Н}})/\Delta S_{\text{Б}} \to 1$. Такі розрахунки можуть привести до того, що може стати реальністю навіть стан системи, для якого заявлено, що $R > 1$. Але це суперечить логіці теорії ймовірностей (рис. 1) і підтверджується наступними міркуваннями про функції взаємодії енергії та ентропії тих чи інших подій і пов'язаних з ними ризиків для самих систем. А саме.

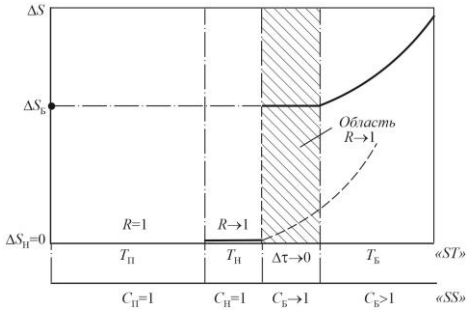


Рисунок 1 – Передбачувана ентропія ризику у співвідношенні часового "ST" та подійового "SS" вимірювання

Для певної системи, що знаходиться в стані слабкої нерівноважності в нескінченно малому інтервалі часу $\delta\tau$, термодинамічний потік J_j, що характеризує швидкість тієї чи іншої події j, залежить від термодинамічних сил F_j, які характеризують потенціал цієї події і визначають послідовність і функціонування інших подій або процесів, що взаємодіють з подією j. Функція дисипації (розсіювання) для такої події пов'язана з цим параметром феноменологічною залежністю Л. Онзагера $\sigma = \sum_{j=1}^{n} B_j J_j F_j$ для слабо нерівноважних систем [6]. У нашому випадку ця функція виконує, крім усього іншого, роль функції обміну ентропією між взаємопов'язаними і послідовними подіями в часі в нескінченно малому інтервалі часу $\delta\tau$ [1].

Величина зміни ентропії може вказувати на ступінь упорядкованості системи, в якій відбувається певна послідовність взаємопов'язаних подій. За Л. Бріллюеном, ступінь упорядкованості Y визначається різницею між максимальним $\Delta_e S_{max}$ і поточним $\Delta_e S$ значеннями ентропії в обміні енергіями між подіями і зовнішнім середовищем. Ступінь невпорядкованості системи X, відповідно, визначається як різниця між поточним $\Delta_e S$ і мінімальним $\Delta_e S_{min}$значеннями ентропії такого обміну, такими, що

$$Y(\tau) = \Delta_e S_{max} - \Delta_e S(\tau); \quad (1)$$

$$X(\tau) = \Delta_e S(\tau) - \Delta_e S_{min} \quad (2)$$

Ступінь упорядкованості і невпорядкованості пов'язана з неоднозначними параметрами вихідної системи і, як правило, не може бути близько порівнянна. У цьому випадку [4] запропоновано переходити до відносних показників для оцінки ступеня впорядкованості системи, наприклад, корелюваних з показниками X і Y в часі, і віднесених до загального масштабу зміни ентропії $\Delta_e S_{max} - \Delta_e S_{min} = \Delta$. При цьому відносне значення для показників упорядкування і невпорядкованості при виконанні очевидної умови $K_Y + K_X = I$ може мати вигляд

$$K_Y = \left(\frac{\Delta_e S_{max}}{\delta\tau} - \frac{\Delta_e S(\tau)}{\delta\tau}\right) / \frac{\Delta}{\delta\tau}. \quad (3)$$

$$K_X = \left(\frac{\Delta_e S(\tau)}{\delta\tau} - \frac{\Delta_e S_{min}}{\delta\tau}\right) / \frac{\Delta}{\delta\tau}. \quad (4)$$

Основним параметром тут є відносна величина зміни локальної питомої зміни ентропії, що бере участь в обмінних процесах системи із зовнішнім середовищем в різні періоди часу.

Методика дослідження визначає 10 випадково вибраних, але впорядкованих і взаємопов'язаних подій для моніторингу та прогнозування найбільш ризикоутворюючих з них, з періодичністю один раз на 5 днів протягом 100 днів. Для кожного ланцюга подій обчислюється відносна величина зміни локальної питомої зміни ентропії за заданий проміжок часу, визначається мінімаксний діапазон і обчислюється значення показників K_Y та K_X. Зі збільшенням відносного значення зміни ентропії значення індексу упорядкування зменшується і, навпаки, зростає значення індексу невпорядкованості. Слід зазначити, що зміна відносного значення локальної питомої зміни ентропії для конкретного ланцюга подій явно не стаціонарна і залежить від безлічі здавалося б випадкових причин. По суті, ланцюжки подій пов'язані між собою своїми причинно-наслідковими зв'язками, що робить їх впізнаваними, а розрахунок зміни ентропії для кожної з них цілком передбачуваним.

Така модель може бути легко представлена у вигляді послідовного орграфа (див. рис. 2), де вершини (qj) є відображенням деяких *передбачуваних* подій (j) або *здійсненої* події «00» на кожному q −рівні прогнозованого інтервалу часу в майбутньому, по відношенню до сьогодення, а ребра графа - причинно-наслідкові зв'язки, які послідовно перетворюють одну $j-$ту причину в іншу, функціонально порівнянну з нею. Тут надані чотири послідовні часові рівні (q=4) запропонованих подій, кожна з яких на своєму рівні є незалежною від інших рівнорівневих подій. І тільки при переміщенні на наступний рівень, з'являється власний міжрівневий зв'язок.

Виділимо три складові:

- очікувані події (чотири рівні в часовому інтервалі майбутнього на рис. 2);
- інтервал подій між потенційними і реальними подіями ($\delta\tau \to 0$);
- область події що відбулася на цей час $T_н$.

Найнижчий, перший, рівень подій показує нам саме біфуркацію, наприклад, у вигляді катастрофи збірки, коли в проміжку часу $\delta\tau$ залишаються тільки три ще невизначених варіанти подій: 11, 12, 13, і тільки одна з них, а саме 12, стає фактично здійсненою вже в момент $\delta\tau$ у теперішньому часі (рис. 2). Ланцюжок передбачуваних подій, що призвели до ризику що здійснився - «00», виглядає наступним чином:

$$00 \leftarrow \overbrace{(12)}^{I} \leftarrow \overbrace{(23)}^{II} \leftarrow \overbrace{(34)}^{III} \leftarrow \overbrace{(34 \to 36)}^{III} \leftarrow \overbrace{(44 \to 46 \to 48 \to 49)}^{IV}$$

Всі інші можливі події, в даному випадку, не привели до реального результату, події «00».

Методологічно такий орграф (рис. 2) формується на основі матрично-хронологічного визначення причинно-наслідкових взаємодій для певної події та умов їх виникнення, які можуть вільним способом змінити послідовність подій, тим самим вносячи в методику високий ступінь невизначеності.

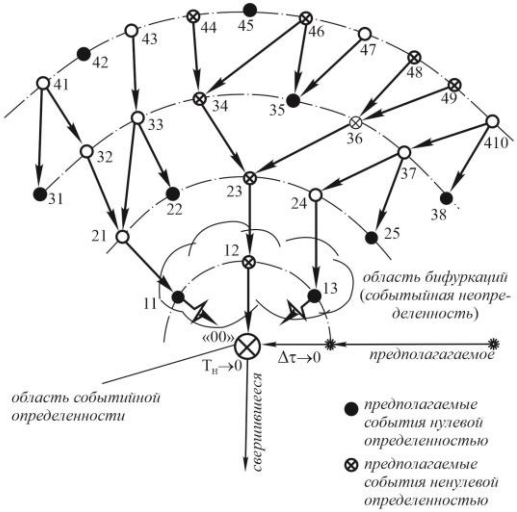


Рисунок 2 – Орієнтований граф відображень подій, що передбачаються, та причинно-наслідкових зв'язків $[J(j=1,1,J) \rightarrow Q(q=1,1,Q)]$ між подіями, що знаходяться у передбаченні до певних рівнозначних умов

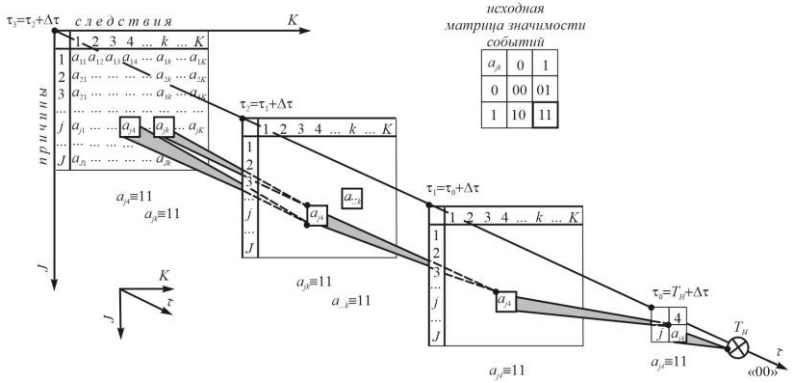


Рисунок 3 –- Динамічні матриці причинно-наслідкових зв'язків для оцінки реальної ризикової події "00" в заданому часовому інтервалі

Причинно-наслідкові взаємодії подієвих процесів легко простежити в кожному конкретному ($i-$ому) одноміттєвому матричному режимі (рис. 3) у вигляді елементів матриці a_{jk}, де: j –порядковий номер причини настання події, $k-$ порядковий номер наслідку, що є підставою для події. Як випливає з таблиці (див. рис. 3), кожному причинно-наслідковому зв'язку може бути присвоєний певний маркер, що складається з нулів і одиниць і відображає відповідність даної події певним умовам. Розмір елемента матриці може бути заданим. Наприклад, якщо елементи матриці відповідності є похідними від експертних оцінок, то вони можуть становити сутність цифрових експертних оцінок. Значення матриці для деякого значення $\tau_i = const$ повністю зберігається, тому що вона має часову складову, яка відокремлює вміст кожного $i-$го елемента матриці в своєму часовому інтервалі τ_i. Це надає певної універсальної форми таким записам. В результаті така матриця дає уявлення про єдину подію, яка стане реальною з передбачуваного майбутнього через проміжок часу, наприклад $3\Delta\tau$. Протягом цього проміжку часу з усіх можливих $a_{j,k}-$их подій ризикоутворююча подія $a_{j,4}$ буде реалізована як така, що реально відбулася.

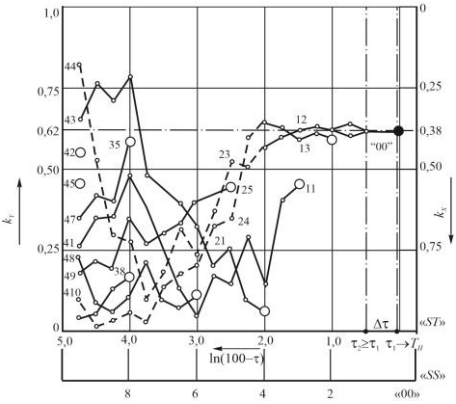


Рисунок 4 – Взаємодія та взаємозв'язки в динаміці змінних показників упорядкування ентропії на шкалах «ST» та «SS» відповідно

Повернемося до рис. 1. Описана тут структурна ієрархія подій передбачає, що на кожному подієвому рівні для кожної передбачуваної події існує своя питома ентропія $\Delta_{p,q}S(\tau)$, де p(0,1,4), q (1,1,10), що визначається за законом Шеннона, і обчислюється в залежності від суми інформації, яка пов'язана з певною послідовністю взаємопов'язаних подій в певному часовому інтервалі. На рис. 4 представлені розрахункові значення показників K_Y і K_X в певному часовому інтервалі, записані для зручності параметричної залежністю $\tau^* = 100 - \tau$, таким чином, що спостерігаються різноспрямовані відносини шкал «ST» і «SS». Протилежність напрямку стріли часу і ентропії, з одного боку, і масштабу подій, з іншого, підкреслюється їх основними властивостями, описаними вище. Для стріли часу і шкали ентропії це послідовність і

неминучість настання наступного часу, подальшого розсіювання енергії або інформації. За масштабами подій це невизначеність і паліативний характер станів, які ще не відбулися. Таким чином, динамічність послідовності подій є похідною від динаміки ентропії системи і визначається цим параметром.

Динаміка відносного значення зміни ентропії окремих подій (див. рис. 2) від хаотичного до впорядкованого стану простежується, зокрема, по наступних ланцюжках: $44 \rightarrow \cdots \rightarrow 23 \rightarrow 12 \rightarrow "00"$. Вони призводять до однозначної події «00», що має властивості об'єктивного ризику. При цьому обране значення індексу впорядкованості дорівнює $K_Y = 0{,}62$. У цих же відносинах був ще один ланцюжок передбачуваних подій: $410 \rightarrow 24 \rightarrow 13$. Однак він, як і всі інші ланцюжки, представлені на рис. 2 не призвели до формування реального ризикоутворення через явно нестабільне значення коефіцієнта K_Y. Решта подійєвих зв'язків тут не оцифровуються тільки через щільність рисунка, та можуть бути простежені читачем самостійно при порівнянні даних, відображених на рис. 2 і на рис. 4. Загальний висновок полягає в тому, що ентропія як міра упорядкованості або невпорядкованості подієвої інформації може представляти варіант презумпціонізму в причинно-наслідкових відносинах між подіями, які передують виникненню реального ризику.

Непереборна відмінність полягає в тому, що майбутнє завжди непередбачуване, а сьогодення цілком визначене. Недосяжність передбачуваного є одним з природних постулатів, на основі якого виникає розуміння невизначеності майбутнього і відповідного ризику. Критерієм такого подолання може бути лише практика того, що сталося у вигляді «накопичувальної ємності подій», що вже відбулися, її вивчення, екстраполяція на майбутні невизначеності, про що свідчать ці методи в практичному застосуванні.

Висновок. Представлена методика є не що інше, як альтернативний метод оцінки та прогнозування ризиків для того чи іншого явища. В даному випадку ризик висвітлюється через послідовність подій, зі своєю енергетикою та інформацією, що призводять до ризикових результатів. Оцінка таких ризикоутворюючих подій проводиться на основі міри розсіювання енергії або інформації, що є індивідуальними для кожного з прогнозованих подій, і робить їх відмінними серед інших.

1. Волошин В. С. Ризик. Альтернативні методи аналізу. Київ. ФОП Семченко. 2024. 490 с.
2. Xiaotian Sun, Sufang An. Early Warning of Systemic Risk in Commodity Markets Based on Transfer Entropy Networks MDPI, *Entropy.* 2024. №6. P.187-192.
3. Renn. K., Schweizer J. ect. Global Polycrisis: The Causal Mechanisms of Crisis Entanglement Cambridge Core, *Global Sustainability.* 2023. №7. P. 231-243.
4. The Second Law of Thermodynamics for Open Systems. LibreTexts Engineering Team. 2023.
5. Systemic Risks and the Connection Between Entropy and Stability in Complex Systems. ScienceDirect, 2022. 117 p.
6. Entropy and Risk in Economic and Social Systems. *Springer.* №11(642). 2022. 251-270 p. Onzager L. Reciprocal Relations in Irreversible Processes I *Physical Review,* Vol. 37. 1931. p. 405–426.

В.С. Волоши

МОЖЛИВОСТІ ОЦІНКИ РИЗИКІВ ВІД ТЕХНОГЕННИХ АВАРІЙ НА ПРИКЛАДІ СЦЕНАРІЮ ПАДДІНГТОНСЬКОЇ КАТАСТРОФИ 1999 РОКУ

У 1999 році на виїзді з вокзалу Паддтінгтон (Лондон) сталася одна з величезних техногенних аварій на транспорті через зіткнення двох поїздів - швидкісної InterCity компанії First Great Western, що прямує з Челтнема до Лондона, і приміського дизель-поїзда компанії Thames Trains, що виїжджає з Лондона [1]. У сучасній техногенній ризикології ця подія стала однією з найбільш значущих, яка вимагала пильної уваги до роботи мобільних систем на транспорті.

Графічна послідовність, або мережа ризикоутворюючих подій показана на рис. 1. Звернемо увагу на хронологічні показники моделі. Очевидно, що аварія сталася в результаті ланцюжка взаємопов'язаних подій, і ризик зіткнення двох поїздів зріс з мінімального нульового за проміжок з часу $t_1 = 8^{07}$ до максимально одиничного в момент часу $t_2 = 8^{11}$ ранку через низку допущених технічних і людських помилок. Перелік і послідовність таких подій наведені в табл. 1. Важливим тут є час від проходження першим поїздом стрілочного переводу на четвертій колії до переходу другого поїзда на цю колію після світлофора SN109. Це так звана точка неповернення, після якої ніякі події не можуть вже зняти реальний ризик зіткнення двох поїздів. Цей мінімальний інтервал (час неповернення) становить $\delta\tau = t_3 - t_2 = 8^{12} - 8^{11} = 1$ хв. У цьому проміжку ризик аварійної події вже дорівнював 1. Нещасний випадок був неминучим.

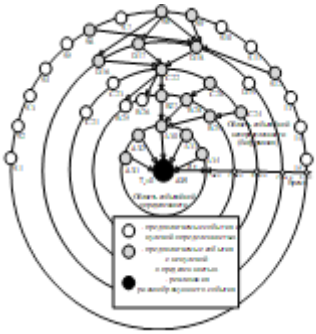


Рисунок 1 – Графічна інтерпретація подій, що призвели до Паддінгтонської аварії

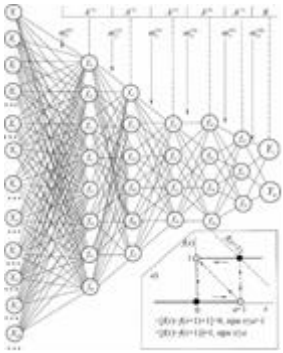


Рисунок 2 – П’ятисинапсна нейромережева модель *NN* для прогнозування та запобігання потенційним ризикам пов’язаним з Паддінгтонською аварією

Таблиця 1. Таблиця відповідності подій у моделі Паддінгтонської аварії

Обозна-чення	Мітка NN	Суть Заходу
S1	x_1	Оголошення про приватизацію залізниці.
S2	x_2	Право на управління залізничною інфраструктурою від приватного монополіста «Rail Train».
S3	x_3	Необхідність проведення планових ремонтів залізниць.
S4	x_4	Відмова від ремонтів залізниці в Паддінгтоні компанією “Rail Train”/
S5	x_5	Установка нових світлофорів з автоматичним оповіщенням водіїв.
S6	x_6	Відсутність системних перевірок світлофорів.
S7	x_7	Професійні дії досвідченого машиніста (8 років досвіду).
S8	x_8	Професійні дії менш досвідченого машиніста (тиждень досвіду).
S9	x_9	Системна погана видимість світлофорів SN109 на виїзді з Паддінгтона.
S10	x_{10}	Вимушений рух на червоне світло при наближенні до світлофора SN109.
S11	x_{11}	Системні зупинки поїздів в районі SN109 за командою поїзної автоматики.
S12	x_{12}	Звичка машиністів до вимикання поїзної сигналізації на світлофорі SN109.
…13	…	Загалом у період з 1995 по 1999 рік на світлофорі SN109 у Паддінгтоні було 8 зупинок поїздів.
…14	…	1995 – Проїзд через SN109 у Паддінгтоні на червоне світло. Поїзд зупинили за 100 м від світлофора.
…15	…	1997. Червоне світло в Саутоллі, аварія ІС: 139 поранених, 7 загиблих. 130 км/год.
D16	x_{13}	Вимушена заміна кваліфікованого машиніста перед поїздкою.
D17	x_{14}	Відсутність досвіду в аварійних ситуаціях у машиніста другого поїзда.
D18	x_{15}	5.10.99 – ранок, сонце заважає видимість світлофору SN109 на виїзді з Лондона.
D19	x_{16}	6.03 – початок руху першого поїзда до Лондона (Паддінгтон).
C20	x_{17}	7.57 – наближення першого поїзда до вокзалу Паддінгтон по IV колії
C21	x_{18}	7.54 – підготовка до відправлення поїзда з Паддінгтона.
C22	x_{19}	8.06 – початок руху поїзда з Паддінгтона по III колії.
C23	x_{20}	8.07 – жовтий сигнал на світлофорі SN109 для другого поїзда.

Кінець таблиці 1

C24	x_{21}	8.07 - автоматичний сигнал в кабіні машиніста відключений і не активується.
B25	x_{22}	8.09 – обмежена видимість червоного світла для другого потягу на світлофорі SN109 з-за сонця.
B26	x_{23}	8.09 – другий поїзд проїжджає світлофор SN109.
B27	x_{24}	8.11 - автоматична спрямованість другого поїзда на IV колію (в бік першого состава).
B28	x_{25}	8.11 – диспетчер не встигає включити червоний світ перед першим поїздом.
B29	x_{26}	8.11- проїзд стрілочного переводу IV колії першим поїздом після світлофора SN120.
A30	x_{27}	**8.11 – точка неповернення.**
A31	x_{28}	8.12 – зіткнення поїздів.
A32	x_{29}	8.12 – механічні розриви паливних баків.
A33	x_{30}	8.12 – іскріння внаслідок зіткнення та тертя металу об метал.
A34	x_{31}	8.12 - вибухи паливних баків.
A35	x_{32}	**8.12 – факт аварії.**
…	**…**	**…**
O36	x_{33}	**Відсутність аварії.**

Звернемося до проблеми потенційного ризику повторення трагедії Паддінгтона. Вона може виглядати так. «*Знайти відображення образів подій, що передували Паддінгтонській трагедії, які утворять безперервний ряд з реальними причинно-наслідковими зв'язками, і можуть призвести, а можуть і не привести до означеної катастрофи*». Тобто ми свідомо орієнтуємо вирішення проблеми лише на два результати: станеться аварія $(\text{ризик } Y_1 = 1)$ або аварія буде виключена $(\text{ризик } Y_0 = 0)$.

Для управління ризиком в даному випадку використовується п'ятисинапсна модель нейронної мережі NS (рис. 2). Кількість нейронів у кожному з п'яти шарів синапсу вибирається виходячи з логіки руху сигналу. Обмежуючим фактором тут виступає навіть не кількість вхідних сигналів в мережі, а їх невизначеність, а також мінливість при роботі такої мережі. Наприклад, перший шар синапсу має справу з 42 зовнішніми сигналами. З означеними 8 нейронами першого прихованого шару показано, вирішальна система повинна мати можливість вибирати з 294 варіантів подій. Потім до другого синапсу їх число збільшується до 13 818 варіантів подій і так далі. При цьому кожен наступний синапс повинен мати раціональне поєднання нейронів, меншої кількості, ніж в попередньому прихованому шарі, щоб рішення завдання не було зайвим.

Перший прихований шар синапсів в моделі *NN*, що складається з 8 нейронів, представлений як відповідальний за поведінку і подієвість, пов'язану з

інфраструктурою системи (стаціонарні елементи – шляхи, стрілки, світлофори, диспетчерська служба). Перевага сигналу залежить від комбінації вагових коефіцієнтів m_{i1}^{01} від кожного вхідного сигналу до кожного нейрона «навченого» першого шару. Другий прихований шар синапсів включає в себе нейрони, налаштовані на образи подій рухомих частин системи (поїздів, машиністів, їх підготовки, системи автоматичного оповіщення в кабінах поїздів, мобільну видимість світлофорів). Система переваг в цьому шарі визначається коефіцієнтами, що позначаються в системі навчання як m_{i2}^{12}. Третій і четвертий шари синапсів представлені можливостями порівняння сигналів першого і другого шарів з метою узгодження їх для образності і комбінації найбільш активних з них в залежності від поєднання коефіцієнтів переваги сигнальних зображень m_{i1}^{01} та m_{i2}^{12} з коефіцієнтом m_{i3}^{23}, а також комбінації коефіцієнтів m_{i1}^{01}, m_{i2}^{12} і m_{i3}^{23} з коефіцієнтом m_{i4}^{34} за принципом

$$max m_{i1}^{01} \cap max m_{i2}^{12} \rightarrow m_{i3}^{23} \quad \text{та} \tag{1}$$

$$max m_{i1}^{01} \cap max m_{i2}^{12} \cap max m_{i3}^{23} \rightarrow m_{i4}^{34}. \tag{2}$$

І, нарешті, п'ятий, останній прихований шар синапсів буде налаштований на синхронізацію активних сигналів двох попередніх нейронних шарів з метою отримання відношення сигналів двох груп нейронів (I і II шарів) до вихідних параметрів моделі Y_1 або Y_0, як підсумок роботи всієї частини прихованих шарів моделі нейронної мережі за умовою

$$max m_{i3}^{23} \cap max m_{i4}^{34} \rightarrow m_{i5}^{45} \text{ та} \tag{3}$$

$$max m_{i3}^{23} \cap max m_{i4}^{34} \cap max m_{i5}^{45} \rightarrow m_{iR}^{5R}. \tag{4}$$

Другою умовою вибору для прихованих шарів активації є тип самої функції активації для нейронів кожного шару. В якості функції активації ($f(x)$ нейронів синапсу виберемо біфуркаційну залежність подвоєного облікового періоду в зв'язку з кількістю і невизначеністю змісту облікових показників, що впливають на кінцевий результат (рис. 2, а).

При створенні такої моделі ми будемо використовувати можливості відкритої бібліотеки програм з надбудовою *Keras*, а також ресурс бібліотеки *MLOps* на платформі *TensorFlow* [2, 3]. При цьому інструментарій машинного навчання *Comet* на мовній платформі *Python* сумісний з існуючими *ML*-бібліотеками, що дозволяє працювати з кодованими параметрами і метриками в напрямку прогнозування вихідних сигналів. Крім того, інструмент *Comet* включає необхідні набори функцій інтеграції для внутрішньої синапсичної бази даних і спрощує їх узгодження з іншим програмним забезпеченням *Machine Learning.*

Вихідні дані для системи тренування NS (*back propogation*) наступні:
- поріг активації моделі приймається для негативних рішень $h_{Y_0} = 0{,}055$, для позитивних рішень - $h_{Y_1} = 1{,}000$;
- параметр очікуваного результату у всіх випадках $D = 12$;
- крок збіжності за алгоритмом «back propagation» $\lambda = 0{,}0001$;
- задана помилка пошуку в мережі $\varepsilon_{зад}$=0.0025.

При цьому вагові коефіцієнти, як носії «пам'яті» нейронної мережі, зазнають суттєвих змін.

Результати моделювання *NN* заданої конфігурації для ідентифікації можливих аварій в системі залізничних перевезень на Великій Західній головній лінії залізниць Великобританії, в обсязі зазначених вхідних сигналів, представлені в табл. 2. Перш за все, звернемо увагу на події, які закінчуються сумою вихідних сигналів $Y_1, Y_0 = [0, 1]$, тобто однозначним підтвердженням умов, коли аварія стає неможливою. Це стосується в першу чергу контролю вхідних сигналів x_3 та x_8, а саме - актуальності своєчасного ремонту всієї залізничної інфраструктури, а також допуску до експлуатації поїздів тільки висококваліфікованих машиністів. За цими параметрами функція початкової біфуркації зведена до мінімуму $minf_3^{A^{(5)}} = 0{,}0001 \approx 0$ і $minf_8^{A^{(5)}} = 0{,}0023 \approx 0$, відповідно. Те ж саме відноситься до вхідних сигналів x_{25} та x_{27} – своєчасне відновлення видимості ключового світлофора SN109 в сонячну погоду і своєчасне повернення стрілочного переводу з 4-ї на 3-ю колію для другого поїзда. Про це свідчить досягнення мінімального значення параметра функції активації тільки до п'ятого синапсу $\left(minf_{25}^{A^{(5)}} = 0{,}00128\right)$ і $\left(minf_{27}^{A^{(5)}} = 0{,}0021\right)$ відповідно.

Події x_4 та x_6 також залишають простір для уникнення аварійної ситуації, але їх функція сумарної активації в останньому синапсі 0,9589 і 9,7757 відповідно, перевищує поріг активації моделі і тому не може бути зарахована як значуща. Для урахування таких подій в моделі, потрібно доповнення іншими неврахованими раніше подіями. Але при цьому модель повинна бути перетренованою, що є одним з її недоліків.

Таблиця 2. Результати роботи *NN* в умовах заданих вхідних сигналів бінарного змісту (світлий колір вказує на вихідні функції системи, які не призводять до реалізації ризику, темний колір вказує на вихідні функції системи, які однозначно призводять до реалізації ризику)

x_i	$m_i^{(A)}$	$m_i^{(A)'}$	$f_i^{A^{(1)}}$	$f_i^{A^{(2)}}$	$f_i^{A^{(3)}}$	$f_i^{A^{(4)}}$	$f_i^{A^{(5)}}$	$Y_1; Y_0$
x_1	0	**0,316**	1,0902721	3,0454421	2,7798888	2,5455654	2,5405554	0; 0
x_2	1	**0,516**	4,3298578	2,7778752	4,1545567	4,2194489	4,1329321	0; 0
x_3	1	**1,932**	0,0001906	0,0001199	0,0001843	0,001934	0,0001651	0; 1
x_4	1	**1,873**	0,5545567	0,9815545	1,1329185	0,9654705	0,9589579	1; 0
x_5	0	**0,045**	2,1186398	2,2988688	1,9823245	2,1184412	2,1524658	1; 1
x_6	1	**1,695**	12,3478122	10,8269352	9,0825580	10,1119111	9,7757794	1; 0

Кінець таблиці 2

x_7	0	**0,451**	0,3845009	0,2569285	0,2321542	0,2778789	0,2545682	1; 1
x_8	1	**1,777**	0,0355483	0,0717111	0,0344444	0,0997683	0,0023617	0; 1
x_9	1	**1,033**	0,1734185	0,3274457	0,2254411	0,9184457	1,0124458	1; 0
x_{10}	1	**0,774**	35,2108235	22,7774602	19,7773759	17,1128290	15,3535550	0; 0
x_{11}	0	**0,581**	18,2548938	24,5545109	2,8759781	5,5564781	8,9997078	1; 1
x_{12}	1	**1,163**	0,2846008	0,3837915	0,4795554	0,7274222	1,0054123	1; 0
x_{13}	0	**0,984**	-	-	-	-	-	0; 0
x_{14}	1	**0,269**	-	-	-	-	-	0; 0
x_{15}	1	**1,759**	-	-	-	-	-	0; 0
x_{16}	0	**0,519**	2,9455554	5,9476654	7,8112223	3,4565847	3,9898334	0; 0
x_{17}	1	**1,823**	0,1459093	0,1296777	0,0451612	0,9175258	1,0032774	1; 0
x_{18}	1	**0,771**	33,7777936	5,5489453	1,2356778	5,0098692	4,0091001	1; 1
x_{19}	0	**0,031**	25,0916666	31,4071045	13,7587555	12,9801421	12,2009689	0; 0
x_{20}	0	**0,256**	38,1104435	35,0931680	29,2128235	37,7278456	35,0091258	1; 1
x_{21}	0	**0,011**	24,1738907	25,0092721	13,1122456	47,2809492	29,1111693	0; 0
x_{22}	0	**0,033**	13,0167777	7,1765270	5,9167729	3,0008846	4,0155370	0; 0
x_{23}	0	**0,718**	1,2777416	0.8912121	0,5561141	1,5783436	1,5504704	1; 1
x_{24}	1	**1,199**	7,0810027	5,3914321	31,1545521	13,7778178	15,2893332	1; 1
x_{25}	1	**1,558**	2,7353359	2,1835583	1,8169480	1,2555500	0,0012889	0; 1
x_{26}	0	**1,481**	1,5482121	1,4802179	1,0930033	0,5569614	0,2255145	0; 0
x_{27}	1	**1,092**	7,1649267	3,1054471	5,7538122	1,4022045	0,0021009	0; 1
x_{28}	1	**1,111**	0,6899888	0,3501487	0,7772275	1,0087729	1,0882588	1; 0
x_{29}	0	**1,589**	7,5755116	9,2846554	5,9888567	6,1235556	6,0009912	1; 1
x_{30}	1	**1,997**	0,2548802	0,0917295	0,0146465	0,0922112	0,05511165	1; 1
x_{31}	1	**1,310**	0,9821495	0,64152169	0,2100123	0,0650721	0,0794431	1; 1
x_{32}	1	**0,823**	1,9619555	0,8829444	1,3494005	1,4309285	1,3502947	1; 1
x_{33}	1	**1,448**	4,6559554	3,9483687	4,0197592	5,4648789	4,2605704	1; 1
x_{34}	1	**1,581**	1,7754498	0,9501111	2,8804400	1,5609090	1,0542009	1; 0
x_{37}	1	**0,786**	4,3859026	6,9888290	3,2155555	2,1235514	2,2263451	1; 1
x_{38}	1	**1,138**	8,849314	9,1274563	8,92754326	7,3331007	7,3749816	1; 1
x_{39}	1	**1,327**	1,5758281	2,1095378	1,7395587	1,9845389	1,1221381	1; 1
x_{40}	1	**1,126**	0,4519482	0,45932276	0,49675254	0,44891321	0,42071603	1; 1
x_{41}	1	**1,064**	0,4581111	0,2100154	0,3841110	0,6547345	0,9810098	1; 0
x_{42}	1	**0,555**	7,2109008	6,5409119	6,2889629	6,92671123	6,5455000	0; 0

Безумовно, нас цікавлять вхідні сигнали в моделях, які однозначно призводять до реалізації ризиків при заданій структурі вхідних сигналів. Вони представлені в табл. 3.

Таблиця 3. Потенційні ризикові події при заданих вхідних сигналах (x_i) для моделі нейронної мережі Паддінгтонської аварії (при умовах $max f_i^{A^{(5)}} \to 1$)

x_i	Y_1, Y_0	$max f_i^{A^{(5)}}$	Зміст патерна
x_9	1, 0	1,0124	Системна недостатність видимості світлофорів SN109 на виїзді з Паддінгтона
x_{12}	1, 0	1,1054	Звичка машиністів до вмикання поїзної сигналізації на SN109
x_{17}	1, 0	1,2032	Відсутність досвіду роботи в аварійних ситуаціях у машиніста другого поїзда.
x_{28}	1, 0	1,1882	Затримка диспетчером включення красного світла перед першим потягом

Кінець таблиці 3

x_{34}	1, 0	1,1542	Наявність повних паливних баків без додаткового захисту від детонації
x_{41}	1, 0	0,82109	Страйки обслуговуючого персоналу та заміна його менш кваліфікованими

Модель показала, що попереднє виключення хоча б однієї будь-якої з можливих помилок в межах траєкторії S8-D16(D17(D18))-C22-B27-A30-A35 не призведе до реалізації образу ризикоутворюючої події табл. 2). У цьому випадку модель представляє як превентивний захід уникнення події S3, що цілком очевидно, або уникнення події S8, яка пов'язана з попередньою роботою з підготовки машиністів і не завжди поєднується з можливими ризиками конкретного походження. Але такі результати можуть бути підтверджені і візуально (рис. 1), що лише підкреслює правильність роботи *NN*.

А ось на траєкторії S12-D18-C22-B27-A30-A35 вже потрібно буде усунути дві можливі помилки, щоб мінімізувати ризик, що є більш складним завданням для звичайної профілактики, а без моделювання він не завжди може проявитися, як потенційний ризик. А якщо взяти до уваги комбінації подій S3 і S5, які ми спочатку вважали припущеними з нульовою впевненістю, але в нашій моделі *NN* вони стають ризикоутворюючими (табл. 2), то результати, отримані моделлю при візуальному огляді цієї траєкторії, взагалі не можуть бути виявлені як передбачені, без моделювання.

Найважливіші помилки в системі, що призводять до реалізації ризику, були пов'язані з подіями в області подієвої невизначеності (біфуркації, рис. 1), а саме B27, B28, B29 і ті, що передують їм - C20, C22, C24. Врахування таких ланцюгів дає можливість забезпечити попередження ризику або на ранніх значних часових інтервалах, або в моменти, що передують виникненню подієвої невизначеності, яка в цьому випадку називається «точкою неповернення».

Представляє інтерес така послідовність подій, як S6(S9(S12))-D18-C22-[біфуркація], що позначена моделлю *NN* і відсутня на схемі (рис. 1), Вона пов'язана з роботою світлофорів і звично пасивною реакцією на їх сигнали з боку машиніста в яскравий сонячний день. Ця залежність однозначно призводить до подієвої невизначеності (послідовність біфуркації сигналів в прихованих синапсах системи), яка полягає у втраті диспетчером контролю над послідовністю подій і відсутність будь-яких превентивних дій. Причиною цього є непідготовленість диспетчерського персоналу, яка взагалі не була врахована Комісією, і їх головна помилка, виключення якої могло б завадити ризику матеріалізуватися зі 100% впевненістю. Це результат, який дає модель NS, всупереч виявлених нами причинно-наслідковим подій (рис. 1). Логічне трактування цього ланцюжка подій повністю вписується у відомий сценарій того, що сталося.

Функціональну визначеність іншого виду супроводжують вхідні сигнали x_{20} та x_{24} з аномально малими ваговими коефіцієнтами відносно початкових. Їх

зміст при проходженні сигналу через всі п'ять синапсів є незмінно впливовим для системи, але явно невизначеним: факт реалізації образу ризикоутворюючої події існує, але при цьому підтверджується і його відсутність (1, 1). Таке пояснення не є логічним, і NS відкидає його зі значеннями вже навчених вагових коефіцієнтів для цих сигналів. Для інших подібних результатів модель показує приблизно однакові вагові коефіцієнти, що вказує на їх рівну участь у NS.

Висновок. Попередження подібних аварій за допомогою нейронних мереж має зводитися до автоматичного відстеження зображень потенційних ризикоутворюючих подій, закладених при навчанні у *NN*, та попередження принаймні одного-двох з таких, що відстежуються. Слід зазначити, що така модель *NN* може бути корисною не тільки для умов Великої Західної головної лінії залізниць Великобританії, але і для інших систем, на які поширюються ті ж правила експлуатації, що і в нашому прикладі. Звичайно, з відповідною перепідготовкою.

1. Ladbroke Grove rail disaster. Електроннийй ресурс – [режим доступу]:http://www.london-fire.gov.uk/museum/history-and-stoties/historical-fire-and-incidents/Ladbroke-grove-rail-disaster/.
2. Abadi M., Agarwal A., Barham P., Brevdo E. and oth. TensorFlow: Large-Scale Machine Learning on Heterogeneous Distributed Systems (Preliminary White Paper, November 9, 2015)//Електронний ресурс – [режим доступу]: https://static.googleusercontent.com/media/ research.google.com/en//pubs/archive/ 45166.pdf.
3. Eryurek T., Gilad U., Lakshmanan V., Kubunguchy-Grant A., Ashdown J. Data Governance: The Definitive Guide, and Tools to Operationalize Data Trustworthiness. Beijng-Boston-Tokyo. O'Reilly. 2021. 428 p.

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

ПІДВИЩЕННЯ ЕКОЛОГІЧНОЇ РЕЗИЛЬЄНТНОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЗА ДОПОМОГОЮ БПЛА, ДОПОВНЕНОЇ РЕАЛЬНОСТІ ТА КІБЕРБЕЗПЕКИ

Війна та вплив форс-мажорних факторів призводять до появи негативних наслідків у вигляді пожеж на об'єктах критичної інфраструктури. Зокрема це стосується об'єктів енергетики, де пожежі відбувались і в мирний час - у наслідок природних впливів (висока температура повітря) або технічних аварій (коротке замикання) [1].

З метою профілактичного попередження та швидкого реагування на пожежі, що виникнули на об'єктах критичної інфраструктури пропонується застосовувати беспілотні літальні апарати. Це дозволяє:

1. Здійснювати в атоматичному режимі профілактичні заходи з метою недопущення пожеж під впливом зовнішніх негативних факторів шляхом здійнення профілактичних регулярних обльотів небезпечних точок об'єкту критичної інфраструктури по заздалегідь заданому маршруту та розкладу [2].

2. При раптовому виникненні пожежі - швидко доставляти засоби пожежогасіння [3] в зону вогню, що буде сприяти швидкій локалізації пожежі та зменшувати збитки завдані вогнем об'єкту критичної інфраструктури.

3. Швидке прибуття БПЛА на місце пожежі дозволяє завдяки зворотньому каналу відеозв'язку [4] - отримати актуальну інформацію про пожежу, її масштаби і прийняти правильні рішення, щодо задіяння сил та засобів необхідних для її пожежогасіння.

З метою отримання відеоінформації можна використовувати стандартні засоби відображення. Однак з погляду інформативності краще застосовувати технологію доповненої реальності, яка дозволяє одночасно з виводом відеозображення з БПЛА, надавати відповідальній особі іншу необхідну інформацію [5] - температуру повітря, точні GPS координати, наявність сил та засобів, які готові до застосування у даний момент для локалізації пожежі, аналітику щодо ефективності гасіння пожежі при використанні різних комбінацій сил та засобів тощо. Використання гарнітур доповненої реальності зменшує час локалізації і гасіння пожежі та підвищує таким чином резильєнтність об'єкту критичної інфраструктури.

Одночасно слід зауважити, що на об'єкті критичної інфраструктури, окрім відеоданих з БПЛА також циркулює значна кількість інформації з обмеженим доступом, яка також використовується в управлінні об'єктом та повинна відображатися на гарнітурі доповеної реальності відповідальної особи. Тому з'являється завдання по кібербезпеці - розділити ці потоки даних та унеможливити можливість витоку даних з обмеженим доступом у потік даних з відкритим доступом. Для цього слід застосовувати удосконалені методи двонаправленої передачі даних у системах з циркуляцією інформації з різним ступенем обмеження доступу.

Як зазначає Горлинський В.В. «Наука – це одночасно і виробнича сила, і соціальний інститут, і діяльність з метою одержання нових знань, і результат діяльності як система одержаних знань. Вплив науки на культуру здійснюється і через систему освіти. У сучасному суспільстві університетську освіту розуміють як підготовку фахівців на основі найсучасніших наукових знань, технологічних і дослідницьких практик, що гарантують необхідні компетентності – спроможність використовувати отримані знання, уміння й особистісні здібності для професійного і персонального розвитку» [6, с.60]. На сьогодні відбуваються значущі зміни в розвитку техніки та її впливі на суспільство, зокрема розвиток технологій машинного навчання, використовується для діагностики захворювань (зокрема раку) або розробки ліків.

Сучасна екологія займає особливе місце, адже вплив техніки на довкілля змусив суспільство переглянути підходи до природокористування. Країни почали заохочувати інновації, які мінімізують викиди парникових газів, забруднення повітря і води. При проектуванні промислових об'єктів почали враховувати повний життєвий цикл продуктів, щоб зменшити кількість відходів. Перехід до електромобілів і використання відновлюваних джерел енергії стає важливим кроком до осмислення людиною потреби балансу між розвитком технологій та екологію. Вдале застосування наукових досліджень в автомобільній промисловості, вже значно знижує залежність від викопного палива. Інвестування в наукові дослідження для вдосконалення зменшення використання невідновлюваних ресурсів і перехід на замкнуті цикли виробництва.

Як пише І. С. Добронравова у підручнику Філософія науки «Найвищим рівнем осмислення всіх вимірів сучасної екології є філософія екології» [7, с. 130]. Філософія екології — це найвищий рівень осмислення екологічних питань, що інтегрує природничі, соціальні та гуманітарні аспекти. Вона зосереджується на розумінні зв'язків між людиною, природою та технологіями, вивчає етичні, культурні та світоглядні виміри ставлення до довкілля.

Технології можуть створити нові екологічні загрози, якщо їх завчасно не протестувати. Застосування БПЛА для профілактики та реагування на пожежі на об'єктах критичної інфраструктури є ефективним засобом для підвищення безпеки та зниження ризиків, пов'язаних із впливом форс-мажорних факторів. Технологія доповненої реальності сприяє оперативному прийняттю рішень під час пожежогасіння, надаючи відповідальним особам важливу інформацію в реальному часі, що підвищує ефективність локалізації пожежі. Кібербезпека на об'єктах критичної інфраструктури є необхідною для забезпечення захисту даних з обмеженим доступом, що використовуються у процесі управління інфраструктурою.

Екологічна резильєнтність об'єктів критичної інфраструктури може бути значно підвищена завдяки інтеграції новітніх технологій, що дозволяють зменшити вплив зовнішніх загроз і забезпечити безперервність функціонування важливих об'єктів.

1. Олексій ЛИПАР, Роман ШЕВЧЕНКО ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ РОБОТЕХНІЧНИХ ЗАСОБІВ ГАСІННЯ ПОЖЕЖ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: "НАУКА ПРО ЦИВІЛЬНИЙ ЗАХИСТ ЯК ШЛЯХ СТАНОВЛЕННЯ МОЛОДИХ ВЧЕНИХ" МАТЕРІАЛИ Всеукраїнської науково-практичної конференції курсантів, студентів, ад'юнктів (аспірантів) 2023 С.155.
2. А.В. Шишацький, С.О. Кашкевич АНАЛІЗ ФОРМ ТА СПОСОБІВ ЗАСТОСУВАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ The 22th International scientific and practical conference "Modern theories and improvement of world methods" (June 06 – 09, 2023) Helsinki, Finland. International Science Group. 2023. 543 p. DOI – 10.46299/ISG.2023.1.22 с.517.
3. Паспорт самосрабатывающего огнетушителя ШАР-«АFO» (https://magazin01.ru/upload/iblock/041/nbpaah7gsd0guzw6bysxe08xnaq1zi48/shar_afo_pasport.pdf?srsltid=AfmBOooFSN-fdUFbuphjnVS5K9JYph9UPWSXTVj9SOsXm9MfYxbna91K).
4. Могильна А.С., Савченко О. В. ТЕОРІЯ ТА ПРАКТИКА ВИКОРИСТАННЯ БПЛА У ДСНС ДЛЯ ЛІКВІДАЦІЇ НАСЛІДКІВ НС: Матеріали Всеукраїнської науково-практичної Інтернет-конференції здобувачів вищої освіти і молодих учених «Метрологічні аспекти прийняття рішень в умовах роботи на техногенно небезпечних об'єктах» 2 листопада 2023 р., м. Харків, Україна с.158.
5. Tao Zhan2 Kun Yin2 · Jianghao Xiong · Ziqian He · Shin-Tson Wu Augmented Reality and Virtual Reality Displays: Perspectives and Challenges Perspective Volume 23, Issue 8101397August 21, 2020 https://doi.org/10.1016/j.isci.2020.101397 Available online: https://www.cell.com/iscience/fulltext/S2589-0042(20)30585-X?sf237492657=1 (accessed on 10 December 2024).
6. Філософські проблеми наукового пізнання: навчальний посібник. / В. О. Ананьїн, В. В. Горлинський, О. О. Пучков. О. В. Уваркіна; за ред. В. О. Ананьїна. Київ : ІСЗЗІ «КПІ ім. Ігоря Сікорського», 2018. 170 с.
7. Філософія науки: підручник / І. С. Добронравова, Л. І. Сидоренко, В. Л.Чуйко та ін.; за ред. І. С. Добронравової. Київ : ВПЦ "Київський університет", 2018. 255 с.

O. Ogir

RESILIENCE OF ENERGY INFRASTRUCTURE IN WARTIME. ASSESSMENT METHODS AND PATHWAYS FOR IMPROVEMENT

The resilience of energy infrastructure is a critical factor in ensuring the stability of energy systems, especially in wartime. In the context of the war in Ukraine, this problem has become one of the most important, after the aggression by Russia is systematically trying to destroy the country's energy infrastructure. Attacks on energy facilities, in particular missile strikes, cyberattacks, sabotage, threaten not only a stable electricity supply, but also the overall functionality of the country, including the medical sector, transport and other critical infrastructure. In this context, assessing the resilience of energy facilities is of utmost importance to prevent or minimize the consequences of such attacks. The resilience of energy facilities can be configured as their ability to adapt to changing conditions, withstand external threats and quickly recover from failures.

Key criteria for resilience in wartime are:

- Resistance to physical damage (e.g., missile or drone strikes).
- Integration of early warning systems (including SCADA – Supervisory Control and Data Acquisition).
- Ability to operate in an autonomous mode (using microgrids or mobile energy sources).
- Introduction of renewable energy sources (RES – wind, solar, biogas plants).

Another aspect is the adaptability of energy facilities, i.e. their ability to change operating modes depending on changing conditions. In wartime, when CI is often exposed to sources of damage, it is important that energy systems can operate autonomously or with alternative energy sources [1]. This may include the use of mobile generators, solar panels or wind turbines. The adaptability of the system allows to minimize energy losses and ensure uninterrupted energy supply even in the event of destruction of the main sources. The speed of recovery after damage is another important indicator of resilience. In wartime, when any support can have serious consequences, rapid recovery of energy facilities is critical. The use of backup energy sources and the availability of effective response mechanisms will not allow for the rapid recovery of destroyed infrastructure. Modeling various failure scenarios and the use of modern mathematical modeling methods, such as MC methods or probability analysis, do not allow for the prediction of risks and optimization of recovery.

Various methods are used to assess the resilience of energy facilities in wartime. One of the main ones is system analysis, which allows for the identification of key nodes of the energy network that are critical for its functioning. Graph theory, in particular, makes it possible to model the structure of the energy network and identify vulnerabilities that may become targets of attacks. Engineering assessment methods involve the modeling of extreme scenarios that take into account physical damage to

facilities, as well as the use of technical means to increase their resilience. Mathematical modeling is also used to predict possible scenarios and assess the probability of damage to key infrastructure elements. For example, models that estimate the probability of failure of energy network components allow developing strategies to minimize these losses. In addition, big data (Big Data) and machine learning technologies allow for real-time monitoring and definitively detecting anomalies, allowing for a rapid response to emerging threats.

Another important aspect is the integration of renewable energy sources (RES), such as solar and wind power plants, as well as the development of microgrids that can operate independently of the main power grid. The implementation of such technologies allows for energy security to be reduced, ensuring dependence on central energy sources and ensuring autonomy even in the event of serious damage to the main infrastructure. All these methods and approaches do not allow for increasing the resilience of energy facilities in war conditions, but for effective application, international cooperation and the implementation of uniform standards for risk assessment and management are also necessary. Developing clear protocols for responding to attacks, training personnel, and integrating new technologies into energy systems are necessary steps to increase their resilience and efficiency [2].

In conclusion, Ukraine's experience in ensuring the resilience of energy facilities in wartime can be valuable to other countries facing similar challenges. The integration of innovative technologies, the development of renewable energy sources, and the improvement of monitoring systems not only increase the resilience of energy systems, but also ensure energy security in global crisis situations.

1. National Institute for Strategic Studies. (2023). Resilience of critical functions implementation: summarizing Ukraine's experience in responding to the destruction of energy infrastructure. https://niss.gov.ua/publikatsiyi/analitychni-dopovidi/stiykist-krytychnoyi-enerhetychnoyi-infrastruktury-ta.
2. Ukrhydroenergo. (2024). Ukrhydroenergo estimates losses from Russian attacks at over 3 billion euros [Press release]. https://www.italaw.com/sites/default/files/case-documents/italaw181408.pdf.

С.В. Матвєєв, І.В. Івченко

ЗАБЕЗПЕЧЕННЯ РЕЗИЛЬЄНТНОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ ШЛЯХОМ ОПТИМІЗАЦІЇ ЕНЕРГОСПОЖИВАННЯ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ

Анотація: У статті розглядається актуальність впровадження енергоефективних рішень у системах штучного інтелекту (ШІ) для забезпечення резильєнтності критичної інфраструктури України. Зокрема, аналізуються методи оптимізації енергоспоживання у ШІ-системах, їх роль у підвищенні стійкості інфраструктури, а також міжнародний досвід у цій галузі. Представлено рекомендації щодо інтеграції енергоощадних технологій у процес розробки та впровадження ШІ в критичну інфраструктуру.

Штучний інтелект стає невід'ємною частиною сучасної критичної інфраструктури, зокрема енергетики, транспорту, логістики та охорони здоров'я. Його використання дозволяє значно підвищити ефективність, автоматизацію та стійкість систем. Однак високий рівень енергоспоживання, пов’язаний із обробкою великих обсягів даних і навчанням моделей ШІ, створює ризики для енергетичної стабільності, особливо в умовах надзвичайних ситуацій.

В Україні, де війна та інші кризи ускладнюють стабільне функціонування інфраструктури, оптимізація енергоспоживання ШІ є важливим чинником забезпечення резильєнтності [1].

Штучний інтелект має значний потенціал у підвищенні ефективності та резильєнтності децентралізованих енергосистем. Одним із ключових напрямків використання ШІ є прогнозування попиту на енергію та оптимізація розподілу ресурсів. ШІ здатний аналізувати велику кількість даних у режимі реального часу, що дозволяє управляти генерацією та споживанням енергії з урахуванням попиту та пропозиції.

Використання ШІ в смарт-грід системах дозволяє інтегрувати відновлювані джерела енергії та автоматично балансувати навантаження на мережу. Застосування смарт-грід технологій може підвищити ефективність енергосистеми на 20-30% і знизити ризик відключень. Наприклад, у США системи на основі ШІ допомагають зменшити втрати у високовольтних мережах на 10–15% [2].

У дослідженні від компанії McKinsey зазначається, що інтеграція ШІ в енергетичні системи дозволяє скоротити енергетичні втрати та підвищити ефективність управління ресурсами. Це особливо важливо для України, яка активно впроваджує відновлювані джерела енергії, такі як сонячні та вітрові електростанції, і прагне до децентралізації енергопостачання [3].

Використання штучного інтелекту у транспортній інфраструктурі відіграє дуже важливу роль. Інтелектуальні транспортні системи (ITS), які базуються на алгоритмах штучного інтелекту, можуть оптимізувати управління дорожнім

рухом. Завдяки аналізу даних у реальному часі (з камер спостереження, датчиків на дорогах, GPS) такі системи:

- зменшують затори на дорогах;
- автоматично коригують роботу світлофорів, враховуючи навантаження;
- забезпечують безперебійну роботу громадського транспорту, адаптуючи маршрути до змін у транспортному потоці.

Штучний інтелект може аналізувати маршрути транспортування вантажів, враховуючи стан доріг, мости та погодні умови. Наприклад, система може прогнозувати оптимальний маршрут для доставки гуманітарної допомоги або матеріалів для відновлення інфраструктури, скорочуючи час і витрати. У Німеччині системи штучного інтелекту зменшили споживання палива громадським транспортом на 8% [4].

Використання штучного інтелекту в поєднанні з дронами дозволяє здійснювати моніторинг стану об'єктів критичної інфраструктури. Алгоритми аналізують зображення, отримані з дронів, і виявляють пошкодження або критичні дефекти, що вимагають негайного ремонту та координують відновлювальні роботи, зменшуючи час простою.

Широке впровадження систем ШІ у різні сектори економікі має великий потенціал, однак їх високі енергетичні потреби ставлять під загрозу ці перспективи. Енергоспоживання ШІ-систем варіюється залежно від типу алгоритму, його структури та інфраструктури, на якій він працює. Основними споживачами енергії є процеси навчання нейронних мереж та їх використання для інференсу (виведення результатів). Інтенсивне енергоспоживання великих дата-центрів, які забезпечують роботу ШІ, створює значний попит на електричну енергію, що призводить до перевантаження регіональних енергетичних мереж. Основними чинниками високого енергоспоживання є: обчислювальна інтенсивність алгоритмів; великий обсяг даних для навчання та постійна робота дата-центрів з охолодженням [5].

Україна стикається із пошкодженнями енергетичної інфраструктури, що обмежує доступ до стабільного енергопостачання. Інтеграція енергоощадних технологій у ШІ-системи може стати ключовим елементом у збереженні енергетичних ресурсів для критично важливих секторів економики.

Одним із рішень оптимізації енергоспоживання систем ШІ є зменшення кількості параметрів моделі або використання компресії даних [6]. Компанії Google та OpenAI активно працюють над оптимізацією моделей, що дозволяє значно знизити споживання енергії без суттєвої втрати точності прогнозів або результатів [7]. Також сучасні енергоощадні процесори, такі як ARM або GPU останніх поколінь, дозволяють значно зменшити споживання енергії без втрати продуктивності [4].

Оптимізація енергоспоживання систем ШІ є важливим кроком до забезпечення резильєнтності критичної інфраструктури України. Застосування малопотужних моделей, сучасного апаратного забезпечення та хмарних обчислень сприятиме зменшенню енергетичних витрат і підвищенню ефективності.

Для успішної реалізації необхідно інтегрувати новітні енергоощадні технології у всі галузі, від енергетики до транспорту, а також забезпечити фінансову та технічну підтримку з боку держави й міжнародних партнерів.

1. Yang, S., Zhang, Z., & Liu, X. (2021). AI for sustainable development: Reducing the carbon footprint of intelligent systems. *Energy Policy*, 160, 112–126. https://doi.org/10.1016/j.enpol.2021.112126.
2. Gielen, D., Boshell, F., Saygin, D., Bazilian, M. D., Wagner, N., & Gorini, R. (2022). The role of renewable energy in the global energy transformation. *Renewable Energy*, 145, 1–12. https://doi.org/10.1016/j.renene.2022.01.101.
3. McKinsey & Company. (2020). *Artificial Intelligence in Energy Systems: New Frontiers and Opportunities.* mckinsey.com.
4. Google AI. (2023). *Energy-efficient AI solutions for sustainable development*. Retrieved from https://ai.google.
5. Strubell, E., Ganesh, A., & McCallum, A. (2020). Energy and policy considerations for deep learning in NLP. *Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics*, 3645–3650. https://doi.org/10.18653/v1/2020.acl-main.365.
6. Han, S., Mao, H., & Dally, W. J. (2015). Deep compression: Compressing deep neural networks with pruning, trained quantization, and Huffman coding. *arXiv preprint arXiv:1510.00149.* https://arxiv.org/abs/1510.00149.
7. OpenAI. (2023). *Environmental impact of large AI models*. Retrieved from https://openai.com.

О.А. Чемерис

ТЕХНІЧНІ МЕТОДИ ПОСИЛЕННЯ РЕЗИЛЬЄНТНОСТІ ЕНЕРГЕТИЧНИХ СИСТЕМ

Впровадження систем штучного інтелекту (ШІ) та автоматизації є ключовим фактором підвищення резильєнтності енергетичних систем [1]. Дослідження показують, що інтелектуальні системи здатні значно покращити стійкість енергетичної інфраструктури до різноманітних загроз. Резильєнтність енергетичних систем – це комплексна характеристика, що визначає здатність енергетичної системи протистояти екстремальним та неочікуваним порушенням, адаптуватися до змін, швидко відновлюватися після збоїв, підтримувати критично важливі функції навіть під час кризових ситуацій, ефективно використовувати наявні ресурси для продовження роботи.

Рисунок 1 – Методи посилення резильєнтності енергетичних систем

Поняття резильєнтності відрізняється від поняття надійності системи. Якщо надійність характеризує ймовірність безперебійної роботи системи в нормальних умовах, то резильєнтність описує здатність системи функціонувати та відновлюватися в умовах серйозних зовнішніх впливів та екстремальних ситуацій[2]. Резильєнтна енергетична система повинна мати такі ключові властивості, як робастність – здатність витримувати порушення; адаптивність – можливість пристосовуватися до змін; відновлюваність – спроможність повертатися до нормального функціонування; гнучкість – здатність працювати в різних режимах; надлишковість – наявність резервних потужностей та альтернативних шляхів енергопостачання, тощо [3].

На рис.1 наведено у графічному вигляді зв'язок між основними викликами для енергетичних систем та методами посилення резильєнтності, до яких відносяться технічні, організаційні та інноваційні підходи [4].Стаття спрямована на аналіз технічних методів посилення резильєнтності енергетичних систем.

В якості основних методів технічного підходу до підвищення резильєнтності можна віднести модернізацію мережевої інфраструктури,технічні рішення для захисту від загроз, системи накопичення енергії, адаптивне управління навантаженням, моніторинг та діагностика. Класифікація методів наведена на рис.2.

Використання елементів штучного інтелекту для даної проблеми є актуальним і перспективним [5]. Впровадження ШІ дозволяє оптимізувати процеси генерації, передачі та розподілу електроенергії, підвищити ефективність використання ресурсів та забезпечити надійність енергопостачання. Сучасні алгоритми машинного навчання та нейронні мережі відкривають нові можливості для розвитку розумних енергетичних систем.

Рисунок 2 – Класифікація технічних методів підвищення резильєнтності енергетичних систем

1. Jasiūnas, J., Lund, P. D., &Mikkola, J. (2021). Energy system resilience – A review. Renewable and Sustainable Energy Reviews, 150, 111476.
2. NREL. (2023). Generative Artificial Intelligence for the Power Grid. National Renewable Energy Laboratory.
3. European Commission. (2023). Digitalisation of the energy systems. Energy, Climatechange, Environment.
4. CISA. (2023). Resilient Power Best Practices for Critical Facilities and Sites. Cybersecurity and Infrastructure Security Agency.
5. IEEE. (2023). Artificial Intelligence/Machine Learning (AI/ML) for Power System Resilience. IEEE Power&Energy Society.

M.V. Prazian

THE FUTURE-PROOF ARTIFICIAL INTELLIGENCE (AI) AND THE RESILIENT DIGITAL AND ENERGY INFRASTRUCTURE NEXUS

About 8000 data centers are worldwide (33% - the USA, 16% - the EU, 10% - China). Between 2017 and 2021 (EPRI, 2024), electricity used by Meta, Amazon, Microsoft, and Google for data center cloud computing doubled. In the USA, data centers will consume up to 9.1% of electricity annually by 2030 versus about 4% in 2024. The total ICT energy consumption in the world can rise from 2-3% up to 16% for the next decades. The growth of data centers and the adoption of artificial intelligence (AI) rely on the availability of electric power. Opportunities for investors in power infrastructure and adjacent sectors are quickly arisen. Electricity operating expenditures comprise about 20 percent of the total cost base for data center business models, which have proved highly profitable for large companies. The US government (gov) currently classifies AI as a national security issue (House, 2024). It also addresses additional sensitive security issues, including countering adversary use of AI. The EU targeted 75% of European enterprises to leverage cloud computing, big data, and AI to drive innovation and efficiency by 2030 (The European Commission, 2023). In 2024, the UA gov and the Ministry of Digital Transformation issued the concept (КОНЦЕПЦІЯ Державної цільової науково-технічної програми з використання технологій штучного інтелекту в пріоритетних галузях економіки на період до 2026 року, 2024), the road map (Ministry of Digital Transformation in Ukraine, 2023), and the white paper (Ministry of Digital Transformation in Ukraine, 2024) about the AI future. The special focus is on the state AI program for 2024-26, including legislation. The World Bank survey has shown that the ICT-energy nodes represent one of the key risks during the war.

Technical and engineering aspects embody a gap in the UA gov documents. The war in Ukraine increased the attention on ensuring energy security, affordability, and achieving the Paris climate goals (Energy Institute, 2024). Intriguingly, the BP Institute put energy security and affordability before or in line with attaining Paris climate goals. Ukraine reflects general trends with the war specific: the frequent outages in conflict zones and beyond. Because energy management for ICT systems has been a relatively underexplored topic in cases of wars and disruptions, it prioritizes the topic of ICT infrastructure resiliency in the energy system nexus.

Future-proofed AI and stable generation should balance immediate resilient digital and energy infrastructure nexus needs with future-proof AI needs and long-term sustainability development goals (SDG). Or (McKinsey, 2024) how can data centers and the energy sector sate AI’s power hunger? The answer lies in assessing data center energy efficiency and how they use electricity (HAI Stanford, 2024). There are three data centers’ hardware facilities depending on the age, configuration, type, and function: 1. IT equipment (servers, storage, network infrastructure), typically composing 40%–50% of data center energy consumption; 2. Cooling systems (HVAC), typically composing 30%–40% of data center energy consumption;

3. Auxiliary components (uninterruptible power supplies, security systems, and lighting), typically composing 10%–30% of data center energy consumption.

Intermediate nexus. Due to the war, diesel generators, energy storage systems, fuel cells, and microgrids are the leading technologies for powering ICT. The three stages of resilience are (i) preparedness, (ii) response and relief, and (iii) recovery and reconstruction within the context of energy resilience and anti-crisis tools. For managing electricity demand, there are mainly three strategies to support data centers (Ana Cabrera-Tobar et al., 2023):

1. Energy efficiency and increased flexibility refer to cooling, water, and types of powering. 2. Close coordination, sometimes convergence, between data center developers and electric companies regarding power needs, decentralized grids, timing, operational and financial flexibility, and constraints. 3. Simulating sustainable and resilient tools to plan the investments for grids considering the interactions and interdependencies between ICT and power suppliers and communities. The author could add substation protection, implement the NFPA (National Fire Protection Association) standards, physical-cyber resiliency, mitigate the supply chain disruption. Cross-disciplinary elements (Mykhailo Prazian, 2024): environmental, social, and governance (ESG) regulations, financials, legals, and skills-set can be considered for the nexus better off.

Future-proof powering AI implies using the 'Power mix'**:** Nuclear track, renewable, oil, and gas. The professional community has witnessed big names such as Amazon, Google, Facebook, Microsoft, and others trying to establish direct lines with power companies, triggering a new era for nuclear energy, for example, with Three Mile Island (Microsoft). The Asia tech companies even considered coal a sustainable resource for AI powering. The top oil players, Exxcon-like, redirect their activism to forge new partnerships with tech giants. The big companies take this time as a big claim for the "AI cake or wedding." (Elliott, 2024). Soluna computing (Soluna, 2024) proposed building an integrated energy ecosystem by establishing renewable energy as a foundation supplemented by nuclear power. It maximizes efficiency through co-location strategies and cooperation between tech companies, energy providers, and policymakers within a framework without compromising safety or environmental protection.

Conclusions. Focusing on the immediate nexus and interdependency between digital and energy infrastructure is necessary, but more is needed. At the strategic level, government, business, and society should foresee the place and growth of AI and digital infrastructure in the economic landscape. Ukraine's acute deficit of electricity and power makes the object's nodes uneasy, but engineering and technological simulations of sustainable and resilient AI should be started without delay. The demand for power will emerge in the world (OECD, 2023). Stakeholders need to mitigate the risks of being behind the technological progress driven by AI. All types of energy mix should be considered for sustainable power production: nuclear, oil and gas, renewable, and others. Future-proofed AI physical-cyber resiliency should be reached with appropriate policies, organizational, and business models, including convergence between ICT and energy units, supply chain reconsidering, and coping with technical, financial, and labor resource deficits.

1. EPRI. (2024). *Powering Intelligence: Analyzing Artificial Intelligence and Data Center Energy Consumption* (ID 3002028905; p. 35). https://www.epri.com/research/products/3002028905.
2. House, T. W. (2024, October 24). *Memorandum on Advancing the United States' Leadership in Artificial Intelligence; Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence*. White House. https://www.whitehouse.gov/briefing-room/presidential-actions/2024/10/24/memorandum-on-advancing-the-united-states-leadership-in-artificial-intelligence-harnessing-artificial-intelligence-to-fulfill-national-security-objectives-and-fostering-the-safety-security/.
3. European Commission. (2023). *2030 Digital Compass: The European way for the Digital Decade*. https://eufordigital.eu/library/2030-digital-compass-the-european-way-for-the-digital-decade/.
4. КОНЦЕПЦІЯ Державної цільової науково-технічної програми з використання технологій штучного інтелекту в пріоритетних галузях економіки на період до 2026 року, № 320-р (2024). https://www.kmu.gov.ua/npas/pro-skhvalennia-kontseptsii-derzhavnoi-tsilovoi-naukovo-tekhnichnoi-prohramy-z-vykorystannia-s320130424.
5. Ministry of Digital Transformation in Ukraine. (2023). *Регулювання штучного інтелекту в Україні: Презентуємо дорожню карту*. MinDigit of Ukraine. https://thedigital.gov.ua/news/regulyuvannya-shtuchnogo-intelektu-v-ukraini-prezentuemo-dorozhnyu-kartu.
6. Ministry of Digital Transformation in Ukraine. (2024). *Біла книга з регулювання ШІ в Україні: Бачення Мінцифри*. MinDigit of Ukraine.
7. Energy Institute. (2024). *BP Energy Outlook 2024* [Review]. Energy Institute (EI). https://www.bp.com/en/global/corporate/energy-economics.html.
8. McKinsey. (2024). *Data centers and AI: How the energy sector can meet power demand | McKinsey*. https://www.mckinsey.com/industries/private-capital/our-insights/how-data-centers-and-the-energy-sector-can-sate-ais-hunger-for-power.
9. HAI Stanford. (2024). *AI Index Report 2024 – Artificial Intelligence Index*. Stanford University. https://aiindex.stanford.edu/report/.
10. Ana Cabrera-Tobar, Francesco Grimaccia, & Sonia Leva. (2023). *Energy Resilience in Telecommunication Networks: A Comprehensive Review of Strategies and Challenges*. https://doi.org/ 10.3390/en16186633.
11. Mykhailo Prazian. (2024). *Cross-disciplinary Cooperation for Digital Resilience* (E. Faure, Y. Tryus, T. Vartiainen, O. Danchenko, M. Bondarenko, C. Bazilo, & G. Zaspa, Eds.; pp. 42–52). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-71801-4_4.
12. Elliott, R. F. (2024, December 11). Exxon Plans to Sell Electricity to Data Centers. *The New York Times*. https://www.nytimes.com/2024/12/11/business/energy-environment/exxon-mobil-data-centers-power-plant.html.
13. Soluna. (2024). *Computational Power Redefined: AI in the Age of Renewable Energy | LinkedIn*. Soluna Resource Center. https://www.linkedin.com/pulse/computational-power-redefined-ai-age-renewable-energy-uqtoe/.
14. OECD. (2023). *A blueprint for building national compute capacity for artificial intelligence* (OECD Digital Economy Papers 350). OECD Publishing. https://www.oecd.org/en/publications/a-blueprint-for-building-national-compute-capacity-for-artificial-intelligence_876367e3-en.html.

A.A. Vladimirsky, I.A. Vladimirsky

SYNCHRONIZATION OF SPATIALLY DISTRIBUTED MEASUREMENTS

A method for synchronizing multichannel measurements on objects distributed in space is presented. The task of multichannel measurements and registration of various diagnostic information in the form of synchronous digital samples is typical for many diagnostic tasks.

We consider a system consisting of several local diagnostic information recorders, for example, from a group of acoustic or vibration sensors. Using subsequent cross-correlation processing of the recorded data, it is possible to determine the coordinates of various sources of acoustic noise and vibration.

The most important requirement for a recording system is to ensure synchronous recording of signal samples. Synchronization of measurements between signals connected to the same recorder is ensured with high accuracy by using the same electrical timing signal. To ensure synchronization of the recording of signal samples by different recorders, a wireless synchronization system is required.

The developed synchronization system has two levels of synchronization: coarse (about 1 second) and fine (no worse than 100 microseconds). All recorders have a radio receiver (for example, analog transceiver Kenwood TK-2206, 400-470 MHz). Radios are programmed for a specific frequency range and user group code. A separate starting (command) radio station operates on the same frequency range and transmits the user group code. This is a built-in feature of such radios.

Recorders begin recording signals from sensors after a signal from the starting radio station appears. Due to the variation in detector parameters, the variation in the start time of different recorder instances can reach 1 second. This is “rough” synchronization.

To reduce the error, the correlation method is used. The starting command radio transmits a reference analog noise-like signal of 200 – 4000 Hz for 10 seconds. This signal is received by recorders, digitized and recorded in output arrays along with signals from sensors.

The recorded arrays are saved in the recorders as files. During the subsequent joint processing of records from different recorders, the time shift of the original records is first determined from the reference noise signal received over the radio channel using cross-correlation processing, followed by compensation for the time shift between the signals from the sensors. It is practically confirmed that the error of “precise” synchronization does not exceed 100 μs.

The presented synchronization system is integrated at the hardware and software [1] levels into the RASTR system, which is designed for diagnosing long underground pipelines using correlation parametric methods [2].

The research was conducted within the framework of project 2023.04/0022, "Development of a Hardware-Software Complex and Methodology for Rapid Detection of Damages in Heating and Water Supply Systems Considering Their Wear

and Tear and Military Impacts," funded by the National Research Foundation of Ukraine (NRFU). The authors express their gratitude to the foundation for support in carrying out this work.

1. Владимирський ОА, Владимирський І.А., Артемчук В.О. Комп'ютерна програма «Багатоканальний реєстратор «Вібрологгер - 3.02» системи виявлення витоків підземних трубопроводів «РАСТР-2В». Заява ІПМЕ ім. Г.Є. Пухова НАН України про реєстрацію авторського права на твір № с202409803 від 02.12.2024р.
2. Vladimirsky A. A., Vladimirsky I. A. Correlation parametric methods for determining the coordinates of leaks in underground pipelines. Electronic modeling. 2021. Vol. 43, № 3. P. 03–16. URL: https://doi.org/10.15407/emodel.43.03.003 (date of access: 1.10.2024).

О.А. Владимирський, І.А. Владимирський

СУЧАСНИЙ СТАН ТА РОЗВИТОК ФІЛЬТРАЦІЇ СИГНАЛІВ ВИТОКІВ У КОРЕЛЯЦІЙНИХ ТЕЧЕШУКАЧАХ

Від частотного налаштування фільтрів у кореляційних течешукачах (КТ) суттєво залежить вказана координата витоку. Причиною цього є різноманітність за розмірами витоків, акустичних властивостей трубопроводів та сторонніх акустичних завад. Тому частотній фільтрації у КТ приділяється значна увага. У сучасних кореляційних течешукачах, крім ручного налаштування частотних фільтрів, розробники КТ розвивають напрям автоматичного налаштування частотних фільтрів. У Local 200 PC це функція comp, у TriCorr – функція AFIS, у інших КТ ця функція присутня без спеціальної назви. Крім того, такі КТ як MicroCorr Touch, AquaScan 610 мають можливість одночасного відображення декількох взаємних кореляційних функцій (ВКФ) з різним частотним налаштуванням фільтрів. Для налаштування у всіх КТ використовується й функція когерентності. Різноманітність підходів до настроювань фільтрів викликана наявністю невизначеності у цьому питанні. ІПМЕ ім. Г.Є. Пухова НАН України проведено відповідні дослідження. Отримані теоретичні результати вказують, що за допомогою "автоматів" з настроювання фільтрів, виразність ВКФ можна штучно максимізувати майже за бідь-якою координатою навіть без внесення у ВКФ фазових зсувів. У роботах [1, 2] це показано з класичних загальних позицій синтезу узгодженого та синтезу формуючого фільтрів. "Автомати" не є рішенням проблеми ще й тому, що крім витоку є корельовані завади від елеваторів, не до кінця закритих чи несправних засувок, протікаючих сальникових компенсаторів і т.п., які автоматичні алгоритми сприймають як шуканий прихований витік та хибно селектують. Є й інші причини недосконалості ідеї амплітудно-частотних "автоматів" [3]. Мабуть тому розробники КТ залишають у своїх приладах також трудомістке ручне налаштування фільтрів. Як компроміс, у MicroCorr Touch реалізована можливість відображати відразу три ВКФ у різних смугах частот, у AquaScan 610 – одночасно п'ять ВКФ, віддаючи оператору відповідальність за обрану координату витоку. Але по-перше, цих варіантів все одно замало. По-друге, потрібні додаткові, достовірні параметричні показники якості налаштування фільтрів для прийняття більш об'єктивних рішень про координату витоку. По-третє, дану проблему без додавання до частотної ще й просторової селекції корисних сигналів, яка дозволяє коректно виправляти не тільки амплітудний, але й фазовий спектр, компенсувати інтерференційні спотворення у реєстрованих сигналах витоків [4 - 8], не вирішити. Тому процедура частотного налаштування у відомих КТ залишається недосконалою. Такий стан суттєво обмежує ефективність застосування найчутливішого, кореляційного методу пошуку витоків, особливо при роботі в складних умовах зносу трубопроводів та міліарних пошкоджень. Тому авторами запропоновано інше рішення, а саме параметрична узгоджена просторово-частотна селекція шумів витоків. Це рішення використовує підхід,

який базується на параметричному просторово-частотному аналізі ВКФ та використовує собі на користь особливості доступу до вітчизняних трубопроводів у теплових мережах та водоканалах. Це дозволяє досягати більш якісних результатів при пошуку витоків [5 - 8].

Зазначений підхід розвивається далі при виконанні проекту 2023.04/0022 «Розроблення апаратно-програмного комплексу та методики оперативного виявлення пошкоджень систем тепло- та водопостачання з врахуванням їх зношеності та мілітарних впливів», що виконується за рахунок грантової підтримки Національного фонду досліджень України (НФДУ). Автори висловлюють подяку фонду за підтримку у проведенні цієї роботи.

1. Владимирский А. А., Владимирский И. А. О некоторых способах автоматической настройки фильтров в течеискателях корреляционного типа. *Збірник наукових праць ІПМЕ ім. Г. Є. Пухова НАН України.* 1998. Вип. 4. С. 179-188.
2. Владимирський О. А., Владимирський І. А., Семенюк Д.М. Алгоритми цифрової обробки кореляційних функцій у течешукачах // Електронне моделювання, 2024, 46 (2). С.60 —74.
3. Владимирский А. А., Владимирский И. А., Семенюк Д. Н. Уточнение диагностической модели трубопровода для повышения достоверности течеискания. Акустичний вісник Інституту гідромеханіки НАН України. 2005. 3 (8). С. 3-16.
4. Владимирський О.А. Параметричні методи діагностування підземних трубопроводів з урахуванням багатохвильового поширення інформаційних сигналів // Електронне моделювання, 2019. 41 (1). С. 3-17.
5. Владимирський О.А., Владимирський І.А. Кореляційні параметричні методи визначення координат витоків підземних трубопроводів // Електронне моделювання, 2021, 43 **(**3). С. 3—17.
6. Владимирський О.А., Владимирський І.А. Просторовий і частотний кореляційні параметричні методи визначення координат витоків підземних трубопроводів // Електронне моделювання, 2021, 43 (4). С.22 —36.
7. Патент на корисну модель № 149956. Владимирський О.А., Владимирський І.А. Параметричний кореляційний спосіб визначення координат пошкоджень трубопроводів. Публікація відомостей 15.12.2021р, Бюл. №50.
8. Патент на корисну модель № 144444. Владимирський О.А., Владимирський І.А. Параметричний кореляційний спосіб визначення координат витоків трубопроводів. Публікація відомостей 25.09.2020, Бюл. №18.

О.А. Владимирський, І.А. Владимирський

РОЗВИТОК ІНСТРУМЕНТАЛЬНОЇ ОЦІНКИ ПАРАМЕТРІВ РЕСУРСУ ДІЛЯНОК ПІДЗЕМНИХ ТРУБОПРОВОДІВ

Оцінка залишкового ресурсу, залишкової міцності та довговічності підземних нафтопроводів, продуктопроводів, газопроводів, трубопроводів тепло і водопостачання, промислових та станційних трубопроводів ТЕЦ, АЕС та ін. є актуальною технічною задачею. Від якості її вирішення залежить своєчасність ремонтів та оновлень ділянок трубопроводів, безаварійність та безпека їхньої поточної та майбутньої експлуатації. Рішення про строки цієї експлуатації приймається на основі результатів інструментального обстеження трубопроводів. Наряду з іншими показниками якості металевої стінки трубопроводу витримувати задані навантаження, широко використовується показник її середньої товщини $S_{ср}$ [1]. Є різні варіації застосування $S_{ср}$ [1, 2]. Ідея оцінки залишкового ресурсу виглядає так:

- Обчислюється швидкість корозії $v_{кор}$:

$$v_{кор} = \frac{S_0 - S_{ср}}{T_{експ}}$$

де S_0 - товщина стінки трубопроводу за його паспортними даними на момент його прокладання; $T_{експ}$ - час експлуатації трубопроводу, який минув до моменту виміру $S_{ср}$;

- Обчислюється залишковий ресурс $T_{рес}$:

$$T_{рес} == \frac{S_{ср} - S_{\min}}{v_{кор}}$$

де $S_{\min}$ - мінімальна дозвільна товщина ділянки трубопроводу виходячи з надлишкового тиску у трубопроводі за результатами його розрахунків на міцність.

Для застосування зазначеного поширеного підходу потрібно мати виміряну товщину $S_{ср}$. Звичайно цю товщину приймають як осереднене значення результатів ультразвукової товщинометрії стінки трубопроводу у шурфах. Недоліком цього є просторова обмеженість виміряного фрагменту трубопроводу. Для оцінки $S_{ср}$ ділянок протяжністю десятки і сотні метрів між наявними місцями доступу до трубопроводу можна застосувати непрямий метод оцінки $S_{ср}$. Наприклад, з застосуванням формули для швидкості гідравлічного удару

М.Є.Жуковського [3], якщо її переписати відносно шуканої товщини стінки d як оцінки S_{cp}:

$$d = \frac{D \cdot \mu}{E \cdot \left[\left(\frac{V_S}{V} \right)^2 - 1 \right]} \quad (1)$$

де V_S – швидкість звуку у воді; V – швидкість поширення хвиль гідравлічного удару; D – діаметр трубопроводу; μ – модуль пружності рідини; Е – модуль Юнга для металу стінки трубопроводу.

Параметром, який потребує вимірювання в (1), є швидкість поширення хвиль гідравлічного удару V вздовж діагностованої ділянки трубопроводу. Але достатньо точне вимірювання V є не простою вимірювальною задачею. Бо у трубопроводі потрібно створити відповідні зондувальні акустичні хвилі, бажано у експлуатаційному режимі трубопроводу, та врахувати акустичні особливості їхньої реєстрації під час зондування. Це в першу чергу багато хвильове поширення зондувальних сигналів, відбиття та інтерференційні спотворення сигналів, які виникають при їхньої реєстрації. Для цього в ІПМЕ ім. Г.Є. Пухова створено кореляційний параметричний метод визначення фактичної швидкості хвиль гідравлічного удару [4, 5], який основано на узгодженій просторово-частотній параметричній селекції відповідних хвиль [6, 7].

1. ДСТУ 4046-2001 Державний стандарт України. Обладнання технологічне, нафтопереробних, нафтохімічних та хімічних виробництв. Технічне діагностування. Загальні технічні вимоги. Київ.Держстандарт України.2001р.
2. Азаров В.Н., Гевлич С.О. та ін.. К расчету остаточного ресурса труб тепловых сетей и сетей горячего водоснабжения. URL: https://science-education.ru/ru/article/view?id=16169.
3. Н.Е. Жуковский. О гидравлическом ударе в водопроводных трубах. Собр. соч. М.: Гостехиздат, 1948. Т. 2. 422 с.
4. A.A. Vladimirsky, I.A. Vladimirsky. Correlation parametric method for determining the velocity of acoustic wave propagation in a pipeline. Electronic Modeling, 2024, V46, № 6.
5. Владимирський О.А., Владимирський І.А. Параметричний кореляційний спосіб визначення фактичного значення швидкості поширення акустичних хвиль гідравлічного удару по трубопроводу. Заявка ІПМЕ ім. Г.Є. Пухова НАН України на корисну модель u202405043 від 25.10.2024 р.
6. Владимирський О.А., Владимирський І.А. Кореляційні параметричні методи визначення координат витоків підземних трубопроводів // Електронне моделювання, 2021, 43, № 3, с. 3—17.
7. Патент на корисну модель № 144444. Владимирський О.А., Владимирський І.А. Параметричний кореляційний спосіб визначення координат витоків трубопроводів. Публікація відомостей 25.09.2020, Бюл. №18.

М.С. Кондратенко, Л.М. Ковальчук

КРИПТОГРАФІЧНА СТІЙКІСТЬ ХЕШ-ФУНКЦІЙ У СВІТІ КВАНТОВИХ ОБЧИСЛЕНЬ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ

Завдяки розвитку квантових комп'ютерів криптографія зіштовхується з потенційними загрозами, які можуть поставити під загрозу шифрування як технологію. Особливої уваги потребують хеш-функції як ключовий елемент цифрової безпеки. Хеш-функції широко використовуються для генерування підписів, аутентифікації даних та забезпечення цілісності цифрової інформації. Ключовими вимогами до хеш-функцій є стійкість до зіткнень (колізій) та перетворення оригінальних даних. Найчастіше для такий цілей використовуються функції з сімейств SHA (наприклад, SHA-256 або SHA-3), які до недавнього часу вважалися надійними. Хешування відноситься до процесу генерації результату фіксованого розміру із вхідних даних змінного розміру. Це робиться за допомогою математичних формул, відомих як алгоритми хешування. Хоча не всі хеш-функції включають використання криптографії, так звані криптографічні хеш-функції лежать в основі криптовалют. Завдяки їм блокчейни та інші розподілені системи можуть досягати значних рівнів цілісності та безпеки даних.

Справжня сила хешування проявляється під час роботи з величезними обсягами інформації. Наприклад, можна запустити великий файл або набір даних через хеш-функцію, а потім використовувати його виходи для швидкої перевірки точності та цілісності даних. Це можливо завдяки детермінованому характеру хеш-функцій: вхід завжди призводить до спрощеного, стисненого виходу (хешу). Такий метод позбавляє необхідності зберігати та "запам'ятовувати" великі обсяги даних. Загалом, злом криптографічної хеш-функції вимагає безліч спроб грубого підбору чисел. Щоб "розвернути" криптографічну хеш-функцію, потрібно підбирати входи методом спроб і помилок, доки не буде отримано відповідного виходу. Однак існує також ймовірність того, що різні входи будуть давати той самий результат, і в цьому випадку відбудеться "колізія". Технічно криптографічна хеш-функція повинна відповідати трьом властивостям, щоб вважатися надійно захищеною. Ми можемо описати їх як: стійкість до колізії, та стійкість до атаки знаходження першого і другого прототипу.

- **Стійкість до колізії:** неможливість знаходження двох різних входів, які утворюють однаковий хеш.
- **Стійкість до знаходження першого прототипу**: відсутність можливості "розвороту" хеш-функції (знаходження вхідних даних через заданий хеш).
- **Стійкість до знаходження другого прототипу**: відсутність можливості знайти будь-який другий “вхід”, який би мав такий самий хеш, що і перший. [1]

У класичних комп'ютерах біт використовується для представлення інформації, і він може мати стан 0 або 1. Квантові комп'ютери працюють із квантовими бітами або кубітами. Кубіт – це основна одиниця інформації у квантовому комп'ютері. Як і біт, кубіт може бути в стані 0 або 1. Однак, завдяки особливості квантово-механічних явищ, стан кубіту може бути і 0, і 1 одночасно. Це стимулювало дослідження та розробки в галузі квантових обчислень. Університети та приватні компанії вкладають час та гроші у вивчення цієї захоплюючої нової області. Вирішення абстрактної теорії та практичних інженерних завдань, які представляє ця область, знаходяться на передовій технологічних досягнень людства. На жаль, побічним ефектом цих квантових комп'ютерів буде те, що алгоритми, що лежать в основі асиметричної криптографії, стануть простими для вирішення, докорінно руйнуючи системи, які на них покладаються. Розглянемо приклад злому 4-бітного ключа. Теоретично 4-кубітний комп'ютер зможе приймати всі 16 станів (комбінацій) одночасно в рамках одного обчислювального завдання. В такому випадку, ймовірність знаходження правильного ключа становитиме 100% під час цих обчислень. [2]

Компанія Google нещодавно представила свій квантовий комп'ютерний чіп Willow, який може вирішувати обчислювальні проблеми майже в 1025 разів швидше, ніж найсучасніші суперкомп'ютери. Це спричинило обговорення в біткоін-спільноті, яка покладається на розв'язання математичних задач для отримання монет (процес майнінгу). Експерти, однак, стверджують, що поточна загроза для криптосвіту є незначною, незважаючи на те, що технологія дійсно є революційною. Willow, продукт Google, ще не досяг цього етапу. Однак, рівні помилок та масштабованість є серед перешкод, з якими стикаються сучасні квантові комп'ютери, такі як Willow. Для того, щоб мережа BTC стала вразливою до атак з використанням квантового комп'ютера, знадобиться мільйони виправлених помилок "логічних кубітів", що значно перевищує 105 фізичних кубітів Willow. Віталій Бутерін, співзасновник Ethereum, гордиться технологією, на якій він побудував екосистему ETH. Він долучився до дискусії, сказавши: "Ethereum готовий, навіть якщо квантові комп'ютери з'являться завтра."

Аналізуючи потенційні загрози, можна виокремити наступні перспективи захисту для існуючих хеш-функцій:

1. **Постквантові хеш-функції**. Розробка нових хеш-алгоритмів, що стійкі до атак за допомогою алгоритмів Гровера [3], стає основним пріоритетом у криптографії.
2. **Збільшення розміру хешів**. Більші хеши ускладнюють злом, оскільки підвищують кількість можливих значень.
3. **Альтернативні підходи**. Дослідження заміни класичних алгоритмів хешування на принципово нові математичні моделі, які враховують можливості квантових обчислень, стають перспективним напрямком. Зокрема, такі моделі можуть базуватися на теорії решіток або кодах

виправлення помилок, які демонструють підвищену стійкість до квантових атак.

4. **Гібридні системи захисту**. Поєднання традиційних хеш-функцій із постквантовими технологіями може слугувати тимчасовим рішенням до повного переходу на нові стандарти криптографії.

Через величезні ставки, пов'язані з інформаційною безпекою, розумно почати закладати основу проти майбутнього вектора атаки. На щастя, проводиться велика кількість досліджень потенційних рішень, які можна було б впровадити в існуючі системи. Теоретично, ці рішення захистять нашу критичну інфраструктуру від загрози квантових комп'ютерів. Квантово-стійкі стандарти можуть бути поширені серед широкої спільноти так само, як і наскрізне шифрування за допомогою добре відомих браузерів і додатків для обміну повідомленнями. Як тільки ці стандарти будуть допрацьовані, криптовалютна екосистема зможе легко інтегрувати максимально надійний захист від цих векторів атак.

1. Що таке хешування? Binance Academy. https://academy.binance.com/uk/articles/what-is-hashing.
2. Квантові комп'ютери та криптовалюти. Binance Academy. https://academy.binance.com/uk/articles/quantum-computers-and-cryptocurrencies.
3. Алгоритм Ґровера. Вікіпедія. https://uk.wikipedia.org/wiki/Алгоритм_Ґровера.

І.В. Плетяний

РОЗВИТОК КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ ТРЕНАЖЕРНОЇ ПІДГОТОВКИ ПЕРСОНАЛУ ДЛЯ ЗАБЕЗПЕЧЕННЯ РЕЗИЛЬЄНТНОСТІ ЕНЕРГЕТИЧНИХ СИСТЕМ

Тренажерна підготовка персоналу в енергетиці відіграє важливу роль і впливає на рівень безпечної експлуатації енергетичного обладнання. Значення тренажерної підготовки під час дії режиму воєнного часу і в умовах значних руйнувань енергетичної інфраструктури України важко переоцінити. Для ефективного відновлення (набуття) професійної підготовленості кадрового резерву оперативно-диспетчерського персоналу, а також для подолання дефіциту кваліфікованого інструкторського персоналу в енергетиці необхідно забезпечити можливість масового випуску комп'ютерних тренажерів з автоматичним оцінюванням операторської діяльності. Рішенням даної проблеми є розвиток комп'ютерних технологій побудови динамічних тренажерів в напрямку більшого спрощення та орієнтації методів і засобів імітаційного моделювання енергетичного обладнання на досвідчених галузевих експертів.

Якщо проводити короткий ретроспективний огляд і аналіз методів, принципів і технологій розробки і побудови тренажерів для підготовки операторів енергетичного обладнання в енергетиці, то можна виділити декілька періодів розвитку відповідних технологій. Першими і найбільш розповсюдженими технологіями побудови динамічних тренажерів для енергетики можна вважати технології 90-х, які реалізують принцип «від моделі об'єкта до організації навчальної діяльності» (рис. 1).

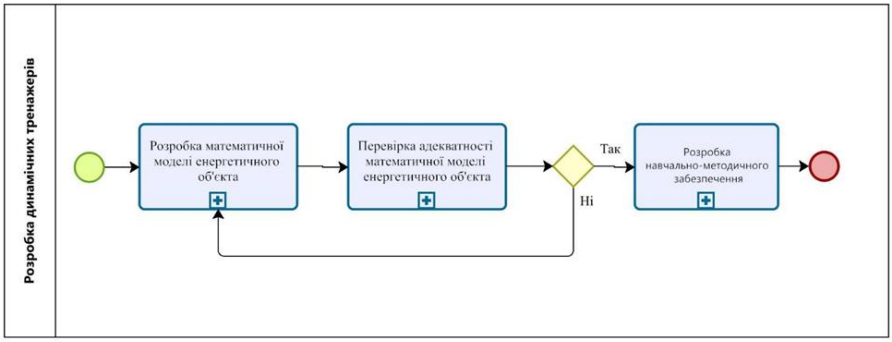


Рисунок 1 – Традиційна технологія розробки динамічних тренажерів

Найяскравішим прикладом такої технології є розробка повномасштабних тренажерів енергоблоків АЕС, які створені американськими компаніями і встановлені на кожній АЕС України. До такої технології також можна віднести розробку комплексу локальних тренажерів «Клотик» для підготовки операторів

АЕС [1], встановленого на Хмельницькій АЕС у 90-х роках, та деякі локальні тренажери на Запорізькій АЕС (локальні тренажери: газового посту генератора, електролізної установки, щита постійного струму, а також локальний тренажер для підготовки операторів хімічного цеху АЕС), які розроблялись і були встановлені у 2000-х роках. Основою технології є розробка складної математичної моделі енергетичного об'єкта. Це тривалий і досить складний та високовартісний процес, до якого залучені багато різноманітних фахівців – інженерів з відповідною технологічною освітою, математиків, програмістів, досвідчених експертів з експлуатації, педагогів та ін. Також, дуже складним етапом технології є досягнення адекватності функціонування математичної моделі. Досяжність необхідних рівнів адекватності моделі встановлюється певним методиками та експертними висновками досвідчених галузевих фахівців з експлуатації.

Після розробки математичної моделі та досягнення прийнятного рівня адекватності наступає етап розробки навчально-методичного забезпечення, тобто проектується та налагоджується організація навчальної діяльності на тренажері. Під керівництвом досвідчених експертів з педагогіки та у взаємодії з вище переліченими фахівцями, причетними до попередніх етапів, розробляється визначений базовий перелік тренажерних занять, при виконанні яких реалізуються навчальні цілі тренажера. Кожне тренажерне заняття має початковий і кінцевий стани математичної моделі і відповідно енергетичного обладнання яке моделюється. Завданням оператора на тренажері є його професійна діяльність у процесі виконання тренажерного заняття, тобто в русі від початкового стану до кінцевого стану і уникненні створення аварійної ситуації на протязі відведеного часу. Перевірка та оцінка дій оператора здійснюється інструктором тренажера після закінчення тренажерного заняття. Метод оцінки – розбір і аналіз відповідного протоколу тренажерного заняття.

Наступним еволюційним кроком розвитку технологій побудови динамічних тренажерів для енергетики, на наш погляд, є поява і розвиток технологій, які реалізують принцип «від навчальної діяльності до імітаційної моделі об'єкта» (рис. 2). Яскравими тренажерами, які реалізовані за даною технологією є ряд тренажерів, створених компанією «АСОТ» і впроваджених на деяких вітчизняних електростанціях і мережевих компаніях [2]. Дослідження щодо створення методології розробки тренажерів для енергетики проводились в рамках науково-дослідних робіт в ІПМЕ ім. Г.Є. Пухова НАН України [3]. Результати досліджень були впроваджені і реалізовані під час розробки тренажерів для підготовки операторів АЕС.

Початок проектування тренажера в рамках даної технології полягає в формуванні списку тренажерних занять, в рамках яких буде розроблятись відповідна математична (імітаційна) модель. Кожне тренажерне заняття має відповідний сценарій де розписано початковий стан обладнання, задана мета діяльності оператора, представлено саму діяльність оператора щодо управління

обладнанням у вигляді BPMN діаграми. Обсяг і глибина моделювання обмежена сценарієм тренажерного заняття.

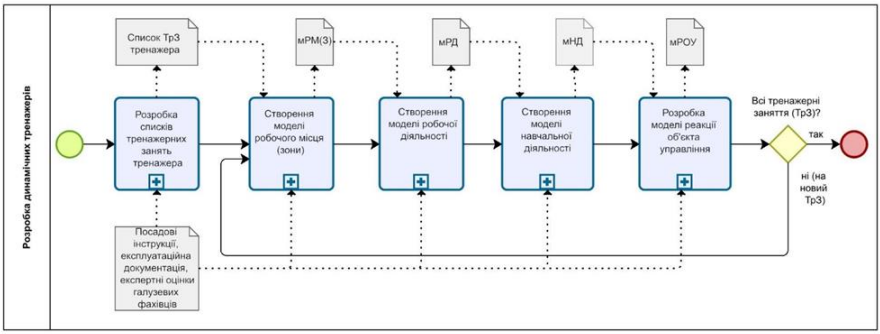


Рисунок 2 – Технологія розробки тренажерів, яка реалізує принцип «від навчальної діяльності до імітаційної моделі об’єкта»

В таких тренажерних системах замість однієї повномасштабної моделі використовується сукупність значно менш складних моделей, кожна з яких відображує роботу в рамках окремих тренажерних занять, а функціонування яких визначається експлуатаційними документами вказаними в посадових інструкціях персоналу. З економічної точки зору менш витратною є розробка тренажерів, на основі тренажерних занять.

При такому підході можливо забезпечити залучення до проектування та побудови тренажерів широкого кола фахівців галузі, добре обізнаних з технологічними процесами на об’єкті, без залучення спеціалістів-програмістів з мінімальними фінансовими витратами та у короткі терміни при умові наявності відповідного спеціалізованого програмно-технологічного забезпечення. Прикладами такого спеціалізованого програмно-технологічного забезпечення є автоматизовані системи для побудови динамічних тренажерів 90-х років САПДИТ [4,5] та ITS [6]. В подальшому, створення, підтримка і супроводження відповідних автоматизованих систем стало економічно не доцільним. Розвиток отримали технології побудови тренажерів, які мали реалізацію у вигляді спеціалізованих авторських підсистем універсальних програмних пакетів світового рівня. Таким програмним пакетом, у свій час, слугував Adobe Flash Professional. На теперішній час, найбільш сучасною програмною системою для реалізації технології конструювання динамічних тренажерів для підготовки персоналу в енергетиці використовується Unity.

Основним недоліком технології розробки тренажерів, яка реалізує принцип «від навчальної діяльності до імітаційної моделі об’єкта» залишається її складність для освоєння і специфічна термінологія.

Наступним еволюційним кроком в розвитку технологій побудови комп’ютерних тренажерів для підготовки персоналу в енергетиці в напрямку

більшого спрощення та орієнтації методів і засобів імітаційного моделювання енергетичного обладнання на досвідчених галузевих експертів має стати новітня технологія побудови динамічних тренажерів на основі моделювання діяльності і відповідної реакції обладнання на діяльність (рис. 3) [7].

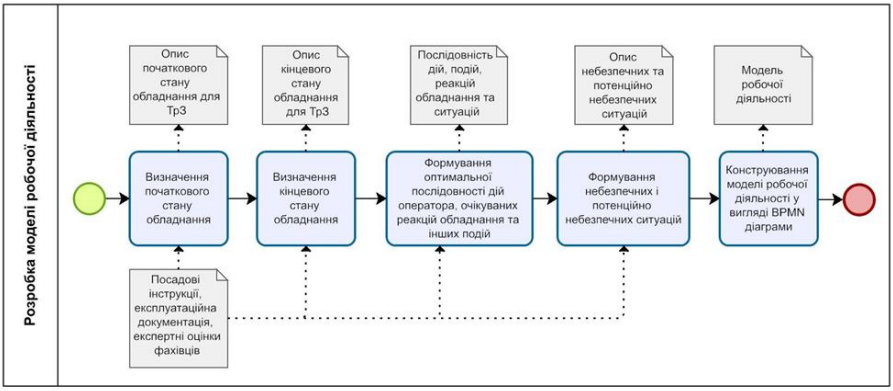


Рисунок 3 – Технологія розробки динамічних тренажерів на основі моделювання діяльності і відповідної реакції на діяльність

Суть технології полягає у пріоритетності моделювання діяльності персоналу яка стає базою для конструювання сценарію тренажерного заняття. Імітаційному моделюванню підлягають лише відповідні реакції енергетичного обладнання на діяльність персоналу що значно спрощує вибір методів математичного моделювання. Таким чином максимально досягається мета тренажерної підготовки персоналу за рахунок значного спрощення математичної моделі енергетичного обладнання. Також при такому підході стає можливим впровадити повністю автоматичну оцінку навчальної діяльності персоналу на тренажері.

Опис робочої діяльності доцільно виконувати за допомогою міжнародного стандарту BPMN. Стандарт є системою умовних позначень (нотацій) для моделювання бізнес – процесів, до яких також належить робоча діяльність персоналу підприємств в енергетиці. Робоча діяльність – це набір активних (вплив на моторні елементи управління, віддача розпоряджень та приймання доповідей) та пасивних дій (спостереження та аналіз інформації). Модель та графічна нотація робочої діяльності представляється у вигляді діаграми. Така діаграма базується на представлені робочого процесу у вигляді блок – схеми, яка семантично схожа на діаграму діяльності. При чому єдина модель робочої діяльності повинна бути зрозумілою для всіх користувачів.

1. Плетяняий І.В., Черьомухін Ю.Д., Воробйов О.С., Волощенко В.К., Зенов В.М. Комплексний тренажер для підготовки оперативного персоналу електроцеха АЕС//Енергетика та електрифікація, №6, 1996, С.23-24.

2. Абрамович Р.П. Досвід розробки тренажера віртуальної реальності для персоналу енергопідприємств // Збірник матеріалів науково-практичної конференції «Технології створення і використання засобів підготовки персоналу на об'єктах критичної інфраструктури – 2023», м. Київ, 8 листопада 2023 р., ІПМЕ ім. Г.Є. Пухова НАН України. – 2023. – 51 с.
3. Абрамович Р.П., Самойлов В.Д. Технології конструювання комп'ютерних систем підготовки персоналу в енергетиці // К.: «Три К», 2021. – 111 с. (ISBN 978-966-7690-58-8).
4. Березников В.П., Писаренко А.П., Самойлов В.Д., Сметана С.И. Автоматизация построения тренажеров и обучающих систем. Киев, Наукова Думка, 1989.
5. Писаренко А.П., Самойлов В.Д., Стеценко О.Я. Компьютерные технологии моделирования для динамических тренажеров. Киев, Наукова думка, 1992.
6. Плетяний І.В. Методика оцінки і вибору автоматизованої технології побудови тренажерів //Електронне моделювання, Т.20, №2, 1998, С.91-99.
7. Плетяний І.В., Самойлов В.Д., Чьочь В.В. Проєктування локальних тренажерів на основі сценарно-імітаційного моделювання // «Ядерна та радіаційна безпека», №4(100) (2023). ISSN (print) 2073-6231. DOI:10.32918/nrs.2023.4(100).05.

Т.О. Білобородова

ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ ГЕНЕРАЦІЇ ЕНЕРГІЇ СОНЦЯ ТА ВІТРУ В УКРАЇНІ

Більша частина електроенергії, що генерувалась в Україні з 1991 по 2023 роки, генерувалась на основі ядерної енергетики та викопного пального, такого як вугілля, газ, нафта. З 2022 року російські атаки на енергетичну інфраструктуру України спрямовані на дестабілізацію електроенергетичної системи шляхом відключення великих вугільних та газових установок, що генерують, і ключових частин мережі передачі. Внаслідок цих цілеспрямованих атак до літа 2024 року потужність енергетичної системи України скоротилася до приблизно третини її довоєнної потужності.

З моменту вторгнення 2022 року споживання електроенергії в промисловості скоротилося вдвічі, і на даний момент споживання електроенергії домогосподарствами становить найбільшу частку загального попиту, незважаючи на те, що воно також скоротилося на 20%. Однак, незважаючи на скорочення споживання, Україна зіткнулася з гострим дефіцитом електроенергії в літні місяці 2024 року, коли її генеруючі потужності впали на 2,3 ГВт нижче пікового попиту в 12 ГВт, незважаючи на імпорт електроенергії із західних сусідів України. Протягом червня та липня, навіть з урахуванням імпорту електроенергії, передбачуваний розрив між попитом та пропозицією становив від 0,8 ГВт до 2,3 ГВт [1]. Це призвело до відключень електроенергії по всій країні, що обмежило доступність об'єктів, які залежать від електроенергії, зокрема й життєво необхідного водопостачання.

Потреби енергетичної безпеки обумовлюють необхідність більш децентралізованої генерації енергії. Використання відновлюваних джерел енергії, таких як сонячна фотоелектрична енергія та вітер, поряд з традиційними джерелами, дозволить розподілити джерела енергії, підвищити стійкість, знизити енергетичну залежність енергосистем від викопного пального та ядерної енергетики [2, 3]. Однак, генерація енергії на основі сонця та вітру має, деякі обмеження, серед яких визначають [4] високу залежність від погодних умов, рельєфу, та неможливість генерації енергії сонячними панелями в нічний час доби. Зважаючи на ці обмеження, доцільне дослідження особливостей генерації енергії джерелами на основі сонця та вітру в контексті розподілення генерації протягом доби, що специфічні саме для України, яке дозволить визначити можливості їх використання для підвищення стійкості генерації.

Україна розташована у двох кліматичних зонах – помірній та середземноморській. Кількість годин сонячного світла на рік коливається від 1700 на півночі до понад 2400 на півдні. Найвища хмарність спостерігається у грудні, січні та лютому. З іншого боку, взимку над Україною розвивається циклонічна діяльність, повітряні маси часто змінюються, що відкриває можливості для генерації енергії на основі енергії вітру.

Можливості генерації електроенергії на основі сонячної енергії визначено на основі усередненої погодинної генерації сонячної енергії для 50.45° N широти та 30.54° E, що відповідає розташуванню Києва, та з наступними характеристиками фотоелектричної (PV) системи: потужність постійного струму системи 4 kW, панелі стандартного типу нерухомої системи, з втратами 14.08%, нахилом масиву 20°, азимутом масиву 180°, коефіцієнтом співвідношення постійного та змінного струму 1.2, ефективністю інвертора96% та коефіцієнтом покриття землі 0.4, проведено з використанням даних [5] для розрахунку показнику вихідної потужності системи змінного струму (AC) протягом доби на основі показнику глобального сонячного опромінення в Україні та зазначених параметрів PV системи наступним чином. На основі даних сонячної опроміненості [5], з урахуванням опроміненості променя, дифузної та відбитої опроміненостей на нахиленій площині, втрат PV системи вихідного сигналу постійного струму та розміру PV системи, з поправкою на коефіцієнт співвідношення постійного та змінного струму розраховано показник вихідної енергії системи змінного струму, що є вихідною енергією змінного струму (AC) після перетворення та представляє собою корисну електроенергію.

Особливості генерації в залежності від місяця року представлені нижче на рис. 1.

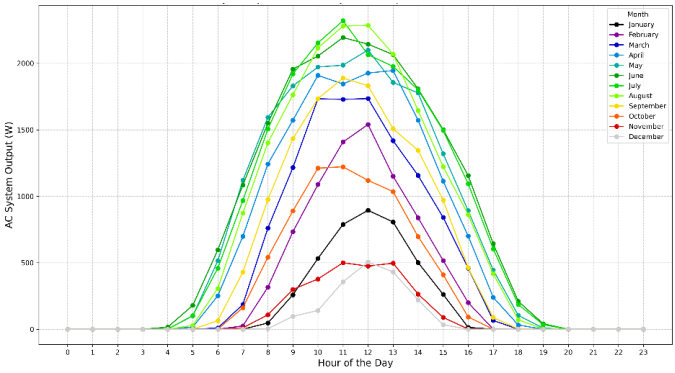


Рисунок 1 – Особливості генерації енергії сонця протягом доби в залежності від місяця року

Пік генерації енергії на основі сонця для всіх місяців приходиться на середину світового дня, з десятої до тринадцятої години. Очевидно, що в літні місяці можливість генерація починається раніше та закінчується пізніше. Найменші можливості генерації має листопад та грудень, найвищі липень та серпень.

Можливості генерації енергії на основі вітру напряму залежать від швидкості вітру. Швидкість вітру є одним із найважливіших факторів у визначенні потенціалу виробництва вітрової енергії. Аналіз можливої

усередненої погодинної генерації енергії вітру в Україні проведено з використанням даних [6] на основі показника швидкості вітру в Україні. Швидкість вітру в контексті особливостей вітрової генерації визначається як cut-in, номінальна та cut-out швидкості. Cut-in швидкість є мінімальною швидкістю вітру, при якій вітрогенератор починає виробляти електроенергію (3–4 м/с). Номінальна швидкість є швидкість вітру, при якій турбіна виробляє максимальну потужність (12–15 м/с). Cut-out швидкість є максимальною швидкістю вітру, при якій турбіна вимикається, щоб запобігти пошкодженню (25–30 м/с). Швидкість вітру в Україні залежить від часу доби, знижуючись ввечорі та починаючи зростати о четвертій ранку. Середня швидкість вітру протягом доби не перевищує номінальну швидкість, що не дозволяє отримати максимальну ефективність енергогенерації. Також, необхідно приймати до уваги, що швидкість вітру коливається в залежності від регіону. Найбільш ефективними з боку вітрової енергогенерації в Україні є Одеська, Донецька області з швидкістю вітру 5,5 – 6,5 м/с та Карпати з 6 – 7 м/с.

Об'єм енергії, що генерується вітрогенераторами розраховується на основі щільності повітря, площі лопатей вітрової турбіни та швидкості вітру, маючи залежність від атмосферних умов, температури повітря та атмосферного тиску. Властивості вітрової турбіни визначені відповідно до даних Української вітроенергетичної асоціації про використовувані в Україні турбіни [7].

Тенденції розрахованої середньої годинної енергії, що виробляється вітрогенератором, протягом дня по місяцях у відповідності до середньої cut-in швидкості вітру, що є вищою за 3 м/с, представлені на рис. 2.

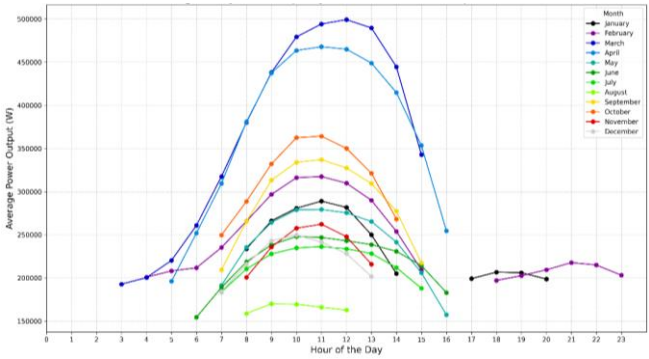


Рисунок 2 – Особливості генерації енергії вітру протягом доби в залежності від місяця року

Генерація вітру демонструє великий розкид в кількості генерованої енергії протягом доби в залежності від місяця року. Найнижчій рівень генерації потенційно в серпні, а найвищий в березні, квітні.

Порівняння можливостей генерації на основі енергії сонця, що у січні, лютому, наприклад, вже недоступні після сімнадцятої години, з можливостями

генерації на основі вітру, що у січні демонструє спроможність до генерації до двадцятої години, а у лютому до двадцять третьої години, підтверджує доцільність використання комбінації цих джерел генерації для балансування генерації протягом доби впродовж року що, таким чином, дозволить підвищити стійкість енергопостачання при використанні відновлюваних джерел генерації.

Дослідження особливостей генерації енергії сонця та вітру в Україні показало, що деякі денні години, що варіюються в залежності від пори роки, та нічні години з двадцять третьої години до, як мінімум, четвертої ранку залишаються непокритими генеруючими можливостями джерел генерації на основі сонця та вітру. Це обумовлює необхідність використання системи накопичення енергії (англ. energy storage system, ESS) поряд з відновлюваними джерелами енергії. ESS зберігають надлишкову енергію, коли генерація перевищує попит, і додають енергію, коли генерація менша за попит [8].

1. International Energy Agency. (2024) *Ukraine's Energy Security and the Coming Winter. An energy action plan for Ukraine and its partners*. https://iea.blob.core.windows.net/assets/cec49dc2-7d04-442f-92aa-54c18e6f51d6/UkrainesEnergySecurityandtheComingWinter.pdf.
2. Katalenich, S.M., Jacobson, M.Z. (2023). Renewable energy and energy storage to offset diesel generators at expeditionary contingency bases. *The Journal of Defense Modeling and Simulation*, 20(2), 213-228.
3. Mori, M., Baškovič, U.Ž., Katrašnik, T., Šipec, R., Drobnič, B. (2023). Securing Autonomy of Military Barracks Through Renewable Energy Solutions. *Contemporary military challenges*, 25(3-4), 87-109.
4. Zhang, S., Wie, Y., Guo, X., Li Z., Song, X., Blaabjerg, F. (2023). Overview of US patents for energy management of renewable energy systems with hydrogen. *International Journal of Hydrogen Energy*, 48(26), 9574-9591.
5. PVWatts® Calculator. *Solar resource data*. https://pvwatts.nrel.gov/pvwatts.php
6. Sengupta, M., Xie, Y., Lopez, A., Habte, A., Maclaurin, G. and Shelby, J. (2018). The national solar radiation data base (NSRDB). *Renewable and sustainable energy reviews*, 89, 51-60.
7. Українська вітроенергетична асоціація. (2019). *Вітроенергетичний сектор України 2019*. https://uwea.com.ua/uploads/reviews/uwea_2019_ua_preview.pdf.
8. Dufo-Lopez, R., Bernal-Agustín, J.L. (2008). Multi-objective design of PV-wind-diesel-hydrogen-battery systems. *Renewable energy*, 33(12), 2559-2572.

І.П. Каменева

ВИЗНАЧЕННЯ РЕЗИЛЬЄНТНОСТІ НА СОЦІАЛЬНОМУ ТА ЕКОЛОГІЧНОМУ РІВНІ

Вступ. Резильєнтність будемо визначати як здатність системи адаптуватися до змін, непередбачених ситуацій і криз, тобто відновлюватися після певного негативного впливу і значних пошкоджень. Цей термін останнім часом використовується в контексті сталого розвитку, критичної інфраструктури, психологічних, соціальних, екологічних досліджень та інших важливих сфер діяльності. Окремо можна досліджувати територіальну резильєнтність або резильєнтність технічних систем.

Термін «резильєнтність» походить від англійської resilience, що перекладається як «стійкість». В фізиці це означає здатність пружних тіл відновлювати свою форму після механічної дії. Вже в минулому сторіччі цей термін активно застосовували в екології та психології, де резильєнтність визначили як здатність людини протистояти складним життєвим обставинам та знаходити ресурси для відновлення після стресових подій [1].

Пізніше цей термін почали також використовувати для аналізу проблем в сфері бізнесу і економіки. Зокрема, резильєнтність економіки країни – це її здатність адаптуватися до нових умов та досить швидко відновлюватися після криз. Так, країни з високим рівнем резильєнтності можуть забезпечити швидкий вихід і прискорене відновлення після криз і катастроф, мають стабільну фінансову систему, належний рівень збереження робочих місць і доходів населення, щоб продовжити економічний розвиток [2].

Наразі можна уточнити визначення резильєнтності щодо складних систем різного походження. Це поняття залишається досить близьким до терміну «стійкість», але його інтерпретація набагато ширше і набуває різного значення в окремих сферах діяльності. Але в цілому резильєнтность на системному рівні передбачає як опір руйнівним впливам, так і здатність швидко відновлюватися після них. Такі системи зазвичай мають гнучкість, ресурсність та здатність до самоорганізації. Вони можуть адаптуватися до нових умов, зберігаючи свої основні функції та структури.

Системи захисту на соціальному та особистому рівні.

Суспільство в цілому можна розглядати як складну систему, на вхід якої надходить потік ресурсів X (t), який залежить від часу, а на вихід – певний обсяг товарів, послуг та інформації Y (t). Основною метою всієї системи має бути створення максимально сприятливих умов для життя людей. Економіка, громадські структури та норми виконують роль досить недосконалих регуляторів такого складного процесу, який реагує на дії середовища з певним запізненням. У випадку природних або техногенних катастроф час запізнювання має бути мінімальним. Тому необхідно забезпечити швидку реакцію на загрозу і ситуаційне управління, підготувавши набір заздалегідь відпрацьованих сценаріїв з використанням зворотного зв'язку.

На суспільному рівні ці функції виконує спеціальна система цивільного захисту населення [3]. На рівні окремого організму таку реакцію забезпечує імунна система, яка може своєчасно розпізнати чужорідні молекули та мікроорганізми, щоб ефективно очистити організм [4]. Обидві системи розраховані на порушення, небезпечні впливи та аварійні ситуації, де в якості критичного параметра виступає час реакції.

Зокрема, важкі хвороби імунної системи характеризуються зростанням часу імунної реакції. В обох зазначених випадках системи розпізнавання повинні мати достатньо високу чутливість, щоб своєчасно відзначати слабкі сигнали. Збільшення часу затримки, недосконаліть системи моніторингу та оцінки вихідної інформації різко знижують їх ефективність. Тому так часто виникає відомий «ефект надмалих концентрацій», тобто при дуже малих дозах зафіксовано сильні ураження, для малих доз організм успішно долає вплив, а великі дози знову ж таки приводять до важкого стану [4, 5].

Це можна пояснити тим, що надмалі дози знаходяться за межами чутливості системи, тобто захисні механізми своєчасно не включаються.

Зауважимо, що в окремих сферах науково-технічної діяльності під впливом подій останнього часу виникла необхідність переходу від концепції захисту складних систем від руйнування до ***концепції резильєнтності.***

На державному рівні наразі особливе значення надається поняттю резильєнтності критичної інфраструктури, зокрема енергетичної системи України, яка опинилася в важкому стані. Для енергетичної системи країни або окремих енергетичних підприємств резильєнтність визначається як здатність енергетичного сектору і його складових адаптуватися до шокових загроз та стресових навантажень, а також протистояти, реагувати та швидко відновлюватися після таких збурень [6].

Механізми екологічної безпеки. Загалом, поняття безпеки для різних ситуацій може бути досить неоднозначним. Зокрема, на рівні екологічної системи безпека визначається підтримкою всіх параметрів чисельності у відповідних межах. При цьому вимоги щодо безпеки всієї системи в цілому та безпеки окремих її частин нерідко можуть вступати в протистояння. Так, для збереження безпеки індивіда інколи потрібно зберегти життя ціною загибелі певної частини клітин і навіть окремих органів.

Загалом поняття безпеки та ризику слід віднести до системних понять, тобто їх визначення залежить переважно від того, які системи необхідно досліджувати. Під системою в даному контексті ми розуміємо складний об'єкт, який має здатність підтримувати власне існування (гомеостаз) за допомогою циклічної структури зв'язків між окремими частинами.

Нагадаємо, що гомеоста́з (гр. ὁμοιοστάσις від ὅμοιος «однаковий, подібний» + στάσις «стояння; нерухомість») — це здатність відкритої системи зберігати стабільність свого внутрішнього стану за допомогою відповідних реакцій, спрямованих на підтримку динамічної рівноваги.

Безпека екологічної системи визначається як відсутність (або низька імовірність порушень гомеостазу протягом конкретного проміжку часу, а

системний ризик – це некерований або не повною мірою керований фактор, здатний порушити або суттєво послабити її гомеостаз [5].

Спробуємо пояснити, яким чином можна підійти до визначення і оцінки стану гомеостазу та його динаміки. На перших етапах потрібно виділити основні фактори, які мають вплив на динаміку досліджуваної системи.

Для ілюстрації з станом динамічної системи можна зіставити число k, яке будемо називати «системним коефіцієнтом підсилення». Якщо $k > 1$, система здатна до відтворення і розширення. Якщо $k < 1$, то система рухається до загибелі. При наявності такої характеристики під ризиком можна розуміти будь-який неконтрольований фактор, здатний зменшити величину k. В такому випадку ступінь ризику легко оцінити. Допустимий ризик призводить до незначних змін: k залишається більше 1. При критичних значеннях ризику величина k буде наближатися до 1, що сприяє вразливості для багатьох інших ризиків. При фатальних значеннях ризику процес вже набуває незворотного характеру, тобто система руйнується.

Отже, для підтримки гомеостазу і компенсації несприятливих зовнішніх впливів системі потрібна певна мінімальна складність. Чим складніша організація системи, тим більше зовнішніх впливів вона може витримати і компенсувати В природних системах виживання забезпечують переважно не окремі особи, а колонії з цих одиниць. В таких системах цінність однієї особи досить невелика, зате колонії продовжують своє існування тривалий час за рахунок високої швидкості розмноження простих організмів.

Засоби оцінювання екологічної безпеки.

Поняття екологічної безпеки можна розглядати в двох аспектах. В першому випадку небезпека приходить ззовні і виникає в зовнішньому середовищі. До цієї категорії ризику слід віднести екологічний ризик, пов'язаний із забрудненням довкілля, стихійними лихами або техногенними аваріями. Зовнішні ризики необхідно відстежувати за змінами тих чи інших параметрів зовнішнього середовища. До зовнішніх ризиків також відноситься ризик поширення інфекційних захворювань, зокрема, гострих вірусних інфекцій (грип, ковід-19 тощо), де визначаються епідеміологічні ризики.

Другий варіант небезпеки відрізняється тим, що загроза знаходиться в самому організмі, тобто має оцінюватись в процесі дослідження стану організму. До цієї групи слід віднести ризик, пов'язаний з генетичними особливостями організму, які можуть стати причиною досить важких захворювань (генетичний ризик). В медичних дослідженнях використовують загальне поняття медичного ризику, який можна обчислити як імовірність виникнення конкретних захворювань.

Основною відмінністю між поняттями резильєнтності та стійкості можна вважати те, що стійкість – це здатність екологічної системи поглинати негативні впливи або протистояти збуренням та іншим стресовим чинникам, залишаючись у межах певного режиму (тобто зберігаючи свою структуру і функції). Поняття резильєнтності екосистеми включає додаткові можливості для переходу на інші режими (або енергетичні рівні), зберігаючи свої основні функції. Отже,

резильєнтність відображує більше можливостей для адаптації екологічних систем, тобто це здатність підтримувати стан рівноваги (баланс всіх складових) на відповідному рівні для даного діапазону значень.

Подібні задачі формально можна описати в рамках багатовимірного аналізу даних, тобто, перейти в простір інформативних показників [4, 5].

Для збереження безпеки навколишнього середовища наразі важливо вдосконалювати систему моніторингу стану довкілля та ретельно стежити за зміною системних властивостей окремих територіальних систем. В процесі контролю таких змін і тенденцій можна вчасно визначити як появу нових ризиків, так і ефективні засоби впровадження нових ресурсів для підтримки, відновлення та розвитку екологічних систем.

Поглибленому дослідженню складних динамічних систем та методам математичного моделювання перехідних процесів (виявленню особливостей та біфуркацій) присвячено ряд фундаментальних робіт [7, 8 та ін.].

Для підтримки екологічної безпеки в ІПМЕ НАН України розроблено багатовимірні моделі та засоби аналізу даних моніторингу, спрямовані на визначення критичних значень та рівнів ризику, що допомагає вчасно виявити ознаки небезпеки та прийняти відповідні рішення [9].

1. Мельничук І.Я. Теоретико-методологічні основи розвитку та корекції резильєнтності. №2 (2024) Наукові записки. Серія: Психологія https://journals.cusu.in.ua/index.php/psychology/article/view/469.
2. Резильєнтність економіки: Сутність і виклики для України. БІЗНЕСІНФОРМ № 7. 2023. https://www.business-inform.net/export_pdf/business-inform-2023-7_0-pages-30_41.pdf.
3. Про затвердження Положення про єдину державну систему цивільного захисту. Редакція від 17.08.2024. https://zakon.rada.gov.ua/laws/show/11-2014-%D0%BF#Text.
4. Каменева И, П., Сердюцкая Л. Ф. Многомерный подход к исследованию адаптационных возможностей организма // Збірник наукових праць ІПМЕ НАН України. – Вип.11. – Львів: Світ, 2001. С. 119-17.
5. Сердюцкая Л. Ф., Каменева И. П. Системный анализ и математическое моделирование медико-экологических последствий аварии на ЧАЭС и других техногенных воздействий. К.:"Медэкол", 2000. С.173.
6. Stout S., Lee N., Cox S., Elsworth J., Leisch J. Power sector resilience planning guidebook. – U.S. Department of Energy's NREL and USAID. – 2019. – 82 p. – URL https://www.nrel.gov/docs/fy19osti/73489.pdf.
7. Gilmore R. Catastrophe Theory for Scientists and Engineers. John Wiley & Sons Inc., 1981. – 686 c.
8. Nikolis, G., Prigogine, I. Exploring complexity: An introduction. W.H. Freeman and Company, New York, 1989. – 328 c.
9. *Артемчук В.А., Каменева И.П., Яцишин А.В.* Специфика применения когнитивного анализа информации в задачах обеспечения экологической безопасности // Электронное моделирование, 2017, **39**, № 6, с. 107–124.

T. Biloborodova

CONCEPT MODEL OF DECISION-MAKING PROCESS IN TRUSTWORTHY AI-BASED SYSTEM

One of the primary domains where artificial intelligence (AI) shows a significant impact is decision-making [1]. From decision support in emergency situations to medical decision-making, the application of AI technologies in facilitating informed decisions support in the efficient processing of large amounts of information. The trustworthiness of these systems is crucial for the successful implementation and integration of this technology. Within the framework of standardization initiatives, guidelines have been developed to ensure the trustworthiness of AI systems [2, 3]. These initiatives assume that trustworthiness is an inherent characteristic of AI, which can be achieved through the optimization of AI systems.

Trustworthiness is used to describe, on one hand, the objective characteristics of a trustworthy agent, and on the other, the subjective perception of these characteristics by the human [4]. Actual (objective) trustworthiness is part of the system's properties, with key factors including accuracy, resilience, security, transparency, and explainability. Perceived (subjective) trustworthiness of AI arises from the user's perception and significantly influences whether the user trusts the system and incorporates its recommendations into their work [5]. This perception is context-dependent and subjective. Trust is emergent and evolving, and it is a property of the interactions between humans and AI. Explainability and interpretability of AI results have been recognized as essential for trustworthy AI and are listed as criteria to gain trust in AI systems [6]. However, AI recommendations can sometimes be erroneous or misleading. An overreliance of human intelligence (HI) on AI recommendations may lead to an overtrust in those being advised, who might misuse the system and potentially make poor choices affecting more than just decision-makers [5, 7, 8]. Interaction with AI systems always involves a degree of uncertainty, necessitating continuing evaluation. The interaction between AI and HI can be presents as a consequence of decisions made with a certain level of uncertainty regarding the final outcome.

Conceptualisation of trustworthy AI-based system helps to study the ways in which decision is formed, and also understand the relationship between the results of AI and HI decisions. Conceptual model of decision-making process is the first step towards trustworthy AI system design which is to convey system principles and functionality [9]. The model represents entities and relationships among them, and serves as basis for identifying actors and possible communication paths and for describing and developing the architecture.

Proposed concept model of decision-making process in trustworthy AI-based system is depicted in the Fig. 1.

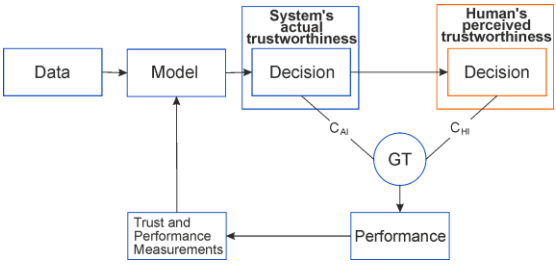


Figure 1 – Concept model of decision-making process in trustworthy AI-based system (Adapted from [10, 11])

The system diagram illustrates the decision-making process in AI-based system. A model proposes a decision, obtains the trust from the human for the proposed decision, takes a subsequent action, such as suggesting a new solution aligned with their interests, takes into account the previous outcomes of decision-making and adjusts their trust sensitivities as necessary for future decision-making. C_{AI} indicates correlations between ground truth (GT) and the actual trustworthiness of a system. C_{HI} indicates correlations between the GT and the human's perceived trustworthiness. The performance reflects the correlation between the actual trustworthiness of the system and the human's perceived trustworthiness.

1. Stettinger, G., Weissensteiner, P., Khastgir, S. (2024). Trustworthiness Assurance Assessment for High-Risk AI-Based Systems. *IEEE Access*.
2. Loh, W., Hauschke, A., Puntschuh, M., Hallensleben, S. (2022). *VCIO based description of systems for AI trustworthiness characterisation*. VDE SPEC, Bd. 90012 V1.0.
3. DIN, DKE (2020) *German standardization roadmap on artificial intelligence*.
4. Schlicker, N., Langer, M. & Hirsch, M.C. (2023). Wie vertrauenswürdig ist künstliche Intelligenz? *Innere Medizin*. 64, 1051–1057. https://doi.org/10.1007/s00108-023-01602-1.
5. Lee, J.D., See, K.A. (2004). Trust in automation: designing for appropriate reliance. *Human Factors*. 46(1), 50–80. https://doi.org/10.1518/hfes.46.1.50_30392.
6. Tabassi, E. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). *NIST Trustworthy and Responsible AI, National Institute of Standards and Technology*. https://doi.org/10.6028/NIST.AI.100-1.
7. Henley, J. (2022). *Chess robot grabs and breaks finger of seven-year-old opponent*. https://www.theguardian.com/sport/2022/jul/24/chess-robot-grabs-and-breaks-finger-of-seven-year-old-opponent-moscow.
8. Hawkins, A.J. (2022). *A Tesla vehicle using 'Smart Summon' appears to crash into a $3.5 million private jet*. https://www.theverge.com/2022/4/22/23037654/tesla-crash-private-jet-reddit-video-smart-summon.
9. Macaulay, T. (2016). *RIoT control: understanding and managing risks and the internet of things*. Morgan Kaufmann.
10. Uslu, S. (2024). *Trustworthy and Causal Artificial Intelligence in Environmental Decision Making* (Doctoral dissertation, Purdue University Graduate School).
11. Schlicker, N., Langer, M. (2021). Towards warranted trust: A model on the relation between actual and perceived system trustworthiness. In *Proceedings of Mensch und Computer 2021* (pp. 325-329).

Д.М. Семенюк

ВРАХУВАННЯ ДЕЯКИХ ОСОБЛИВОСТЕЙ ПОШУКУ ВИТОКІВ НА ТРУБОПРОВОДАХ МІСЬКИХ ТЕПЛОВИХ МЕРЕЖ

Для пошуку місць витоків рідини в рубопроводах, що працюють під тиском, у тому числі міського водо і теплопостачання, широко застосовуються кореляційні течешукачі. Сутність методу пошуку полягає в тому, що витікання води крізь дефект супроводжується акустичними сигналами, які фіксуються на трубопроводі в місцях доступу по обидві сторони від витоку. Результатом пошуку є відстань L_u від одного з датчиків до витоку, яка у приладі обчислюється за формулою:

$$L_u = \frac{L}{2} + \frac{T \cdot V}{2} \qquad (1)$$

де L — відстань між датчиками; V — швидкість поширення вібросигналів по трубопроводу; T — різниця за часом між надходженням вібросигналів до одного та до другого датчиків кореляційного течешукача. Ця різниця визначається у течешукачі за обчисленою у ньому взаємною кореляційною функцією зафіксованих на трубопроводі сигналів.

Звичайно значення V запрограмовано у приладі та обирається в залежності від діаметра та матеріалу труби, а також від температури води. Однак, відповідно до відомої формули [1], отриманої Кортвегом, у вираз для швидкості поширення хвиль в рідині, що заповнює трубу, входить ще товщина стінки труби. У пошкоджених корозією трубах ця товщина може значно відрізнятись від товщини, яка була при прокладанні трубопроводу. Внаслідок цього, відповідно до згаданої формули Кортвега, фактична швидкість поширення V акустичних хвиль вздовж трубопроводу може відрізнятися від заданої у приладі до 30 %. Для наочності, на рис. 1 [2] надана діаграма відмінності реальної, фактичної швидкості поширення акустичних хвиль від закладеної у течешукачах, в залежності від ступеню зносу трубопроводу, тобто втрати частини основного металу трубою внаслідок корозії. Діаграма надана для типових діаметрами труб. Це діаметри, які звичайно використовуються у міських теплових мережах: 102 мм, 219 мм, 325 мм, 720 мм, 1020 мм, 1220 мм. Не відповідність фактичної швидкості закладеній у приладі призводить до похибки $L_П$ визначення координати витоку, яка дорівнює:

$$L_П = \frac{T \cdot V_П}{2} \qquad (2)$$

де $V_П$ - різниця між приладовою швидкістю та фактичною.

Як випливає з (2), похибка визначення координати витоку $L_П$ пропорційна виміряній у приладі різниці часу T. Цю обставину можна використати шляхом вибору такого місця встановлення датчика на трубопровід, при якому значення T буде найменшим. Цьому методичному прийому сприяє наступна особливість прокладання тепломереж. Звичайно ці трубопроводи прокладено у непрохідних каналах. Це канали з залізо бетонних П-подібних коробів чи блоків, у яких трубопровід покладено на рухомі та нерухомі опори. Відсутність демпфування трубопроводу грунтом (за виключенням місць затоплення чи замулення каналів) сприяє поширенню вібросигналів на значні відстані. Як правило, збитковий тиск є не менше 2 Атм., що забезпечує виникнення у місці витоку акустичного шуму. Відстань між місцями доступу до трубопроводу звичайно не перевищує 200м. Вказані особливості тепломереж приводять до того, що шуми витоку можна зареєструвати датчиками течешукача не тільки в найближчих до витоку місцях доступу до труб, наприклад у теплових камерах, але й в інших, більш віддалених тепло камерах, підвалах будинків, теплових пунктах тощо. Значення T є малим, якщо виток опиняється близько до центру ділянки трубопроводу між датчиками. Якщо виток опиняється далеко від цього центру, то вказані особливості тепломереж іноді дозволяють штучно створити умови для зменшення T та відповідно похибки координати $L_П$. Відбувається це шляхом перестановки ближнього до витоку датчика у сусіднє, наявне місце доступу до трубопроводу у напрямку від пошкодження. Цей методичний прийом можна поєднувати з відомим трьох точковим методом визначення координати витоку, при якому, за рахунок виконання додаткових вимірювань при суттєво зміненій відстані між датчиками, можна визначати координату витоку без явного завдання швидкості V.

Пошук витоків в тепломережах кореляційними течешукачами часто утруднений наявністю потужних акустичних перешкод від елеваторів, засувок, механізмів насосних станцій і т.і. Враховуючи багатомодовість поширення хвиль трубопроводами з канальною прокладкою, акустичні перешкоди нерідко призводять до помилкових показань кореляційних течешукачів. Тому важливим етапом пошуку витоків у тепломережах є ідентифікація джерела вібросигналів. Для цього в ІПМЕ ім. Г.Є Пухова НАН України розроблено приладовий комплекс, що складається з кореляційного параметричного течешукача К-10.5М2 [3] та термоакустичного течешукача А-10Т3 [4]. Комплекс добре пристосований для діагностики тепломереж і призначений не тільки для визначення місця витоку на пошкодженій ділянці, але і для пошуку даної ділянки в розгалуженій підземній мережі трубопроводів. Відбувається це шляхом проведення коректних вимірювань та порівнянь за допомогою А-10Т3 рівнів вібрації на трубопроводі як між тепловими камерами, так і всередині них. Пошук витоків за допомогою приладового комплексу не обмежується визначенням координати

найпотужнішого джерела шуму на трубопроводі. Такий підхід часто призводить до помилок, оскільки крім витоку на трубопроводі є інші джерела шуму - бойлера, елеватори, насоси, шуми в засувках тощо. Тому комплекс К-10.5М2/А-10Т3 пристосований для роботи в умовах декількох джерел шумів і для їх ідентифікації наступним чином:

1) Кореляційний параметричний течешукач К-10.5М2 має спеціальний режим, в якому оператору в наочній та зручній формі надаються параметри джерел шуму: частотний діапазон, потужність, якість, координата [5].

2) Акустичний течешукач А-10Т3 пристосований для роботи як ззовні, так і всередині теплокамер і має необхідні для цього характеристики. Це дуже малі розміри, міцний корпус, цифрова багаторозрядна індикація рівня сигналу. А-10Т3 має можливість підключення датчиків з магнітним тримачем для кріплення на трубопроводі для точного вимірювання рівнів вібрації на трубах у теплокамерах у різних точках. У більшості випадків це дає можливість визначити напрямок приходу вібросигналів і з'ясувати їх джерело.

Враховуючи відсутність демпфування трубопроводів ґрунтом, динамічний діапазон реєстрованих вібросигналів і відповідно виміряних рівнів вібрації перевищує 60 дБ. Особливо важливо це враховувати при пошуку пошкодженої ділянки теплотраси на розгалуженій системі тепломережі шляхом порівняння рівнів вібрації труб у різних місцях доступу.

Тому течешукач А-10Т3 має просту у застосуванні, багаторозрядну цифрову індикацію рівнів вібрації, що дозволяє швидко скласти карту рівнів шумів і по ній виявити пошкоджену ділянку. Прилад А-10Т3 добре себе зарекомендував при пошуку витоків у внутрішньо будинкових системах опалення та водопостачання на ПВХ трубопроводах.

Поширення вібросигналів трубопроводом відбувається у вигляді декількох хвиль з різними швидкостями, через що кореляційна функція часто розмивається і її інтерпретація стає неоднозначною. У таких випадках важливо не помилитися у виборі діапазону частот із достовірними даними про координату джерела шуму. Для вибору частотного діапазону кореляційної функції з достовірними показаннями витоку у К-10.5М2 реалізовано режим параметричного просторово-частотного аналізу кореляційних функцій. Цей режим застосовується у випадках нечітких показань кореляційної функції, викликаних значним загасанням вібросигналів витоків, а також за наявності більше однієї течі.

До формули (1) входить відстань між датчиками, яку часто визначають за кресленнями та схемами прокладання інженерних мереж. З особистого досвіду відомо, що у 50% випадків схеми не відповідають дійсності чи відсутні. Часто, особливо на малих діаметрах, не вказуються температурні компенсатори, повороти, точний напрямок трубопроводу тощо. Щоб уникнути помилок з відстанню між датчиками, тобто довжини трубопроводу включаючи всі повороти, температурні компенсатори, спуски та підйоми,

потрібно визначити фактичне розташування трубопроводу. Для цієї мети використовують трасопошуковий комплект приладів, який призначений для безконтактного визначення фактичного розташування та глибини прокладання підземних металевих трубопроводів, силових та зв'язкових, працюючих кабелів, а також інших металевих протяжних підземних комунікацій. На закінчення слід сказати, що згадані методичні та приладові засоби дозволяють на трубопроводах тепломереж забезпечувати визначення місць витоків із ймовірністю не менше 0,9 з похибкою до 1 метра.

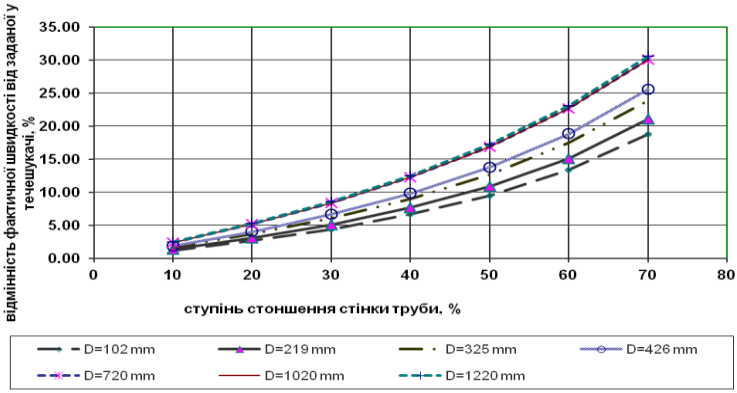


Рисунок 1 – Вплив корозійного стоншення стінки трубопроводу на швидкість інформативних акустичних хвиль від витоку

1. Бергман Л. Ультразвук. — М.: ИИЛ, 1957.— 726 с. — С. 393. Семенюк Д.Н. Особенности поиска утечек в подземных трубопроводах теплових сетей. Сантехніка, опалення, кондиціонування (С.О.К) 2006, №6, с.10-12.
2. А.А Владимирский, И.А Владимирский, И.П Криворучко, Н.П. Савчук Разработка модернизированного корреляционного течеискателя К-10.5М2 Моделювання та інформаційні технології. Збірник наукових праць. Інститут проблем моделювання в енергетиці НАН України. Вип. 79, Київ, 2017р.-с.69-70.
3. Владимирский А.А., Владимирский И.А., Криворучко И.П. Термоакустический течеискатель А-10Т3. XXXVIII науково-технічна конференція молодих вчених та спеціалістів інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. Збірник тез конференції. Київ. 15 травня 2020р. – С 72.
4. Владимирський О.А., Владимирський І.А. Просторовий і частотний кореляційні параметричні методи визначення координат витоків підземних трубопроводів// Електрон. моделювання, 2021, 43, № 4, с.22 —36.

О.А. Владимирський, І.А. Владимирський, Д.М. Семенюк,
І.П. Криворучко, Г.В. Анфімова

ВИМОГИ ДО АКУСТИЧНИХ ТЕЧЕШУКАЧЕЙ МЕРЕЖ ЦЕНТРАЛІЗОВАНОГО ТЕПЛО ТА ВОДОПОСТАЧАННЯ

Проаналізовано можливості сучасних акустичних течешукачей (АТ) відомих виробників щодо врахування особливостей пошуку витоків на вітчизняних підземних мережах централізованого тепло- та водопостачання. Цими особливостями є розгалуженість, значний ступінь зносу запірної арматури та трубопроводів, міліарні впливи та підвищена інтенсивність застосування приладів. Бо на відміну від західних умов, у крупних містах, пошук витоків у вітчизняних мережах є не сервісним обслуговуванням, а елементом щоденної технології тепло і водопостачання населення.

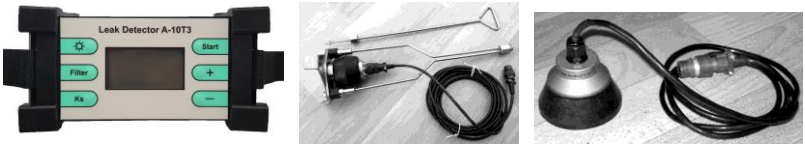
Можливості течешукачів визначались з опису приладів, демонстрацій та наведених технічних характеристик: DXmic Hydreka SA компанії Halma, Франція [1], HL-7000, SebaKMT, Німеччина [2], Aquascope 550 Gutermann, Швейцарія [3], HL 50-BT, SebaKMT, Німеччина [4], Mikron3 Junior Ovarro Connecting Technologies, Велика Британія [5], Aqua M300 F.A.S.T. GmbH, Німеччина [6], Lmic, HWM-Water Ltd — дочірнє до Halma Plc, Велика Британія [7], Tmic, HWM-Water Ltd — дочірнє до Halma Plc, Велика Британія [8].

Проведений аналіз свідчить про наступне.

У багатьох АТ маються GPS приймачі та безпровідні навушники. Стосовно наявних умов роботи ці властивості є корисними. Однак слід враховувати, що GPS навігація не вказує фактичного положення підземного трубопроводу, місця п-подібних компенсаторів та поворотів, перетину електрокабелів. Тому цей сервіс не замінює необхідності застосування індукційного трасошукача чи достатньо точної документації. Безпровідні навушники додають зручності у роботі внаслідок відсутності кабелю. Але, на відміну від простіших, кабельних навушників, повинні мати заряджений акумулятор. В умовах інтенсивної роботи та багатої кількості інших обов'язкових акумуляторів це потребує додаткової уваги. Наприклад, є велика кількість курвіметрів – вимірювальних коліс з електронною індикацією відстані. Але внаслідок наявних у них акумуляторів, для пошуку витоків перевагу віддають чисто механічним пристроям. Мабуть тому деякі з зазначених моделей АТ мають комбіноване, дротове та бездротове підключення навушників. Також відзначимо, що ці сервіси збільшують вартість АТ, особливо при використанні корисної високоточної GPS навігації. Бездротовість навушників має й інші наслідки. Наприклад, у HL 7000 при використанні інших, не з комплекту приладу, бездротових навушників, не працює функція захисту слуху оператора від гучних впливів, що зазначено у керівництві з експлуатації. Це важливо, бо при інтенсивній польовій роботі навушники зношуються.

Майже всі зазначені АТ добре пристосовані для пошуку витоків по грунту над трубопроводом. Для цього використовуються чутливі електромагнітні акустичні геофони, акселерометри, спектральний аналіз сигналів, ретельне налагодження частотних фільтрів. Використовуються різні за принципом дії системи захисту слуху оператора від несподіваних гучних впливів. Все це актуально й для наших умов роботи. Але щодо вимірювань на арматурі, на трубопроводах у місцях доступу до трубопроводів - МД (теплові камери, підвали, теплові пункти тощо), прилади розраховані на занадто спрощену технологію діагностування. Бо стосовно роботи на розгалужених мережах централізованого тепло та в та водопостачання, можливості зазначених сучасних приладів не повною мірою відповідають умовам експлуатації, стану трубопроводів, доступу до труб та, виходячи з цього, більш складній технології результативного пошуку витоків. Пояснимо це. Відмінною акустичною особливістю діагностування трубопроводів, особливо трубопроводів теплових мереж, є великий динамічний діапазон рівнів акустичних сигналів на трубах у МД, які потрібно оперативно порівнювати між собою. Це потрібно для визначення пошкодженої ділянки трубопроводу, при з'ясуванні, яка труба є з витоком – подавальна чи зворотна, ЦО чи ГВП, бо ці труби часто прокладені в одному коробі з якого ллється вода, при оцінці несуперечності виміряних рівнів по кінцях трубопроводу вказаній течешукачем координаті витоку тощо. Проведені ІПМЕ ім. Г.Є. Пухова НАН України у ході виробничого пошуку витоків у "Київенерго" дослідження вказують, що навіть діапазону у 60 дБ буває замало. При цьому виявлені закордонні АТ відображають виміряний рівень сигналу у формах: гістограми, рядка з кількох світлодіодів та у числовому вигляді, який містить лише 2 десяткових знаки. Динамічний діапазон порівнювальних рівнів, таким чином, не перевищує 40 дБ. Ці АТ дозволяють додатково налаштовувати коефіцієнт посилення для забезпечення чутливості шкали індикації рівнів до фактичної їх зміни. Це припустимо для роботи по грунту. Але порівнювати між собою рівні сигналів на трубах, різниця між якими зазвичай перебільшує 40 дБ, аналізувати їх, зіставляючи з наявним фактичним тиском, з вказаною течешукачем відстанню до витоку та іншими чинниками у ході оперативного виконання робіт є проблематичним. Крім того, проведені експерименти довели, що закладати значну нелінійність по типу логарифмічної у шкалу вимірювань для збільшення її фактичного динамічного діапазону не припустимо, бо при цьому зменшується чутливість приладу до абсолютної різниці рівнів сигналу. А це є критичним при порівнянні рівнів шумів на грунті і на трубах у межах теплової камери при з'ясуванні напрямку надходження у неї шуму та відповідно природи його джерела. Отже, з одного боку, маємо потребу у великому динамічному діапазоні шкали вимірювань рівнів акустичних сигналів, а з іншого – у достатній чутливості. Тому ІПМЕ ім. Г.Є. Пухова НАН України розроблено АТ А-10Т3 [9], рис.1, у якому результати вимірювань відображаються у цифровій формі 4 десятковими розрядами у діапазоні 66 дБ, рис.2. Прилад є універсальним, тобто пристосованим і для пошуку пошкодженої ділянки трубопроводу, і для

визначення місця витоку на ньому. Додатково прилад призначений для визначення витоку за тепловою ознакою бо має датчик температури з розподільчою здатністю 0,02°С. Виходячи з того, що такі вимірювання в умовах зносу та пошкоджень запірної арматури та трубопроводів є дуже витребуваними, доцільно розробити та опрацювати відповідну методику застосування А-10Т3 на розгалужених мережах трубопроводів. Ця робота проводиться за проектом «Розроблення апаратно-програмного комплексу та методики оперативного виявлення пошкоджень систем тепло- та водопостачання з врахуванням їх зношеності та мілітарних впливів», що виконується за рахунок грантової підтримки Національного фонду досліджень України (НФДУ). Автори висловлюють щиру подяку Фонду за підтримку виконання цієї витребуваної роботи.



а) б) в)

Рисунок 1 – Блок оператора акустичного течешукача А-10Т3 (а) з акустичним (б) та тепловим (в) датчиками

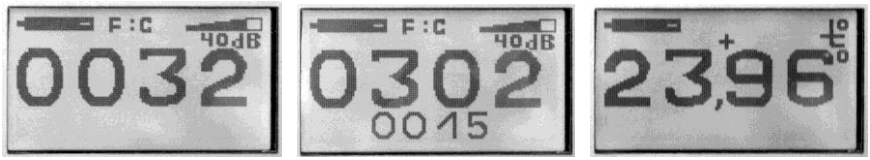


Рисунок 2 – Індикація результатів вимірювання рівнів акустичних сигналів та температури течешукачем А-10Т3. 40 дБ – єдине додаткове кероване посилення сигналів в датчику

1. DXmic User Manual.URL: https://www.inlec.com/media/view/2019/02/man-150-0001-b_dxmic_user_guide__1337.pdf (дата звернення 15.12.2024).
2. SebaKMT – Модель HL 7000. URL: https://www.environmental-expert.com/products/sebakmt-model-hl-7000-electro-acoustic-leak-detection-with-ground-microphone-1018089 (дата звернення 15.12.2024).
3. AquaScope – Модель 550 – Акустический комплект для обнаружения утечек воды. URL:https://www.environmental-expert.com/products/aquascope-model-550-acoustic-water-leak-detection-kit-208965 (дата звернення 15.12.2024).
4. Leak detection and monitoring of water supply networks. URL: https://www.megger-sebakmt.de/files/sebakmt/downloads/brochures/EN/Water-catalogue_EN_2022_V02b.pdf (дата звернення 15.12.2024).

5. Оварро Микрон3 Юниор. URL:https://www.accurate.kiwi/Product/leak-ovarro-mikron3junior/https://fastgmbh.de/en/products/listening-devices/aqua-m300(дата звернення 15.12.2024).
6. АКВА М300 Интеллектуальній геофон для поиска утечек. URL:https://fastgmbh.de/en/products/listening-devices/aqua-m300.
7. Lmic USER MANUAL: Operators Guide.URL: https://www.fluidconservation.com/wp-content/uploads/2024/03/Lmic-Manual.pdf (дата звернення 15.12.2024).
8. Tmic Portable Electronic Listening Stick. URL:https://www.axiomams.eu/en/get-attachment/22342?name=Tmic.pdf.
9. Владимирский А.А., Владимирский ИА., Криворучко И.П. Термоакустический течеискатель А-10Т3. XXXVIII науково-технічна конференція молодих вчених та спеціалістів інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. Збірник тез конференції. Київ. 15 травня 2020р. – С 72.

С.В. Сушко

МЕТОДИ ВІДДАЛЕНОГО МОНІТОРИНГУ ПАРАМЕТРІВ ЕНЕРГОМЕРЕЖІ

Отримання результатів об’єктивного спостереження для енергомережі необхідне для оперативного контролю параметрів роботи енергосистеми та для швидкого виявлення аварійних ситуацій, перевантажень та пошкоджень об’єктів енергомережі. Останнім часом через військові дії контроль стану енергооб’єктів ще більш актуальний.

Дистанційне спостереження за віддаленими об’єктами, які, до того ж, можуть бути обстріляні, є важливим елементом енергобезпеки та енергетичної резильєнтності. Швидке визначення на операторському пульті пошкоджених або знищених енергетичних об’єктів надає необхідну інформацію щодо планування тимчасової або довготривалої реконфігурації енергетичних мереж, а також дозволяють запланувати найбільш ефективні ремонтні дії для максимально швидкого відновлення енергопостачання.

В контексті моніторингу генерації та споживання набули так звані Smart Grid [1]. Ця технологія використовує вимірювання енергопостачання і енергоспоживання і дозволяє більш ефективно використовувати ресурси через управління споживачами і генерацією. Таким чином Smart Grid – це модернізовані мережі електропостачання, які використовують інформаційні технології для збору інформації про енерговиробництво й енергоспоживання. На практиці це дозволяє автоматично підвищувати ефективність, надійність, економічну вигоду, а також стійкість виробництва й розподілу енергії в режимі реального часу.

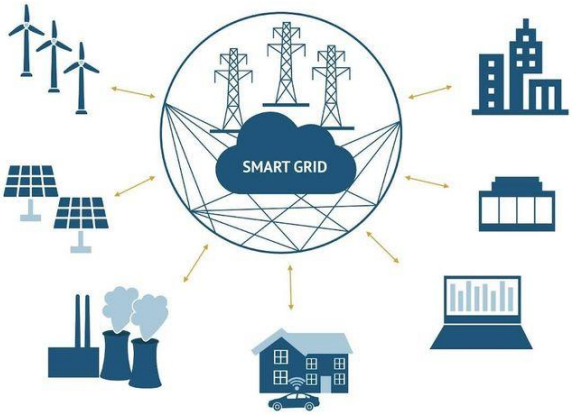


Рисунок 1 – Елементи мережі Smart Grid

Загалом, енергомережа не обов'язково може бути державною мережею змінного струму. Це також може бути енергомережою виробничого підприємства, домогосподарств, медичних закладів або військових підрозділів, або навіть низьковольтною мережею [2]. У такому випадку моніторинг ресурсів енергомережі надає змогу реагувати на зміни генерації та споживачів. В такому випадку важливо також монітори рівень напруги на акумуляторних батареях, щоби мати змогу оцінити час роботи без генерації.

Методи віддаленого моніторингу можна класифікувати за різними показниками, наприклад на дротові та бездротові, на вимірювальні та контролюючі та інші.

Побудова систем віддаленого моніторингу можлива як із застосуванням професійного обладнання, так і на основі апаратного забезпечення широкого вжитку, модифікованого під конкретні задачі.

Важливою частиною систем моніторингу параметрів енергомережі є програмне забезпечення, що передає, накопичує та відображає отримані результати вимірів для оператора енергомережі. Загалом, розроблення такого програмного забезпечення є складною задачею з використанням багатьох компонентів для розробки: протоколів даних, баз даних, графічного інтерфейсу та інші. Написання програмного коду настільки різноманітних компонентів вимагає високої кваліфікації розробників.

Іншим можливим шляхом для програмного забезпечення є використання існуючого програмного забезпечення. Особливий інтерес мають компоненти системи Інтернету речей (IoT). Інтернет речей – це комплексна система, яка містить різноманітні технології та компоненти для забезпечення обміну даними між пристроями. В основі IoT лежить збір, передача та аналіз даних для автоматичного керування пристроями. Такі принципи побудови і наявні компоненти Інтернету речей можуть бути використані в побудові системи моніторингу параметрів енергомережі. Значення напруги, споживаний струм, виміряна частота, індикатори наявності напруги і інші показники енергомережі можуть бути виміряні, передані, накопичені і відображені повністю або частково засобами, що використовуються в Інтернеті речей: протоколи (MQTT), сервери накопичення і збереження даних (node-RED [3]). Інформація може зберігатись як локально на спеціальному сервері або ж у хмарі.

1. Chen, Z., Amani, A. M., Yu, X., & Jalili, M. (2023). Control and Optimisation of Power Grids Using Smart Meter Data: A Review. *Sensors*, *23*(4), 2118. https://doi.org/10.3390/s23042118.
2. Alymov, I., & Averbukh, M. (2024). Monitoring Energy Flows for Efficient Electricity Control in Low-Voltage Smart Grids. *Energies*, *17*(9), 2123. https://doi.org/10.3390/en17092123.
3. Z. Chaczko & R. Braun. (2017) Learning data engineering: Creating IoT apps using the node-RED and the RPI technologies. *16th International Conference on Information Technology Based Higher Education and Training (ITHET)*, Ohrid, Macedonia, pp. 1-8, doi: 10.1109/ITHET.2017.8067827.

С.В. Сушко

ПРИКЛАД ЗАСТОСУВАННЯ КОМПОНЕНТІВ ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ ДЛЯ ВІДДАЛЕНОГО МОНІТОРИНГУ НАПРУГИ

Побудова системи віддаленого моніторингу напруги є актуальною задачею. Це дозволить контролювати напругу однієї або декількох батарей постійного струму, що корисно для спостереження рівня заряду/розряду елементів резервного живлення або інших критичних застосувань, коли необхідно достатньо точно знати напругу на одному або декількох точках вимірювання не перебуваючи безпосередньо біля пристроїв [1].

Автор створив експериментальну систему вимірювання, передачі, зберігання та відображення даних використовуючи компоненти технології Інтернету речей. Ця технологія безпосередньо спрямована на збір, передачу та аналіз даних для автоматичного керування пристроями. Таким чином, концепція Інтернету речей може бути використана безпосередньо для моніторингу напруги.

За основу системи отримання, накопичення і відображення інформації автор використав програмний пакет Node-RED [2], що встановлюється на веб-сервер та є головним вузлом накопичення інформації. Загальна система вимірювання і зберігання значень напруги відображена на рис. 1.

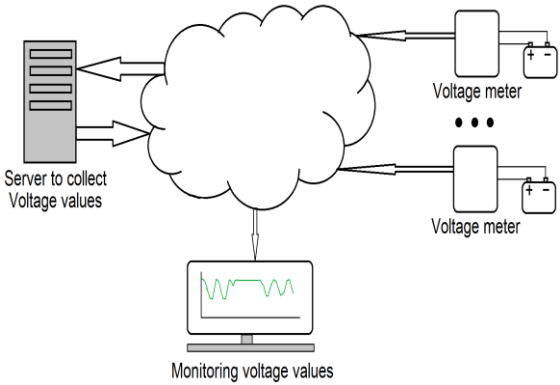


Рисунок 1 – Структура системи віддаленого моніторингу напруги

Важливим елементом такої системи є сенсор, який виміряє і передає виміряні значення напруги. Такий сенсор має містити всі необхідні інтерфейси для отримання і передачі значень напруги, а для практичного застосування бути компактним і дешевим. Автор обрав модуль ESP32-S3-Zero, який відповідає вказаним вимогам. Для вимірювання напруги використовувався акумулятор типу 18650, який і живив вказаний модуль. Для зручності автор поєднав усі компоненти на одному пристрої.

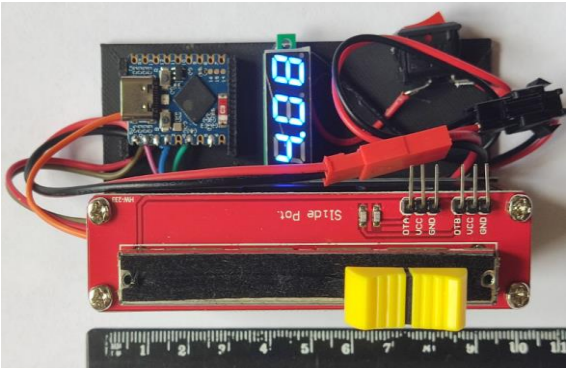


Рисунок 2 – Модуль вимірювання напруги

Автор провів тривалі експерименти, в яких переконався, що побудована система здатна виконувати закладені функції: вимірювати, передавати, накопичувати та відображати значення напруги в моменті та надавати графіки вимірів, як відображено на рис. 3.

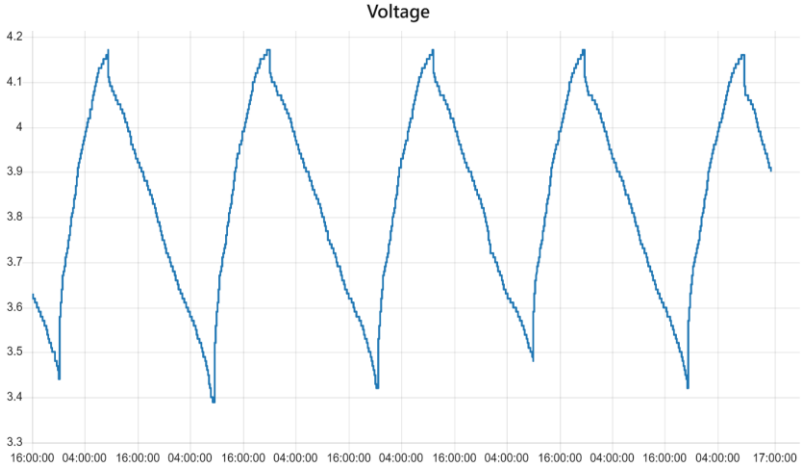


Рисунок 3 – Значення вимірів напруги впродовж одного тижня

1. Alymov, I., & Averbukh, M. (2024). Monitoring Energy Flows for Efficient Electricity Control in Low-Voltage Smart Grids. *Energies*, *17*(9), 2123. https://doi.org/10.3390/en17092123.
2. Z. Chaczko & R. Braun. (2017) Learning data engineering: Creating IoT apps using the node-RED and the RPI technologies. *16th International Conference on Information Technology Based Higher Education and Training (ITHET)*, Ohrid, Macedonia, pp. 1-8, doi: 10.1109/ITHET.2017.8067827.

І.П. Криворучко, О.А. Владимирський

ОСОБЛИВОСТІ ФОРМУВАННЯ СИГНАЛІВ УПРАВЛІННЯ В УСТАНОВЦІ НАВКУ-3

Для переміщення каретки віброкалібрувальної установки НАВКУ-3 [1] передбачається використання крокового двигуна (КД) у поєднанні з драйвером. Для точного відтворення закону переміщення каретки з мінімальним рівнем вібрації, як правило, синусоїдального виду, вимагається застосування мікрошагового режиму роботи двигуна. При цьому один період коливального переміщення каретки може складатися до декількох сотень тисяч елементарних кроків, величина яких представляється не менш ніж 22 двійковими розрядами. Крім того, мінімальні величини міжкрокових інтервалів можуть сягати 5 мкс тривалості. Ці інтервали часу потрібно відтворювати з точністю не гірше 1%. Це досить напружена задача реального часу для локального контролера на основі доступних однокристальних рішень. У свою чергу ОС Windows, яка встановлена на основному комп'ютері, не будучи системою реального часу, не може забезпечити необхідний ритм передачі даних у зовнішній пристрій. Можливе вирішення проблеми – проміжна буферизація потоків даних.

Можливим варіантом вирішення цієї задачі є використання USB-конвертора FT245R. Це швидкісний інтерфейс USB, який формує на своїх виходах паралельний 8-ми розрядний код і має швидкість передачі до 1 Мбайт/с [2]. Застосовується дворівнева буферизація: апаратурна - за рахунок блоків FIFI всередині мікросхем FT245 і програмна - драйвером D2XX, що встановлюється на ПК. У роботі пропонується використання розробленого блоку формування сигналів управління КД на базі цього інтерфейсу та мікроконтролера. Головною задачею цього блоку є отримання, трансформація кодів міжкрокових інтервалів у реальні часові інтервали і генерація сигналів управління КД.

Підготовлені на ПК масиви даних про міжкрокові інтервали передаються через USB-конвертор у форматі 3-х байт на одне значення інтервалу. Отримані мікроконтролером байти у паралельному вигляді передаються у регістри лічильника. Завантажені у регістри дані починають вираховуватися з частотою F_{gen} так, що час необхідний для появи сигналу переносу (carryout) якраз відповідає міжкроковому інтервалу. Цей сигнал є підставою для формування сигналу STEP схемою управління і формування (рис.1).

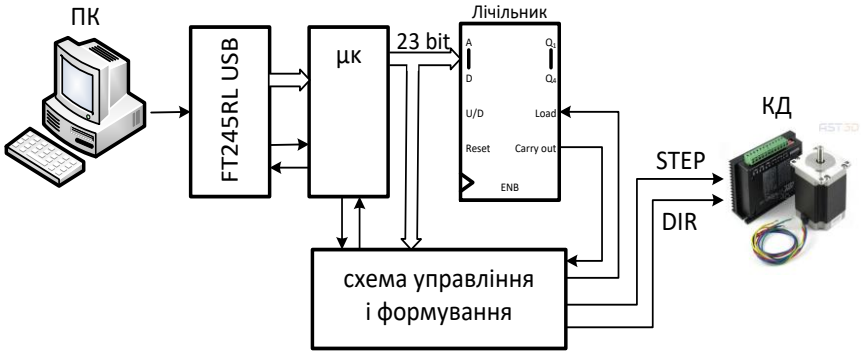


Рисунок 1 – Структура блока формування сигналів управління КД

Одночасно з цим формується сигнал *Load* для завантаження чергового слова даних (23 біт) у регістри лічильника. У цей же час за сигналом зі схеми управління і формування мікроконтроллер *μк* зчитує чергові 3 байти з буферу FIFO конвертора USB і передає їх на входи регістрів. Зображений на рис.1 лічильник насправді складається з шести 4-х розрядних лічильників з відповідними зв'язками. Для кодування максимального значення міжкрокового інтервалу достатньо 22 біта (4194304), що з урахуванням F_{gen} рівною 32 МГц відповідає максимальному значенню міжкрокового інтервалу =131 мсек. Цей режим відповідає мінімальній швидкості руху каретки 6,3 мм/сек. 23-й біт слова даних несе інформацію про напрямок руху каретки НАВКУ-3. Зчитаний 23-й біт використовується схемою управління та формування для генерації сигналу DIR. Особлива увага при використанні USB-конвертора на FT245R має бути зосереджена на забезпеченні синхронізації даних переданих з ПК та прийнятим мікроконтроллером *μк.*

1. О.А. Владимирьский, І.А. Владимирський, А.П. Іващенко, І.П. Криворучко. Розробка структури низькочастотної автоматизованої віброкалібрувальної установки НАВКУ-3. Моделювання та інформаційні технології. Збірник наукових праць. Інститут проблем моделювання в енергетиці НАН України. Вип. 89, Київ, 2019р.
2. Future Technology Devices International Ltd. FT245R USB FIFO IC Datasheet [Електронний ресурс]. – Режим доступу: https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://ftdichip.com/wp-content/uploads/2020/08/DS_UM245R.pdf.

С.С. Шевченко, С.Д. Вінничук

РОЛЬ АВТОМАТИЗОВАНИХ НАВЧАЛЬНИХ ПЛАТФОРМ У ЗАБЕЗПЕЧЕННІ СТІЙКОСТІ ДИНАМІЧНИХ СИСТЕМ ДО ЗОВНІШНІХ ЗМІН

У сучасних умовах складності й мінливості зовнішніх середовищ резильєнтність (стійкість та адаптивність) динамічних систем стає критичним фактором їхньої ефективності. Динамічні системи характеризуються постійними змінами параметрів під впливом внутрішніх і зовнішніх чинників, що вимагає розробки інноваційних підходів до їх стабілізації та адаптації.

Одним із перспективних рішень у цьому напрямку є впровадження автоматизованих навчально-тренувальних платформ (АНТП), які моделюють роботу технічних і організаційних систем у віртуальному просторі [1]. Ці платформи дозволяють навчати операторів і обслуговуючий персонал, тестувати сценарії роботи систем і прогнозувати поведінку в умовах відмов чи непередбачуваних ситуацій [2].

Основні переваги АНТП для забезпечення резильєнтності динамічних систем:

1. **Моделювання сценаріїв зовнішніх змін.**

АНТП здатні створювати віртуальні середовища, що імітують різні зовнішні впливи на систему, включно з аваріями, зростанням навантаження, збоєм компонентів або зміною умов експлуатації. Це дозволяє підготувати користувачів до роботи в реальних кризових ситуаціях.

2. **Адаптивне навчання.**

Використовуючи елементи штучного інтелекту, платформи можуть аналізувати прогрес користувачів і автоматично підлаштовувати складність завдань для ефективного навчання. Це сприяє розвитку критичного мислення та адаптації операторів до динамічних змін.

3. **Кооперативний підхід.**

АНТП надають можливість кільком користувачам одночасно вирішувати завдання у віртуальному просторі, покращуючи координацію та взаємодію команд у складних умовах.

4. **Цифрові двійники.**

Використання цифрових моделей реальних систем дозволяє точно відтворити їх поведінку в умовах впливу зовнішніх факторів. Це не лише сприяє прогнозуванню й тестуванню, але й дозволяє розробляти оптимальні стратегії реагування.

5. **Економічна ефективність.**

Навчання у віртуальному середовищі зменшує витрати на обладнання, матеріали та час, що особливо важливо для навчання роботи з високотехнологічною технікою.

Впровадження автоматизованих навчальних платформ сприяє розвитку стійкості динамічних систем до зовнішніх змін через навчання персоналу, оптимізацію управління, моделювання сценаріїв та аналіз цифрових двійників. Завдяки цьому динамічні системи стають не лише більш стійкими до викликів, але й здатними швидше адаптуватися до нових умов.

1. Інтерактивні автоматизовані дистанційні навчально-тренувальні системи як важлива ланка у резильєнтності критичної інфраструктури. Шевченко С.С., аспірант, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. Науково-практична конференція «резильєнтність критичної інфраструктури – 2023», 21 червня 2023 року.
2. Підвищення кваліфікації персоналу як засіб покращення безпеки енергетики у цифрову епоху. Шевченко С.С., аспірант, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. V науково- практична конференція «Безпека енергетики в епоху цифрової трансформації». 22 листопада 2023 року.

В.Д. Самойлов, А.О. Тарановський

ВДОСКОНАЛЕННЯ УСТАЛЕНИХ МЕТОДОЛОГІЙ ЗА ДОПОМОГОЮ ГЕНЕРАТИВНОГО ШТУЧНОГО ІНТЕЛЕКТУ НА ПРИКЛАДІ СИСТЕМ КОНТРОЛЮ ЗНАНЬ

Протягом десятиріч склалися та вийшли на плато методології обробки інформації з використанням комп'ютерних систем. За всіх їх переваг, притаманний їм високий ступінь формалізації лишає актуальним питання підвищення їх стійкості та адаптивності до змін, обумовлених властивостями природньої мови, формалізація якої має певні обмеження. Разом із тим, розвиток технологій на перетині обробки природньої мови та штучного інтелекту, особливо технологій так званого генеративного штучного інтелекту, демонструє здатність до подолання таких пов'язаних із формалізацією обмежень. Тоді, включення технологій генеративного штучного інтелекту до складу вже сталих методологій дозволило б підвищити стійкість та адаптивність до змін.

Так, ще до набуття обробкою природньої мови на основі великих мовних моделей вибухового характеру, висвітлювалося їх використання для генерування запитань до запропонованого фрагмента тексту у вигляді документа, абзацу або речення [1]. Цей підхід полягав у тому, що в якості вихідних даних для мовної моделі використовувався фрагмент тексту, в якому речення містили певні твердження, та до цього фрагменту генерувалися запитання, відповіді на які були закладені у цих твердженнях. При цьому, на відміну від поширених тепер засобів генеративного штучного інтелекту, використання таких мовних моделей у межах цього підходу поміж іншого вимагало значних організаційних й обчислювальних ресурсів, що саме по собі обумовлювало доволі високий поріг входження. Натомість широко доступні тепер засоби генеративного штучного інтелекту дозволяють нівелювати таку проблему ресурсоємності за умови отримання співставних результатів[1].

Ілюстративним тут може бути приклад включення технологій штучного інтелекту до методології генерування тестових завдань з використанням комп'ютерних систем, яка була запропонована більш ніж 20 років тому [2]. Визнаючи ефективність тестових завдань з точки зору контролю знань, в якості проблеми зазначалося, що складання таких завдань вимагає значного часу та інтенсивної праці. Натомість використання комп'ютерних систем пропонувалося як альтернатива, що дозволяла б вирішити цю проблему вимогливості до витраченого часу й докладених зусиль. Проте саме використання комп'ютерних систем як складова такої методології має певні

[1] Експериментальні дані використання доступних засобів генеративного штучного інтелекту у співставленні із висвітленими мовними моделями доступні за наступним посиланням: https://gist.github.com/taranowskiatpimee/fbe40dc2db0d87c4314e7edb2d291c54

обмеження, які могли б бути істотним чином зменшені за рахунок використання в якості такої складової технологій генеративного штучного інтелекту.

В найбільш загальних рисах, згадана методологія полягає в обробці текстів розповідального характеру в електронній формі (підручників, посібників тощо) за певною процедурою, яка дозволяє автоматизувати генерування запитань за такими текстами. Процедура пропонувалася з трьох етапів: (1) виокремлення ключового терміну; (2) підбір неправильних варіантів відповіді; (3) безпосереднє генерування запитання. До цих етапів процедури пропонувалися відповідні компоненти комп'ютерної системи.

Щодо першого етапу процедури увага акцентувалася на віднайденні ключових концепцій, охоплених текстом, на протиставлення другорядним й несуттєвим з точки зору предметної області. Віднайдені таким чином ключові терміни були покликані слугувати в подальшому так званими якорями для генерування запитань та одночасно правильними варіантами відповідей на такі згенеровані питання.

Щодо другого етапу процедури наголошувалося на важливості підбору таких неправильних варіантів відповіді, які б семантично були максимально наближеними до правильного варіанту відповіді та водночас не були б очевидно неправильними — не містили б підказки та не дозволяли б іншим чином визначити їх за неправильні варіанти безвідносно до наявності знань з поставленого питання. Такі семантично наближені неправильні варіанти відповіді дозволяють краще відокремити тих, хто є більш впевненим в предметній області з точки зору наявних знань від тих, кому притаманна невизначеність у цьому відношенні.

Щодо третього етапу процедури пропонувалося генерування запитань з використанням декларативних речень розповідального характеру шляхом застосування простих правил з перетворення, за якого передбачалися лише мінімальні зміни до первісних формулювань таких речень — шляхом примітивного перетворювання розповідного речення на питальне. Прямо за перевагу цього підходу визначалося збереження ясності й зрозумілості та уникнення додаткового ускладнення. Проте принаймні частково це пов'язано із особливостями англійської мови, які дозволяють реалізувати це в достатній мірі формалізовано для того, аби це було здійсненим з використанням комп'ютерних систем. Що лишає цей підхід прийнятним для використання англійською мовою, але залишає відкритим питання щодо його прийнятності для використання іншими мовами.

Навіть експерименти у першому наближенні та із застосуванням тільки найбільш поширених й доступних засобів генеративного штучного інтелекту[2] дозволяють вести мову про потенціал використання замість

[2] Експериментальні дані застосування засобів генеративного штучного інтелекту за процедурою автоматизації генерування запитань за поданими текстами доступні за наступним посиланням: https://gist.github.com/taranowskiatpimee/246a0754e7daaa5398a8e3603683d521

запропонованих первісно компонентів комп'ютерної системи для всіх етапів процедури у складі згаданої методології, а також про перспективи подальшого дослідження вдосконалення цієї методології у цьому напрямі.

Таке включення технологій генеративного штучного інтелекту до складу методології генерування тестових завдань потенційно дозволяє мати позитивний вплив на кожному з етапів процедури. Так, в частині виокремлення ключових термінів, це дозволяє зокрема відступити від визначення таких через частоту використання певних слів у тексті, що нерідко може призводити до викривлення результатів його визначення таким чином. В частині підбору неправильних варіантів відповіді, це дозволяє відмовитися від використання сторонніх ресурсів на кшталт згаданого в методології WordNet, використання якого потребує належного поводження із побічними ефектами, які це супроводжують. В частині безпосереднього генерування запитання, це дозволяє відійти від надмірної формалізації та надмірного спрощення, які значним чином звужують діапазон можливих результатів та можуть обумовлювати результати, що позбавлені сенсу.

В цілому ж, застосування засобів генеративного штучного інтелекту замість окреслених методологією компонентів комп'ютерної системи дозволяє зняти обмеження з використання цієї методології тільки для англійської мови та поширити її використання для інших мов, адже сучасні технології генеративного штучного інтелекту демонструють результати для тієї ж української мови, що є співставними із результатами для англійської мови, а також дозволяють істотним чином зменшити ризик так званих галюцинацій коли про обробку природньої мови йдеться за поданим фрагментом тексту [3].

Розглянутий приклад дозволяє дійти висновку про здатність технологій генеративного штучного інтелекту вивести на новий виток вдосконалення вже усталені методології, дозволяючи розглядати питання підвищення стійкості та адаптивності до змін охоплених ними процесів, принаймні у контексті обробки природньої мови.

1. Ushio, A., Alva-Manchego, F., & Camacho-Collados, J. (2022). Generative Language Models for Paragraph-Level Question Generation. In *Proceedings of the 2022 Conference on Empirical Methods in Natural Language Processing*. Association for Computational Linguistics. https://doi.org/10.18653/v1/2022.emnlp-main.42.
2. Mitkov, R., & Ha, L. A. (2003). Computer-aided generation of multiple-choice tests. In *Proceedings of the HLT-NAACL 03 workshop on Building educational applications using natural language processing*. Association for Computational Linguistics. https://doi.org/10.3115/1118894.1118897.
3. Тарановський А. О., & Самойлов В. Д. (2023). ChatGPT і можливість його використання для безекспертного створення тестів. *Електронне моделювання, 45(2),* 44–60. https://doi.org/10.15407/emodel.45.02.044.

A.V. Iatsyshyn, A.M. Lahoiko, O.P. Podliashchuk, Ie.V. Pylypchuk,
V.O. Kutsenko, Y.B. Krasnov

INTERNATIONAL AND NATIONAL ASPECTS OF REGULATING THE TRANSPORTATION OF DANGEROUS GOODS BY ROAD

The modern economy heavily relies on the transportation of hazardous substances such as fuel, chemicals, and toxic materials. The increasing volume of such goods transported by road elevates risks to the population, environment, and infrastructure, necessitating a clear regulatory framework to minimize these risks. Therefore, analyzing legal acts regulating the transportation of dangerous goods by road in international and national contexts is of paramount importance.

In [1], special attention is paid to the European Agreement concerning the International Carriage of Dangerous Goods by Road (ADR), which serves as a foundation for international regulations, updated periodically. Key Ukrainian legislative acts, including the laws "On the Transportation of Dangerous Goods" and "On Ukraine's Accession to ADR," as well as relevant resolutions of the Cabinet of Ministers of Ukraine, are also highlighted. These documents define requirements for the organization, safety, insurance, and training of personnel involved in the transportation of hazardous materials.

Studies [2-4] focus on legislative adaptations in the Republic of Korea to mitigate risks associated with hazardous chemicals, particularly through the Chemical Control Act. They emphasize the need to strengthen safety standards and chemical management, given the rising frequency of accidents in this field.

In the United States, attention is drawn to the role of the Department of Transportation through the Pipeline and Hazardous Materials Safety Administration (PHMSA), which regulates the transportation of dangerous goods. Topics such as classification, labeling, packaging, and personnel training under HMR regulations are discussed in [5]. These measures aim to minimize threats to life, property, and the environment.

Regulation within the European Union is presented through Directive 2008/68/EC, covering all modes of hazardous goods transportation and incorporating international agreements such as ADR, RID, and ADN. These standards impose stringent requirements for labeling, vehicle technical condition, and personnel training, ensuring a high level of safety [6, 7].

The Ukrainian context stands out due to numerous challenges, particularly frequent violations of regulations and risks associated with ongoing military actions. The necessity of strengthened control, the introduction of penalties for rule violations, and the adaptation of the legal framework to European standards is underscored. In [1], legislative amendments aimed at improving the transportation of dangerous goods are detailed, including requirements for labeling, insurance, and technical equipment for vehicles. Special attention is also given to ensuring safety during transportation under combat conditions, with additional measures such as the use of armored vehicles, specialized personnel training, and

international cooperation. Examples of countries employing military protection for dangerous goods transportation illustrate the need to adapt transportation methods to high-risk conditions.

The relevance of the topic is emphasized by the importance of harmonizing Ukrainian legislation with international standards to reduce ecological, social, and economic risks associated with the transportation of dangerous goods by road.

1. Lahoiko A., Podliashchuk O., Iatsyshyn A., Bandola O., Hromova I., Kontsydailo A. Features of Hazardous Cargo Transportation: Regulatory Framework and Modelling Tools. Systems, Decision and Control in Energy VII. Studies in Systems, Decision and Control. 2025 (in press).
2. Park J, Park S, Park H, Kwon H. A Brief Review of the Legal Definition of Chemical Accident under the Current Chemical Substances Control Act. Journal of Environmental Health Sciences. 2023. Vol. 49. 179-182. https://doi.org/10.5668/JEHS.2023.49.4.179.
3. Korea Toxic Chemicals Control Act (TCCA): https://www.cirs-reach.com/KoreaTCCA/Korea_Toxic_Chemicals_Control_Act_TCCA.html .
4. Korea CCA (Chemical Control Act): https://www.reach24h.com/en/service/chemical-service/korea-cca-chemical-control-act-compliance.html.
5. Hazardous Materials Regulations (2017). https://www.phmsa.dot.gov/standards-rulemaking/hazmat/hazardous-materials-regulations.
6. ADR 2023 - Agreement concerning the International Carriage of Dangerous Goods by Road (2023). https://unece.org/transport/standards/transport/dangerous-goods/adr-2023-agreement-concerning-international-carriage.
7. Directive 2008/68/EC of the European Parliament and of the Council of 24 September 2008 on the inland transport of dangerous goods (Text with EEA relevance) (2024) https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32008L0068.

З.Х. Борукаєв, В.А. Євдокімов, К.Б. Остапченко

АЛГОРИТМІЧНА МОДЕЛЬ АНАЛІЗУ ЦІНОВОЇ ДИНАМІКИ НА ОПТОВОМУ РИНКУ ЕЛЕКТРОЕНЕРГІЇ ДЛЯ ВИРІШЕННЯ ЗАВДАНЬ УПРАВЛІННЯ ПОПИТОМ

Основним завданням впровадження комп'ютерних систем у галузі енергетики є забезпечення фахівців необхідними даними для якісного і обґрунтованого ухвалення рішень, які ґрунтуються на використанні достовірної інформації про динаміку змін ключових показників функціонування ринку та забезпечують певною мірою мінімізацію ризиків впливу зовнішніх факторів на формування цін на ринку. Правильне прийняття рішень на різних рівнях управління забезпечує надійне та економічне функціонування енергопідприємств виробників електроенергії, активних споживачів та інших учасників ринку - постачальників енергії та допоміжних послуг, споживачів. Якщо класифікувати та ідентифікувати місце комп'ютерної системи моделювання в складі комплексу систем інформаційно-технологічного забезпечення процесів прийняття рішень в електроенергетиці, то вона є середовищем комп'ютерних моделей процесів функціонування енергетичних об'єктів ринкової структури [1].

Функція моделювання комп'ютерної системи обумовлює необхідність аналітичної обробки вхідних оперативних і ретроспективних даних функціонування суб'єктів і сегментів ринку з наступною підготовкою інформації для процесів оцінки і прогнозування показників діяльності. Однією із важливих комп'ютерних моделей оцінки процесів функціонування ринку є модель аналізу динаміки попиту на електроенергію на ціноутворюючих сегментах оптового ринку.

Розглянемо процес утворення моделі, який починається з визначення вхідних і вихідних змінних величин і параметрів моделі та формалізації критеріїв оцінки попиту. Відповідно до Правил ринку визначено наступні часові інтервали в організації процесу купівлі-продажу електроенергії: доба постачання - доба, в якій відбувається фізичне постачання обсягів електричної енергії, визначених за результатами торгів; розрахунковий період – мінімальний відрізок часу доби постачання (година), щодо якого визначено результати торгів (ціна та обсяги) на сегменті ринку. Вихідними даними аналізу динаміки розподілу купівлі-продажу електроенергії для оцінки попиту на оптовому ринку в розрізі часток сегментів ринку є наступні погодинні вхідні величини:

1) $q^{\text{РДД},k}(i,j)$ - обсяги продажу електроенергії в об'єднаної енергетичної системі (ОЕС) України та Енергетичному острові «Бурштинська ТЕС» (БуТЕС) на ринку двосторонніх договорів (РДД);

2) $q^{\text{РДН},k}(i,j)$ - акцептовані обсяги купівлі-продажу в ОЕС та БуТЕС на ринку «на добу наперед» (РДН);

3) $q^{\text{ВДР},k}(i,j)$ - акцептовані обсяги купівлі-продажу в ОЕС та БуТЕС на внутрішньодобовому ринку (ВДР);

4) $q^{\text{БР},k}(i,j)$ - обсяги балансуючої енергії «вгору» та «вниз» в ОЕС та БуТЕС на балансуючому ринку (БР);

5) $p^{\text{РДН},k}(i,j)$ - маржинальна ціна в ОЕС та БуТЕС на РДН.

Наведені позначення змінних обсягів і ціни узагальнено подаються наступним чином:

а) $q^{s,k}(i,j)$ – обсяг продажу на сегменті $s \in$ {РДД, РДН, ВДР, БР} у системі $k \in$ {ОЕС, БуТЕС}, що склався на аукціоні у розрахункову годину $j \in (1,24)$ доби постачання $i \in (01.01,\ldots,31.12)$;

б) $p^{\text{РДН},k}(i,j)\,\text{p}^{\text{s,k}}\text{(i,j)}$ – ціна продажу на сегменті s у системі k, що склався у годину j доби i.

Вважатимемо, що розглядається тільки маржинальна ціна на РДН у системі ОЕС, як визначальна (індикативна), за якою обчислюються всі цінові показники про витрати на допоміжні послуги у процесі виробництва, постачання і розподілу електроенергії у ОЕС.

Показниками оцінки попиту на оптовому ринку будемо вважати наступні вихідні величини, які позначимо наступним чином:

1) $\left\{v^s(n,j)\middle| j=\overline{1,24}, s \in (\text{РДД, РДН, ВДР, БР})\right\}$ - погодинні профілі середніх обсягів продажу електроенергії на сегментах ринку s за період постачання (сезонною ознакою) $n \in$ (рік, кліматичний період, місяць);

2) $\left\{w^s(n,j)\middle| j=\overline{1,24}, s \in (\text{РДД, РДН, ВДР, БР})\right\}$ - погодинні профілі відсотків (часток) середніх обсягів продажу електроенергії на сегментах ринку s за період постачання n;

3) $\left\{v^s(n)\middle| n \in (\text{рік, кліматичний період, місяць}), s \in (\text{РДД, РДН, ВДР, БР})\right\}$ - інтервальні (сезонні) профілі середніх (середньогодинних, середньодобових) обсягів продажу електроенергії на сегментах ринку s;

4) $\left\{w^s(n)\middle| n \in (\text{рік, кліматичний період, місяць}), s \in (\text{РДД, РДН, ВДР, БР})\right\}$ - інтервальні (сезонні) профілі відсотків (часток) середніх обсягів продажу електроенергії на сегментах ринку s;

5) $\left\{z^{\text{РДН}}(n,j)\middle| j=\overline{1,24}\right\}$ - погодинні профілі середньої (середньозваженої) ціни продажу електроенергії на РДН за сезонною ознакою n;

6) $\left\{z^{\text{РДН}}(n)\middle| n \in (\text{рік, кліматичний період, місяць})\right\}$ - інтервальні (сезонні) профілі середньої (середньозваженої) ціни продажу електроенергії на РДН.

Для оцінки попиту розрахунок профілів визначається наступними алгоритмами:

$$v^s(n,j)=\frac{1}{K(n)}\sum_{i\in S(n)}\left(q^{s,\text{ОЕС}}(i,j)+q^{s,\text{БуТЕС}}(i,j)\right),\ w^s(n,j)=\frac{v^s(n,j)}{\sum\limits_s v^s(n,j)},$$

$$v^s(n)=\sum_{j=1}^{24}v^s(n,j);\ w^s(n)=\frac{v^s(n)}{\sum\limits_s v^s(n)},$$

$$z^{\text{РДН}}(n,j)=\frac{\sum\limits_{i\in S(n)}p^{\text{РДН,ОЕС}}(i,j)\times q^{\text{РДН,ОЕС}}(i,j)}{\sum\limits_{i\in S(n)}q^{\text{РДН,ОЕС}}(i,j)},\quad z^{\text{РДН}}(n)=\frac{1}{24}\sum_{j=1}^{24}z^{\text{РДН}}(n,j),$$

де $S(n)$ – множина одиниць часу, що належать до інтервалу сезонності $n\in$(рік, зима, весна, літо, осінь, місяць), $K(n)=|S(n)|$ – кількість одиниць часу інтервалу.

В результаті використання алгоритмічної моделі надається можливість визначати наступні залежності: ціни купівлі-продажу (погодинну, інтервальну) від структури продажу електроенергії; загального обсягу (погодинного, інтервального) від структури продажу електроенергії.

Інтегрованим критерієм оцінки динаміки попиту в наведеній моделі визначено загальну (середньодобову) ціну електроенергії з урахуванням ціни на РДН, яка визначається за формулами:

$$Z(n)=\sum_s\sum_{j=1}^{24}\sum_{i\in S(n)}p^{\text{РДН,ОЕС}}(i,j)\times\left(q^{s,\text{ОЕС}}(i,j)+q^{s,\text{БуТЕС}}(i,j)\right),\ \tilde{Z}(n)=\frac{1}{K(n)}Z(n).$$

Для аналізу динаміки змін обсягів попиту на електроенергію на відповідних сегментах ринку та ціни на РДН використано модельні профілі за період з 2020 по 2021 роки [2]. А саме - погодинні середні обсяги і ціна продажу, посезонні середньогодинні обсяги і ціна продажу, річний середньогодинний обсяг і ціна продажу електричної енергії на сегментах ринку.

В таблиці наведені результати розрахунків відсоткових річних, сезонних профілів динаміки попиту на електроенергію, яка визначає структуру продажу та приріст ціни і обсягів для якісної оцінки залежностей цих основних показників функціонування оптовому ринку.

За річними, сезонними профілями можна встановити наступні тенденції у зміні структури продажу електроенергії на оптовому ринку – постійними компонентами є РДД до 70-75%, РДН до 25-30%, ВДР до 5%, а змінною (непостійною) компонентною є БР.

Прирости ціни та обсягу у цих профілях мають певну залежність у динаміці напряму зміни. Так, напрями зміни обсягу і ціни у поточному розрахунковому періоді постачання в цілому збігаються, але сповільнення спаду ціни поточного періоду (літо 2020р. у -2%) обумовлює зростання

обсягу наступного періоду (осінь 2020р. у 17%), а пришвидшення зростання ціни поточного періоду (зима 2021р. у 40%) обумовлює спадання обсягу наступного періоду (весна 2021р. у -15%). Наведені в таблиці результати ґрунтуються на погодинних значеннях шуканих величин. Їх короткий аналіз оціночно показав, що за погодинним профілем середніх обсягів у 2020 році для годин 1-16 частка БР складає 10-20%, що є орієнтовно половиною від частки РДН у 25-30%. Це може вказувати на «не ефективну» участь частини учасників аукціону РДН, внаслідок недостатньо якісного прогнозування тенденцій на ринку або наявність «коаліційної гри» деяких учасників ринку. Що було враховано у 2021 році і частка БР у погодинному розрізі вже склала 1-4%.

Таблиця 1 – Результати розрахунків алгоритмічної моделі

Профіль	Період постачання		Відсоток					
	Рік	Інтервал(сезон, година)	Обсяг РДД	Обсяг РДН	Обсяг ВДР	Обсяг БР	Приріст ціни	Приріст обсягу
Річний середньогодинний	2020		78,3%	27,4%	4,5%	-10,2%		
	2021		71,6%	25,2%	3,6%	-0,3%	39,3%	6,4%
Посезонний середньогодинний	2020	Зима	68,3%	30,8%	2,1%	-1,2%		
		Весна	79,6%	30,3%	4,7%	-14,7%	-7,1%	-24,5%
		Літо	89,4%	24,7%	6,1%	-20,3%	-2,2%	-10,6%
		Осінь	80,1%	22,7%	5,8%	-8,7%	14,9%	17,3%
	2021	Зима	69,5%	25,9%	2,9%	1,7%	40,6%	25,1%
		Весна	73,3%	23,3%	6,3%	-2,9%	-38,1%	-15,0%
		Літо	74,4%	23,9%	2,5%	-0,8%	26,9%	-8,5%
		Осінь	69,7%	27,4%	2,6%	0,3%	63,6%	7,5%

Результати розрахунків створюють основу для побудови комп'ютерних імітаційних моделей, які відображають залежності взаємопов'язаних динамічних потокорозподілів - обсягів та фінансів на всіх стадіях технологічного процесу виробництва, передачі і розподілу електроенергії.

1. Євдокимов, В. А., Борукаев, З. Х., & Остапченко, К. Б. (2024). Комп'ютерна система моделювання процесів ціноутворення на оптовому ринку електроенергії. *Технічна електродинаміка*, 2, 72-81. https://doi.org/10.15407/techned2024.02.072.
2. Результати торгів: Оператор ринку. https://www.oree.com.ua/index.php/control/results_mo/DAM.

В.А. Євдокімов, З.Х. Борукаєв, К.Б. Остапченко

МОДЕЛЬ РЕГІОНАЛЬНОГО ДЕЦЕНТРАЛІЗОВАНОГО РИНКУ ЕЛЕКТРОЕНЕРГІЇ ЯК СПОСІБ ПІДВИЩЕННЯ РЕЗИЛЬЄНТНОСТІ ЕНЕРГОСИСТЕМИ

Проектування ринку електроенергії є одним з основних інструментів Європейського Союзу для ефективного переходу до вуглецевої нейтральної енергетичної системи, яка залежить від чистої електроенергії. Правильно спроектовані ринки електроенергії можуть стимулювати впровадження екологічно чистих енергетичних технологій, включаючи потужності відновлюваних джерел енергії, та гнучкі модульні станції, необхідні для їх підтримки, тим самим зберігаючи безпеку постачання. Окрім цього, на сьогодні постає питання при проектуванні дизайну ринку електричної енергії враховувати дії в умовах мілітарного впливу (гібридних воїн), коли на енергетичну систему здійснюється цілеспрямовані удари на руйнування об'єктів енергетики. Тому, при проектування енергосистеми необхідно враховувати не тільки фактори природнього чи техногенного характеру, але і загроз гібридного характеру, які можуть спричинити наслідки, від перебоїв у електропостачанні до хронічного недопостачання електричної енергії.

Резильєнтність енергетичної системи – це її властивість, яка забезпечує здатність передбачати, готуватися та адаптуватися до мінливих умов, а також протистояти, реагувати та швидко відновлюватися після збоїв за допомогою адаптивного та цілісного планування, організаційно-технологічних та технічних рішень. Це все потребує створенню принципово нових критеріїв забезпечення надійності електропостачання, що в свою чергу призводить до пошуку нових організаційно-технологічних рішень, тобто такої енергосистеми, потенційні масштаби ураження якої є суттєво обмеженими, а наслідки ураження ліквідуються значно швидше ніж в сьогоднішніх умовах.

Технологічно вироблена електрична енергія з відновлювальних джерел енергії в межах локальної (розподільчої) мережі, споживається споживачами цієї ж самої мережі, що може забезпечити критерії надійності електропостачання. Враховуючи факт зростання виробленої енергії з відновлювальних джерел енергії, можна дійти до висновку, що потрібен новий підхід до децентралізації ринку на регіональному рівні.

Встановлено, що децентралізацію можливо реалізувати за рахунок використання власного ресурсного потенціалу регіонального рівня. Тобто, в кожній регіональній енергосистемі має бути встановлений такий обсяг генераторів СЕС, ВЕС, малих модульних станцій та систем зберігання енергії, які забезпечують потреби в електроенергії, що сукупно споживається населенням, житлово-комунальними господарствами, транспортом та сільським господарством виділеного регіону. Забезпечення електроенергією власного регіонального виробництва зазначених категорій споживачів

дозволяє максимально убезпечити життєдіяльність кожного регіону від впливу руйнівних дій на загальнодержавну енергосистему України.

В такому разі, централізований рівень підтримує регіональні енергосистеми узгодженими обсягами маневрових потужностей і їх резерву та забезпечує постачання електроенергії підприємствам промислової, будівельної, транспортної та іншим видам економічної діяльності. У випадках руйнування окремих регіональних енергосистем загальнодержавна енергосистема України забезпечує нагальні потреби таких регіонів в електроенергії.

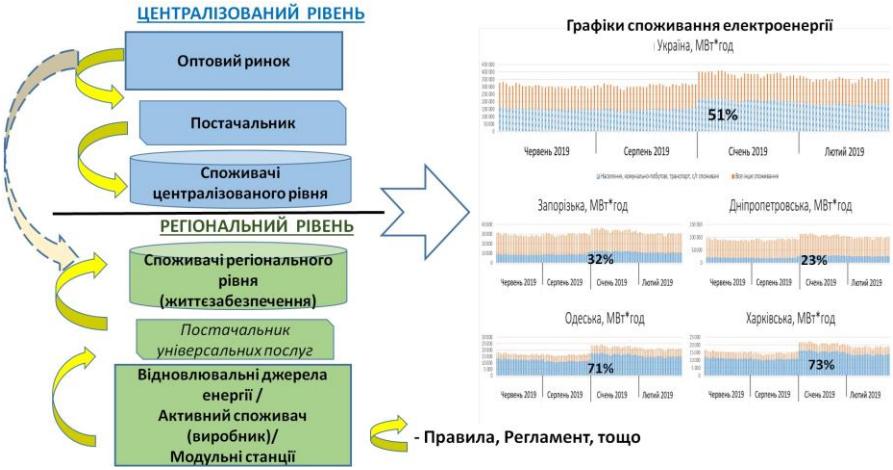


Рисунок 1 – Модель децентралізованого ринку

Засобом досягнення і реалізації властивості резильєнтності децентралізованої системи є побудова інформаційно-аналітичного середовища [1] для дослідження особливостей взаємодії учасників ринку, органів виконавчої влади та регулятора, а також для інформаційного забезпечення розробки модельних інструментів, які призначені для ефективного переходу до вуглецево-нейтральної енергетичної системи, яка залежить від розвитку чистої електроенергії та можливих дій в умовах мілітарного впливу.

Модельним інструментом у пропонованому інформаційно-аналітичному середовищі стала програмно-апаратна комп'ютерна система моделювання під назвою Equant [2], яка побудована із використанням веб-технологій та уніфікованого візуального інтерфейсу модельних інструментів. Основою цієї системи є збір, збереження та обробка вихідної інформації, що може бути використана для побудові різних модельних інструментів - імітаційних, розрахункових, прогнозних моделей.

Вхідні дані в автоматичному режимі поступають на сервер системи в залежності від часу їх актуалізації – погодинно, щоденно та щомісячно. Інформація надходить із майже 56 джерел або сайтів, що дає можливість формувати масиви даних не тільки актуальних, а й ретроспективних даних для рішення задач прогнозування.

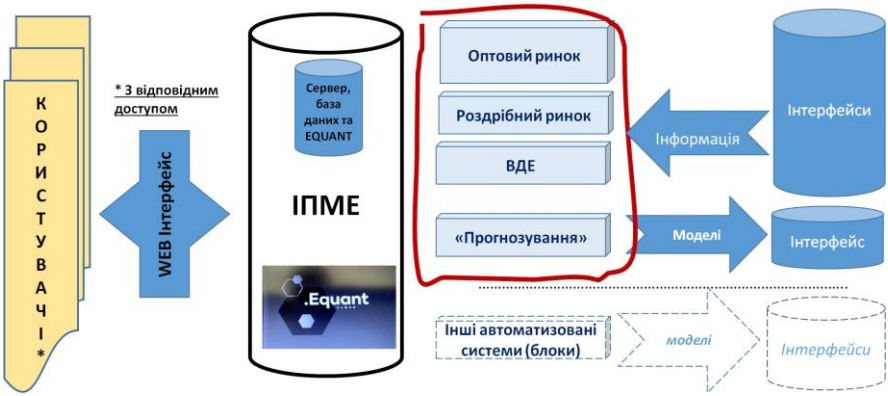


Рисунок 2 – Технологічна схема інформаційно-аналітичного середовища

Функціонал системи підтримує інформаційні потреби її користувачів про основні показники ринку електричної енергії та їх візуалізоване подання, серед них:

- середньозважені ціна на ринку на добу наперед України та сусідніх держав;
- стан роботи блоків теплових станцій, теплоцентралей та атомних станцій;
- актуальна інформація прогнозованого балансу виробництва електроенергії на рік, а також інформація по термінах виходу обладнання генерації в ремонти;
- тарифи на роздрібному ринку із актуальною інформацією по учасниках цього ринку, а також посилання на нормативного акту, який впроваджував такі тарифи;
- прогнозування цін на сегменту ринку на добу наперед на основі використання прогностичної моделі, яка розроблена с використанням штучних нейронних мереж;
- та інші дані, про що свідчить відкритість системи до подальшого розвитку за рахунок включення до його складу нових модельних інструментів.

Основними користувачами такої системи, окрім учасників ринку, таких як Енергоатом, ДТЕК, є органи виконавчої влади, такі як Міненерго, НКРЕКП та інші, а також науковці, які можуть використовувати систему, як

середовище для модельних інструментів побудови імітаційних та сценарних моделей поведінки.

1. Остапченко, К. Б., Лісовиченко, О. І., Євдокимов, В. А., & Борукаев, З. Х. (2021). Створення інформаційно-моделюючої системи аналізу процесів ціноутворення на ринку електричної енергії. *Електронне моделювання*, 43(4), 51-68. https://doi.org/10.15407/emodel.43.04.051.
2. Євдокимов, В. А., Борукаев, З. Х., & Остапченко, К. Б. (2024). Комп'ютерна система моделювання процесів ціноутворення на оптовому ринку електроенергії. *Технічна електродинаміка*, 2, 72-81. https://doi.org/10.15407/techned2024.02.072.

О.Ю. Будякова

БІОЕКОНОМІЧНА РЕЗИЛЬЄНТНІСТЬ В КОНТЕКСТІ АДАПТАЦІЇ ЕКОСИСТЕМ

Війна кардинально вплинула на суспільство, економіку, інфраструктуру, екосистему України. Військове вторгнення руйнує природні екосистеми, втрачається біорізноманіття, забруднюються та отруюються токсичними речовинами ґрунти, вода, повітря, що в свою чергу впливає на здоров'я населення. Ризик невиконання Україною поставлених кліматичних цілей та зниження сільськогосподарського виробництва й як наслідок ризики для продовольчої безпеки обумовлюють пошук концепцій, здатних забезпечити резильєнтність в контексті адаптації екосистем.

Резильєнтність і стійкість являють собою дві унікальні концепції у безпековому домені, що визначають динаміку функціонування як природних, так і антропогенних систем в умовах зовнішніх впливів і внутрішніх змін [1].

Резильєнтність, на відміну від традиційного розуміння стійкості, акцентує увагу на «здатності системи передбачати, витримувати, відновлюватися та адаптуватися» [2, 3] у відповідь на значні збурення та непередбачувані зміни, що є особливо актуальним у контексті нелінійних динамічних систем. Резильєнтність, на відміну від стійкості, не просто має на увазі здатність системи зберігати свій початковий стан в умовах зовнішніх збурень, а й охоплює її адаптивну здатність до еволюції і переходу на нові рівні функціонування у відповідь на ці збурення. Таким чином, резильєнтні системи мають гнучкість, що дає їм змогу не тільки відновлюватися після непередбачуваних подій, а й отримувати з цих подій користь, стимулюючи розвиток і поліпшення своїх функціональних механізмів [1].

Це підкреслює адекватність і доречність спрямування на резильєнтність як цільового вектора в стратегіях управління безпекою. Визнання динамічного та нелінійного характеру безпекового ландшафту вимагає від системи не тільки стійкості, а й здатності до гнучкого реагування, адаптації і розвитку у відповідь на мінливі умови. Резильєнтність, у цьому контексті, стає не лише реактивною здатністю до відновлення, а й проактивним процесом безперервного самовдосконалення та еволюції, що забезпечує системі довгострокове виживання та ефективність в умовах непередбачуваних і мінливих загроз [1].

Резилієнтність спільнот, організацій, екосистем – це їхня здатність протистояти кризам, виживати та розвиватися у посткризових умовах. Резилієнтність доцільно визначити як послідовну та взаємопов'язану здатність системи, по-перше, поглинати потрясіння, уникаючи власної подальшої деградації; по-друге, реорганізовуватися для підтримки своїх внутрішніх структур та збереження функцій; по-третє, зберігати простір для позитивних трансформацій та розвитку, структурних і поведінкових змін, що

дає змогу не лише відновлюватися, але й виходити після шоків та потрясінь на вищий рівень розвитку [4].

Резилієнтність екологічних систем – це дещо інше, ніж їх стійкість або стабільність. Резилієнтність виникає завдяки кумулятивним ефектам, циклам зворотного зв'язку та динамічним рухам. Вона пов'язана з можливостями оновлення, рекомбінації процесів і появою нових траєкторій розвитку системи. Отже, резилієнтність включає такі основні системні можливості, як поглинання, адаптація й трансформація [5].

Сучасні економічні теорії в парадигмі сталого розвитку передбачають економічний розвиток, соціальну стійкість та екологічну сталість.

Біоекономіка є парадигмою та інструментом досягнення цілей сталого розвитку [6].

Біоекономіка пропонує сталі рішення для підвищення резильєнтності та адаптації екосистем до військового екоциду під час воєнного стану та повоєнного відновлення України.

Концепція біоекономіки фокусується на заміні викопних ресурсів та сталому використанні біологічних ресурсів (біомаси), мінімізації відходів на принципах циркулярної економіки (рециклінгу) та негативного впливу на навколишнє середовище (збереженні природних екосистем).

Біоекономіка охоплює знання, дослідження, технології та інновації, пов'язані з виробництвом біологічних ресурсів. Попри те, що біоекономіка вимагає впровадження передових технологій та інновацій, основним двигуном є біорізноманіття [7]. Оскільки біорізноманіття впливає на здатність біологічних систем до адаптації та змін у мінливому середовищі, біологічне різноманіття особливо важливе для резильєнтності екосистем.

За останні кілька років концепція біоекономіки набула популярності в усьому світі. Біоекономіка вирішує багато глобальних проблем сталого розвитку.

Людство стикається з глобальними проблемами, включаючи зміну клімату, продовольчу кризу та ін. Біоекономіка готова відігравати центральну роль у вирішенні цих проблем, зокрема забезпечення продовольчої безпеки [8]. Біоекономіка є перспективним вирішенням проблеми зміни клімату [9]. Біоекономіка як вектор інклюзивного економічного розвитку дозволяє розробити сталі та інклюзивні бізнес-моделі, які розширять можливості первинних виробників та інших учасників ланцюгів постачання та створення доданої вартості, модифікувати кліматичні та екологічні проблеми на можливості збільшувати та диверсифікувати доходи та створювати нові робочі місця [10].

Біоекономіка передбачає принципи циркулярної економіки, тобто ланцюги доданої вартості утворюють замкнуті цикли, в яких відходи призначені для утилізації та переробки. Біоекономіка на циркулярній основі базується на фундаментальних принципах повторного використання продуктів та матеріалів, усунення відходів та викидів в атмосферу із циклу та відтворення природних екосистем. Це зменшує споживання ресурсів за

рахунок використання відходів та викидів в атмосферу, водночас створюючи нову додану вартість з речей, які раніше визначались відходами. Розвиток біоекономіки на циркулярній основі також створює нові ланцюжки доданої вартості та дають можливість виробляти нові продукти з відходів, формує нові сфери економіки та нові робочі місця.

Екосистеми надають послуги, які підтримують глобальну цивілізацію. Навколишнє середовище контролює кліматичні умови та регулює клімат, управляє природними процесами очищення повітря, генерації води, стабілізації ґрунту тощо та задовольняє фундаментальні потреби людей.

Екосистемні послуги, або структури та функції екосистем, необхідні для підтримання економіки, здоров'я та добробуту суспільства. Для безпечного функціонування екосистемні послуги повинні бути диверсифіковані. Економічна діяльність, яка забезпечує екосистемні послуги, включає такі сфери: сільське господарство, тваринництво, енергетику, будівництво, промисловість тощо. На додаток до забезпечення продовольства та продуктів харчування, біоекономіка спрямована на збільшення сільськогосподарського виробництва непродовольчих товарів, таких як біоенергія та біоматеріали для заміни викопних ресурсів. Тому, для того, щоб не поставити під загрозу ресурсозберігаючі цілі, виробництво біомаси повинно відповідати принципам ефективності використання ресурсів.

Біоекономіка надає можливість розвитку екосистемних послуг для різних сфер бізнесу в таких галузях як енергетика, будівництво, туризм, рекреація, культура та здоров'я людей тощо.

Екосистемні послуги з розвитком біоекономіки відкривають нові перспективи: децентралізоване виробництво біоенергії, будівництво з біоматеріалів потребують ресурси біомаси, управління ландшафтами, на кшталт, включення зелених насаджень в екологічно свідомий дизайн у архітектурі нового будівництва, передбачає розширення біорізноманіття. Отже, розвиток біоекономіки розширює та забезпечує екосистемні послуги.

Галузі промисловості, які можуть отримати резильєнтність завдяки розвитку біоекономіки з використанням біотехнологій, включають біохімічний сектор, харчову, фармацевтичну, лісову промисловість та виробництво товарів з деревини, легку промисловість, виробництво біорозкладних матеріалів, фільтрацію води тощо.

Отже, концепція біоекономіки виникла як перспектива для вирішення проблем, пов'язаних з виснаженням викопних ресурсів, утворенням відходів, деградацією навколишнього середовища та збереження й адаптації екосистем. Біоекономіка зосереджена на сталому використанні біологічних ресурсів для виробництва товарів та послуг з одночасною мінімізацією негативних наслідків природним екосистемам.

Стала біоекономіка на циркулярній основі пропонує величезний потенціал для переходу до більш стійкої та резильєнтної економіки через створення ресурсних циклів, зменшення залежності від невідновлюваних ресурсів та застосовування цілісного та регенеративного підходу. Стала

біоекономіка визнає фундаментальну важливість збереження природних екосистем у досягненні своїх цілей.

Російська агресія в Україні впливає на усі виміри сталого розвитку суспільства: економічний розвиток, соціальну стійкість та екологічну сталість. Економіка, соціальна складова та екологічний стан України потребує комплексного підходу вирішення проблем безпеки під час воєнного стану та в перспективі повоєнного відновлення. Руйнування екосистем, зменшення біорізноманіття, забруднення та отруєння ґрунтів, води та повітря вимагає нових підходів, які резильєнтні в контексті адаптації екосистем. Біоекономіка пропонує рішення, які в повоєнній перспективі здатні відновити природні екосистеми до безпечного стану.

1. Мохор, В. В., & Коробейніков, Ф. О. (2024). Стійкість і резильєнтність у безпековому домені. *Реєстрація, зберігання і обробка даних*, *26*(1), 113-120. DOI: https://doi.org/10.35681/1560-9189.2024.26.1.308655.
2. NIST Special Publication 800-160, Volume 2. Developing cyber-resilient systems: A systems security engineering approach. Official edition. National Institute of Standards and Technology, 2021. 254 p. https://doi.org/10.6028/NIST.SP.800-160v2r1.
3. Korobeynikov, F. (2023). Resilience Paradigm Development In The Security Domain. *Electronic Modeling*, *45*(4), 88–111. DOI: https://doi.org/10.15407/emodel.45.04.088
4. *Напрями повоєнного відновлення довкілля та забезпечення резилієнтності екосистем* : монографія / за наук. ред. акад. НАН України Е. М. Лібанової. Київ : Інститут демографії та проблем якості життя НАН України, 2023, 249 с.
5. Хвесик, М. А., & Мандзик В. М. (2024). Концепція екологічної резилієнтності в управлінні водними ресурсами: повоєнні перспективи. *Природа в окупації – 10 років російської військової агресії проти довкілля. Перспективи відновлення природоохоронних територій України:* збірка матеріалів Всеукраїнської науково-практичної конференції (м. Хмельницький, 28-29 березня 2024 р.) – К. : Центр екологічної освіти та інформації, 113-115.
6. *Зелена трансформація та стала біоекономіка* : монографія / за наук. ред. А. А. Олешко, О. Ю. Будякової. Київ : КНУТД, 2024, 497 с. DOI 10.30857/978.617.7763.34.4 https://er.knutd.edu.ua/handle/123456789/27008.
7. Anikwe, M. A. N., & Ife, K. (2023). The role of soil ecosystem services in the circular bioeconomy. Frontiers in Soil Science, 3, 1209100.
8. Будякова, О.Ю., & Дьяконов, І.О. (2023). Біоекономіка: перспективи розвитку агропромислового комплексу України для подолання продовольчої кризи. *Цифрова економіка та економічна безпека, 6*(06), 68-74. DOI: https://doi.org/10.32782/dees.6-13.
9. Будякова, О. Ю. (2024). Біоекономіка як перспективне вирішення проблеми зміни клімату . *Здобутки економіки: перспективи та інновації*, (10). https://doi.org/10.5281/zenodo.13924099.
10. Будякова, О.Ю. (2023). Біоекономіка як вектор інклюзивного економічного розвитку в формуванні людського капіталу. *Цифрова економіка та економічна безпека, 9*(09), 68-77. DOI: 10.32782/dees.9-12.

STRATEGIES FOR ENSURING ENERGY SYSTEM RESILIENCE IN THE CONTEXT OF RENEWABLE ENERGY INTEGRATION

Abstract. The integration of renewable energy sources (RES) into power systems offers significant benefits for sustainability but also introduces challenges related to variability, uncertainty, and the resilience of the energy infrastructure. This study explores advanced strategies and technologies to enhance the resilience of energy systems, emphasizing mobile energy storage systems (MESS), distributed energy resources (DER), and artificial intelligence (AI)-driven monitoring and adaptation solutions. The findings highlight the interconnected roles of economic, environmental, and technological factors in achieving resilient energy systems.

Introduction. The global shift towards renewable energy sources (RES) is essential for mitigating climate change and achieving sustainability goals. However, the integration of RES poses challenges to the resilience of power systems due to their inherent variability and susceptibility to extreme events. Resilient energy systems are crucial to ensure stable operations, minimize disruptions, and adapt to adverse conditions. This paper examines advanced resilience strategies, focusing on mobile energy storage systems (MESS), distributed energy resources (DER), and AI-enabled solutions as pivotal tools in addressing these challenges.

Methods. This study employs a systematic review and analysis of existing resilience strategies in energy systems, with data synthesized from recent publications and case studies. Key methodologies include:

1. Evaluation of resilience metrics for energy systems, incorporating probabilistic models and real-time optimization [1].
2. Analysis of mobile and distributed energy solutions using Mixed-Integer Linear Programming (MILP) for cost and resilience trade-offs [2].
3. Review of AI-driven anomaly detection frameworks for monitoring and adapting to disruptions in energy networks [3].

Results and Discussion

Mobile Energy Storage Systems (MESS) and Distributed Energy Resources (DER). MESS and DER play a critical role in mitigating the impact of disruptions. Studies show that pre-positioning MESS in strategic locations significantly reduces expected load curtailment during extreme events [4]. Integration with DER enhances operational flexibility, enabling local energy supply during outages and minimizing dependence on centralized infrastructure [5].

Artificial Intelligence in Resilience Enhancement. AI-driven anomaly detection and prediction systems improve real-time monitoring and decision-making, allowing systems to address potential disruptions preemptively. Machine

learning models, such as LSTM and reinforcement learning algorithms, effectively optimize resource allocation under uncertainty [6].

Economic and Environmental Implications. The adoption of resilience strategies, such as DER and MESS, reduces recovery times and operational costs while supporting decarbonization goals. Optimization models indicate that these technologies contribute to both economic resilience and environmental sustainability by reducing dependency on fossil fuels [7].

Conclusion. Enhancing the resilience of energy systems in the context of renewable energy integration requires a multifaceted approach. Mobile and distributed energy solutions and AI-driven technologies are pivotal in building adaptive, cost-effective, and sustainable energy infrastructures. Policymakers and industry stakeholders should prioritize these strategies to ensure robust energy systems capable of withstanding future challenges.

1. Jesse, B.-J., Kramer, G. J., & Koning, V. (2024). Characterization of necessary elements for a definition of resilience for the energy system. *Energy, Sustainability and Society*, 14(1), 46. https://doi.org/10.1186/s13705-024-00478-9.
2. Rajabzadeh, M., & Kalantar, M. (2024). Enhancing resilience of distribution systems: Integrating mobile energy storage systems and information gap decision theory for uncertainty management. *Journal of Energy Storage*, 102, 113996. https://doi.org/10.1016/j.est.2024.113996.
3. Aghazadeh Ardebili, A., et al. (2024). Enhancing resilience in complex energy systems through real-time anomaly detection: A systematic literature review. *Energy Informatics*, 7(1), 96. https://doi.org/10.1186/s42162-024-00401-8.
4. Gautam, M., & Benidris, M. (2023). A graph theory and coalitional game theory-based pre-positioning of movable energy resources for enhanced distribution system resilience. *Sustainable Energy, Grids and Networks*, 35, 101095. https://doi.org/10.1016/j.segan.2023.101095.
5. Shafiei, K., et al. (2024). Planning for a network system with renewable resources and battery energy storage, focused on enhancing resilience. *Journal of Energy Storage*, 87, 111339. https://doi.org/10.1016/j.est.2024.111339.
6. Massel, L., et al. (2023). Assessment of the energy systems resilience using artificial intelligence methods. *E3S Web of Conferences, 470*, 01044. https://doi.org/10.1051/e3sconf/202347001044.
7. Yazdanie, M., et al. (2025). Strengthening energy system resilience planning under uncertainty by minimizing regret. *Renewable and Sustainable Energy Transition*, 6, 100093. https://doi.org/10.1016/j.rset.2024.100093.

V.O. Artemchuk

ENHANCING ENERGY SYSTEM RESILIENCE THROUGH ADVANCED TECHNOLOGICAL AND POLICY INTERVENTIONS

Abstract. The resilience of energy systems is critical for ensuring reliable energy supply amidst increasing challenges from climate change, natural disasters, and cyber threats. This study investigates the role of emerging technologies, such as edge computing, artificial intelligence (AI), and distributed energy resources (DER), alongside policy interventions in enhancing energy system resilience. Findings highlight the necessity of integrated approaches combining technical, economic, and regulatory measures to build adaptive and sustainable energy infrastructures.

Introduction. Energy systems worldwide face mounting challenges, including extreme weather events, rising energy demands, and the transition to renewable energy sources. Resilience is essential for these systems to adapt and recover from disruptions. Advanced technologies like edge computing and AI, paired with robust policy frameworks, can significantly enhance the resilience of energy systems. This paper explores these solutions and their implementation to address current and future challenges.

Methods. The research employs a mixed-methods approach, integrating:

1. Review of resilience-oriented frameworks incorporating emerging technologies such as edge computing and AI [1].

2. Case studies analyzing the role of distributed energy resources (DER) and mobile energy systems in enhancing operational flexibility [2].

3. Examination of policy interventions supporting energy resilience, including regulatory frameworks and incentive programs for renewable energy integration [3].

Results and Discussion.

1. Technological Interventions

1.1. Edge Computing and AI. Edge computing enables real-time data processing and decision-making, enhancing the operational resilience of energy systems [4]. AI-driven algorithms improve predictive maintenance and resource optimization, reducing downtime during disruptions [5].

1.2. Distributed Energy Resources (DER). DER enhances localized energy generation and distribution, reducing the dependency on centralized systems and providing critical support during outages [6].

2. Policy Interventions

2.1. Regulatory Frameworks. Policies promoting the adoption of DER and advanced technologies, such as tax incentives and subsidies for renewable energy systems, are crucial for fostering resilience [7].

2.2. Resilience Metrics and Standards. Establishing standardized resilience metrics aids in benchmarking and improving system performance under varying conditions [8].

3. Integrated Approaches

The combined application of technological and policy interventions shows significant potential in building adaptive and resilient energy systems. Case studies demonstrate reduced recovery times and improved reliability through the integration of edge computing, DER, and supportive policies.

Conclusion. Energy system resilience demands a holistic approach integrating advanced technological solutions and supportive policy frameworks. Edge computing, AI, and DER play a pivotal role in enhancing resilience, while policy interventions ensure the widespread adoption and integration of these technologies. Future efforts should focus on standardizing resilience metrics and fostering global collaboration to address the evolving challenges of energy systems.

1. Fiondella, L., Hogewood, L., Ligo, A., & Linkov, I. (2024). Edge computing as an enabler of energy and water system resilience. *IEEE Engineering Management Review, 52*(1), 28-42. https://doi.org/10.1109/EMR.2023.3320876.
2. Chen, C.-I., et al. (2024). Enhancement of system resilience for islanded microgrid with clean energy. *E3S Web of Conferences, 521*, 01005. https://doi.org/10.1051/e3sconf/202452101005.
3. Bui, T.-D., et al. (2024). Assessing energy resilience under uncertainty in Taiwan: System response ability and energy sufficiency. *Energy Strategy Reviews, 53*, 101403. https://doi.org/10.1016/j.esr.2024.101403.
4. Aghazadeh Ardebili, A., et al. (2024). Enhancing resilience in complex energy systems through real-time anomaly detection: A systematic literature review. *Energy Informatics, 7*(1), 96. https://doi.org/10.1186/s42162-024-00401-8.
5. Massel, L., et al. (2023). Assessment of the energy systems resilience using artificial intelligence methods. *E3S Web of Conferences, 470*, 01044. https://doi.org/10.1051/e3sconf/202347001044.
6. Shafiei, K., et al. (2024). Planning for a network system with renewable resources and battery energy storage, focused on enhancing resilience. *Journal of Energy Storage, 87*, 111339. https://doi.org/10.1016/j.est.2024.111339.
7. Taghavi, A., et al. (2025). A resilience-oriented approach to integrated energy management systems: Addressing energy conversion unit unavailability and cost efficiency. *Energy Conversion and Management, 325*, 119291. https://doi.org/10.1016/j.enconman.2024.119291.
8. Lotze, J., et al. (2024). On resilience of future decarbonized energy systems in Europe. *IET Conference Proceedings, 2024*(2), 83-88. https://doi.org/10.1049/icp.2024.1822.

O.O. Tsypliak, V.O. Artemchuk

LARGE LANGUAGE MODELS IMPACT ONTO GATED COMMUNITIES SOCIAL MEDIA RESILIENCE

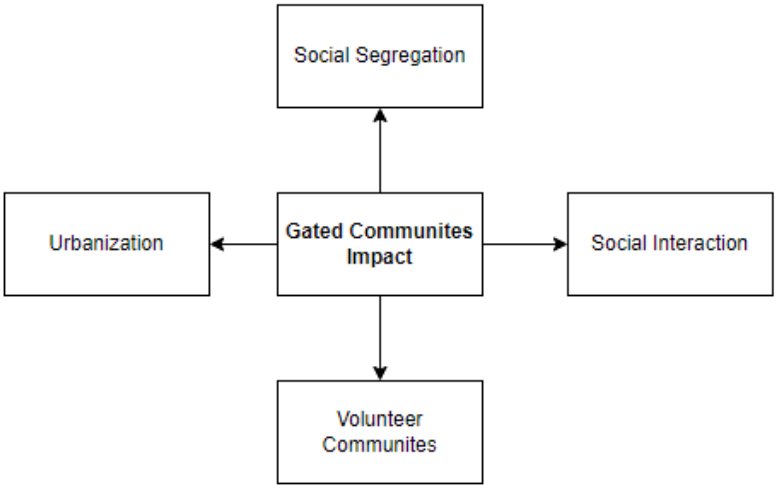
Urbanism as sociology segment that studies towns and cites more than two decades ago started the discussion about “gated communities”. [1] Meaning social and organizational communities behind some large residence places separated from outer town by a gate in some form. [2]

In modern Ukraine clear example of gated communities can be smaller like:

- Modern housing estates/complexes
- Old courtyard framed by soviet period multi-apartment building

Or larger like villages or small towns logistically separated from neighborhoods. The idea remains the same large group of people who are majorly hardly acquainted with each other have to live together, obviously having common problems, interests and shared resources like yards or parking spots to use.

Sociology studies phenomenon of gated communities as a one of the most common modern social self-organization that got significant impact onto the way modern cities grow and develop. (see picture 1) On the other hand the resilience of such community is a key to higher live quality of all residents.



Picture 1 – Gated Communities Impact

Modern generative artificial intelligence (AI) after recent economical grown in 2021 impacted many areas of modern economy [3]. During following years AI investments into majority of areas decreased dramatically, but one of exceptional

areas is social medias that keep engaging more and AI investments every years showing significant grows larger than other areas.

There are many studies showing demonstrating tools for text summarization and automated analysis [4]. Only the matter of time when new tools in social medias will appear that will dramatically impact the way people communicate each other in gated communities.

The way modern social networks are designed is far beyond just digitalizing physical group meeting, that were out to resolve common problems of some gated communities. [5] Social medias like Facebook and Twitter impacted the way people communicate overall.

Nowadays “Private Groups” of a yard or housing complex in Viber or Telegram is not only a platform for discussion, its also a storage of a lot of data that single participant willingly shares about oneself via messages available to big group of people.

All these data are stored social media hosting side, and assured to be secure. But in fact these data may got leak even though single stollen personal account of a group participant or using bots [6]. And considering modern generative AI as a fruit of large language models development[7] all this data can be used in multiple possible harmful ways for social medias users from certain gated communities, for example to design unwanted advertisements or share personal profile with a third parties.

In conclusion, gated community is a form of residence self-organization that started as digitalized platforms to discuss problems and be used for socialization. Consequence of such digitalization of last decades resulted into low unsecured private groups contains a lot of sensitive personal information that can be used to harm social media users from gated communities.

To remain resistant and transparent such groups should be considered as source of personal information leak that considering modern generative AI progress can be used against social media users as cheap as never before. How this process can be prevented using cybersecurity or social engineering is a subject of further studies.

1. Lang, R. E., & Danielsen, K. A. (1997). Gated communities in America: Walling out the world? Housing Policy Debate, 8(4), 867–899. https://doi.org/10.1080/10511482.1997.9521281.
2. Low, S. M. (2004). Behind the gates: Life, security, and the pursuit of happiness in fortress America (1st Routledge paperback ed.). Routledge. Originally published: 2003. ISBN: 9780415944380.
3. Tsypliak, O., & Artemchuk, V. (2024). Generative AI text summarization performance analysis prospects. Modeling, Control and Information Technologies: Proceedings of International Scientific and Practical Conference, (7), 132–135. https://doi.org/10.31713/MCIT.2024.037.
4. Tsypliak, Oleksandr, and Volodymyr Artemchuk. “Console Application Development for Articles` Highlights Generation Based on Artificial Intelligence

Designed Using Autonomous Large Language Model." In Information Technology for Education, Science, and Technics, 53–64. Springer NatureSwitzerland, 2024. https://doi.org/10.1007/978-3-03 1-71801-4_5.

5. BeerBergman. (2014, November). Building gated communities: Freedom and social media. Retrieved December 20, 2024, from https://medium.com/@BeerBergman/building-gated-communities-3dfeb012b8b8.
6. Thales Group. (2024, April). Bots now make up nearly half of all internet traffic globally. Retrieved December 20, 2024, from https://www.thalesgroup.com/en/worldwide/security/press_release/bots-now-make-nearly-half-all-internet-traffic-globally.
7. S. Minaee, T. Mikolov, N. Nikzad, M. Chenaghlu, R. Socher, X. Amatriain, J. Gao, Large language models: A survey, 2024. doi:10.48550/ARXIV.2402.06196.

В.В. Годлюк

АЛГОРИТМИ ІДЕНТИФІКАЦІЇ АНОМАЛІЙ У ДИНАМІЧНИХ ЦИФРОВИХ ПЛАТФОРМАХ З ВИКОРИСТАННЯМ МЕТОДІВ МАШИННОГО НАВЧАННЯ

У сучасному цифровому середовищі платформи відіграють ключову роль у функціонуванні різних сфер, таких як економіка, освіта, охорона здоров'я та комунікації. Їх динамічна природа забезпечує високу адаптивність до потреб користувачів, але водночас створює нові виклики, пов'язані з ідентифікацією та реагуванням на аномалії. Аномалії, як несанкціонований доступ, збої у функціонуванні чи несподівані зміни у даних, можуть значно впливати на стабільність і безпеку цифрових платформ.

Традиційні методи аналізу аномалій виявляють низьку ефективність у складних і масштабних системах через їхню недостатню здатність обробляти великі обсяги даних у реальному часі. У зв'язку з цим методи машинного навчання набувають дедалі більшого значення, забезпечуючи інструменти для автоматизації аналізу та прогнозування.

Методи машинного навчання пропонують ефективні інструменти для автоматизації процесів аналізу великих даних, виявлення аномалій і прогнозування потенційних збоїв. Їх застосування дозволяє забезпечити вищий рівень стійкості цифрових платформ до несподіваних змін і загроз, покращуючи їхню адаптивність і стабільність у динамічному середовищі.

Існують два основні підходи до ідентифікації аномалій у цифрових платформах: традиційні методи аналізу та сучасні алгоритми машинного навчання. Традиційні підходи зазвичай базуються на статистичних моделях, які оцінюють відхилення від нормального функціонування системи. Вони використовують такі інструменти, як середні значення, стандартні відхилення та гістограми, для визначення потенційно небезпечних подій. Наприклад, перевищення порогового значення трафіку може бути позначене як аномалія. Хоча ці методи є зрозумілими та простими у впровадженні, вони мають суттєві обмеження. Їх ефективність значно знижується в умовах динамічних систем, а також вони неспроможні виявляти аномалії, які раніше не спостерігалися. Крім того, ці підходи вимагають постійного ручного налаштування параметрів.

Сучасні алгоритми машинного навчання значно розширюють можливості аналізу. Вони базуються на обробці великих обсягів даних, включаючи інформацію про поведінкові патерни, взаємозв'язки елементів системи та історичні дані. Наприклад, методи кластеризації, такі як K-Means або DBSCAN, дозволяють знаходити аномалії, які не належать до жодного кластеру. Нейронні мережі й алгоритми на основі дерев рішень забезпечують високу точність у визначенні складних аномалій, таких як незвичні транзакції або поведінкові зміни користувачів. Гібридні моделі, що

поєднують статистичні підходи з машинним навчанням, дозволяють підвищити надійність аналізу.

Водночас алгоритми машинного навчання стикаються з певними викликами. Для їхньої ефективної роботи потрібні великі обсяги навчальних даних. Крім того, такі методи часто є обчислювально складними, що може створити труднощі під час обробки даних великих платформ у реальному часі.

Ідентифікація аномалій у динамічних цифрових платформах потребує ефективних математичних моделей, які враховують складність системи та її взаємозв'язки. Одним із ключових підходів є використання методів кластеризації, таких як K-Means або DBSCAN. Ці алгоритми дозволяють групувати об'єкти за схожими характеристиками та визначати елементи, які відхиляються від загальних закономірностей [1].

Наприклад, у соціальних мережах кластеризація може використовуватися для виявлення груп користувачів зі схожою активністю або аномальних дій, які порушують нормальні патерни взаємодії.

Ще одним важливим методом є використання нейронних мереж, які здатні виявляти складні нелінійні залежності між даними. Ці моделі аналізують великі обсяги історичної інформації та прогнозують потенційні збої на основі виявлених відхилень. Для точнішого аналізу може застосовуватися спектральна кластеризація, яка використовує спектр матриці зв'язків (наприклад, лапласіан графа) для визначення груп взаємопов'язаних вузлів [2].

$$L = D - A, \tag{1}$$

де

L — матриця розподілу зв'язків графа,

D — діагональна матриця ступенів вершин,

A — матриця суміжності.

Математичні моделі також дозволяють створювати метрики для оцінки резильєнтності систем. Наприклад, графові моделі зважують ступінь зв'язків між вузлами, що дає змогу оцінити, наскільки швидко система може відновитися після збоїв [3].

$$C_D(v) = \sum_{u \in V} a(v, u), \tag{2}$$

де

$C_D(v)$ — ступінь центральності вузла v,

$a(v, u)$ — наявність зв'язку між вузлами v і u.

Для цього використовуються формули для розрахунку ступеня центральності, які визначають ключові вузли, що забезпечують стійкість платформи.

Алгоритми регресії дозволяють визначати тренди у зміні параметрів системи та прогнозувати її стан у майбутньому. Наприклад, вони можуть

використовуватися для передбачення збільшення трафіку або виникнення пікових навантажень, що дозволяє адаптувати ресурси системи.

$$y = b_0 + b_1 x + \varepsilon, \quad (3)$$

де

y — залежна змінна,

x — незалежна змінна,

b_0 , b_1 — параметри моделі,

ε — випадкова похибка.

Запропоновані математичні моделі й алгоритми забезпечують не лише виявлення аномалій, але й прогнозування їхніх можливих наслідків, що дозволяє динамічним платформам функціонувати стабільно навіть у складних умовах.

Для підвищення резильєнтності цифрових платформ необхідно комбінувати традиційні методи аналізу та алгоритми машинного навчання. Такий підхід дозволяє адаптуватися до динамічних умов і ефективно реагувати на нові загрози.

Практична реалізація алгоритмів для ідентифікації аномалій на цифрових платформах базується на інтеграції методів машинного навчання з інструментами для аналізу великих даних. У сучасних платформах використовуються різноманітні моделі, які адаптуються до специфічних вимог системи, наприклад, платформи електронної комерції, соціальних мереж чи інтернет-платформ.

Одним із прикладів є застосування алгоритмів кластеризації для сегментації користувачів. Такі алгоритми допомагають визначити групи користувачів зі схожою поведінкою, що дозволяє виявляти аномалії, наприклад, підозрілі транзакції або спроби несанкціонованого доступу [4]. Наприклад, на платформах електронної комерції такі методи використовуються для виявлення шахрайських операцій, аналізуючи відхилення від типових шаблонів покупок.

Інший важливий приклад — використання нейронних мереж для аналізу поведінкових даних. Ці моделі виявляють складні взаємозв’язки між параметрами системи, що дозволяє прогнозувати виникнення аномалій до того, як вони вплинуть на роботу платформи [5]. Наприклад, у системах потокового відео такі підходи використовуються для виявлення затримок у передачі даних, що дозволяє вчасно оптимізувати маршрутизацію трафіку.

Спектральна кластеризація демонструє високу ефективність у складних мережевих структурах, таких як соціальні платформи. Використання спектра матриці зв’язків дозволяє виділити ключові групи вузлів, що сприяє підвищенню ефективності моніторингу мережевої активності.

Практичні результати впровадження таких підходів демонструють значне підвищення стійкості систем до зовнішніх і внутрішніх загроз. Наприклад, адаптація ресурсів у реальному часі дозволяє зменшити навантаження на сервери під час пікової активності, а виявлення та ізоляція аномалій мінімізують ризик масштабних збоїв.

Загалом практичне використання математичних моделей і алгоритмів дозволяє забезпечити високу резильєнтність цифрових платформ, покращуючи їхню стійкість і ефективність навіть за складних умов експлуатації.

Сучасні динамічні цифрові платформи функціонують у складному та швидкозмінному середовищі, що потребує використання передових математичних моделей і алгоритмів для забезпечення їхньої стійкості. Аналіз існуючих підходів демонструє, що поєднання традиційних методів із алгоритмами машинного навчання дозволяє ефективніше ідентифікувати аномалії, прогнозувати їхні наслідки та адаптувати системи до нових викликів.

Практичні результати підтверджують, що такі алгоритми, як кластеризація, спектральний аналіз і нейронні мережі, підвищують резильєнтність платформ. Це дозволяє не лише оперативно реагувати на загрози, але й запобігати їм, забезпечуючи стабільну роботу систем навіть у пікових умовах навантаження.

Однак, попри досягнення, залишаються виклики, пов'язані з обчислювальною складністю алгоритмів, необхідністю великих обсягів навчальних даних і ризиком появи хибнопозитивних результатів. Подальші дослідження мають зосередитися на розробці більш адаптивних і менш ресурсомістких моделей, інтеграції з такими технологіями, як Інтернет речей (IoT) та блокчейн, а також впровадженні гібридних систем для підвищення точності.

Водночас перспективними є напрямки розробки алгоритмів для роботи з потоковими даними в режимі реального часу, що є критичним для платформ із високими вимогами до швидкодії. Використання передових технологій, зокрема штучного інтелекту та аналізу великих даних, дозволить значно підвищити стійкість цифрових платформ, забезпечуючи їхню надійність і адаптивність у динамічному середовищі.

Таким чином, впровадження сучасних моделей та алгоритмів є не лише способом підвищення ефективності цифрових платформ, але й ключовим чинником їхньої резильєнтності, що має вирішальне значення для їхньої стабільності та конкурентоспроможності в умовах швидких технологічних змін.

1. Gross, J. L., Yellen, J., & Anderson, M. (2018). Graph Theory and Its Applications (3rd ed.). Chapman and Hall/CRC. https://doi.org/10.1201/9780429425134.
2. Bishop, C. M. (2006). Pattern Recognition and Machine Learning. Springer.
3. Shi, J., & Malik, J. (2000). Normalized Cuts and Image Segmentation. IEEE Transactions on Pattern Analysis and Machine Intelligence, 22(8), 888–905.
4. Meleshko, Ye. (2019). Методи кластеризації графів соціальних мереж для побудови рекомендаційних систем. Системи управління, навігації та зв'язку, (2.54), 129-134.
5. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.

Г.П. Костенко, А.О. Запорожець

ОЦІНКА ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ ВТОРИННИХ БАТАРЕЙ ЕЛЕКТРОМОБІЛІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ РЕЗЕРВНОГО ЖИВЛЕННЯ В УМОВАХ НАДЗВИЧАЙНИХ СИТУАЦІЙ

В умовах сучасних викликів енергетична резильєнтність стає одним із ключових факторів національної безпеки. Регулярні обстріли критичної інфраструктури створюють значні ризики для стабільності електропостачання, особливо в осінньо-зимовий період, коли навантаження на енергетичну систему значно зростає [1]. Відключення електроенергії стають серйозною проблемою для роботи критично важливих об'єктів, які потребують безперебійного живлення. У таких умовах традиційні рішення, такі як дизельні генератори, демонструють низку обмежень, які знижують надійність їх застосування.

Серед цих обмежень слід відмітити складність забезпечення безперебійного постачання пального під час надзвичайних ситуацій. Логістичні проблеми, руйнування інфраструктури та дефіцит ресурсів ускладнюють використання генераторів. Окрім того, генератори створюють значний вплив на довкілля викидами CO2 та забруднюючих речовин. Все це у підсумку зумовлює необхідність пошуку альтернативних рішень.

Вторинні літій-іонні батареї, що вже відслужили свій термін у електротранспорті, можуть стати екологічною та економічною альтернативою для забезпечення резервного живлення [2]. Ці батареї мають достатню залишкову ємність для підтримки роботи критичних об'єктів у разі відключення основного живлення. У порівнянні з генераторами, вторинні батареї є більш екологічними, менш залежними від логістики та можуть бути інтегровані у сучасні системи управління енергоспоживанням, що сприятиме підвищенню стійкості енергетичних систем до кризових ситуацій [3].

Порівняння резервних джерел живлення: дизельні генератори та вторинні батареї

У виборі резервного енергозабезпечення для критичних об'єктів важливу роль відіграють технічні, економічні та екологічні показники. Традиційно основним рішенням для резервного живлення залишаються дизельні генератори. Проте, із розвитком технологій, вторинні літій-іонні батареї починають займати значне місце в енергетичних стратегіях завдяки своїй ефективності, екологічності та здатності інтегруватися в сучасні системи управління енергоспоживанням

Необхідно враховувати різні аспекти резервного енергозабезпечення. Табл. 1 демонструє ключові відмінності між традиційними дизельними генераторами та вторинними літій-іонними батареями, які все частіше розглядаються як альтернатива в критичних системах. Хоча генератори мають переваги у сценаріях тривалих перебоїв, вторинні батареї

забезпечують менший екологічний вплив, нижчу вартість експлуатації та можуть бути інтегровані в енергосистеми для балансування навантажень [4]. Це робить їх використання доцільним для об'єктів із короткочасними перебоями в електропостачанні.

Таблиця 1. Порівняння характеристик дизельних генераторів та вторинних - батарей для резервного енергоживлення

Параметр	**Дизельні генератори**	**Вторинні батареї**
Вартість придбання	Середня/Висока	Середня
Вартість експлуатації	Висока (паливо, обслуговування)	Низька (мінімальне обслуговування)
Екологічний вплив	Високий (викиди CO_2, шум)	Низький (відсутність прямих викидів)
Надійність	Залежить від палива, механічні збої	Стабільна, менше рухомих частин
Період служби	10–15 років	5–10 років
Придатність до повторного використання	Немає	Повторне використання можливе
Сценарії використання	Тривалі енергоперебої, високе навантаження	Короткочасні перебої, балансування навантажень

Ефективність вторинних батарей у резервному живленні

Вторинні батареї електромобілів мають значний потенціал для забезпечення резервного живлення критичних об'єктів, зокрема лікарень, диспетчерських центрів та високовольтних підстанцій. Використання вторинних батарей у критичних об'єктах дозволяє ефективно забезпечити резервне живлення, пристосоване до специфіки кожного типу об'єкта (Табл. 2). Для лікарень основним завданням є безперервна робота медичного обладнання, від якого залежить здоров'я та життя пацієнтів. У диспетчерських центрах батареї забезпечують живлення серверів та систем зв'язку, що є ключовими для координації дій у надзвичайних ситуаціях.

Таблиця 2. Порівняння показників використання вторинних батарей у різних критичних об'єктах

Показник	**Лікарні**	**Диспетчерські центри**	**Високовольтні підстанції**
Потужність резерву (кВт)	50-200	20-50	500-1000
Час автономної роботи (год)	4-8	6-12	2-4
Вимоги до надійності	Високі	Дуже високі	Критично високі

Кінець таблиці 2

Цільове обладнання	Медичне обладнання	Сервери, системи зв'язку	Захист енергосистеми
Витрати на впровадження ($/кВт)	70-90	70-90	70-90
Основні ефекти	Зниження викидів CO_2 Зменшення споживання енергії Зниження ризику збоїв та підвищення надійності		

Варто окремо відзначити можливість використання вторинних батарей у складі високовольтних підстанцій. Ці об'єкти є критичними вузлами енергетичної системи, і їхня стійкість безпосередньо впливає на стабільність електропостачання великих регіонів. Вторинні батареї можуть забезпечувати живлення систем релейного захисту, автоматизації та керування, що дозволяє уникнути масових відключень та збоїв у роботі енергосистеми. Крім того, їхнє впровадження значно скорочує залежність від дизельних генераторів, підвищуючи економічну ефективність та зменшуючи викиди CO_2. Зменшення викидів CO_2 та залежності від постачання пального робить їх привабливим вибором для впровадження у критично важливих об'єктах.

Для ефективного впровадження вторинних батарей у системи резервного живлення важливо також враховувати їхню деградацію та залишкову ємність. Моделі прогнозування продуктивності таких батарей дозволяють краще планувати їх використання та інтеграцію у існуючі енергетичні системи [5]. Це сприятиме підвищенню стійкості критичних об'єктів до енергетичних криз та сприятиме розвитку циркулярної економіки в енергетичному секторі України.

Економічні та екологічні показники

Використання вторинних батарей у системах резервного живлення дозволяє значно знизити витрати на експлуатацію порівняно з традиційними дизельними генераторами. Згідно з дослідженнями, вартість експлуатації вторинних батарей становить $0,05–0,10 за кВт·год, тоді як для дизельних генераторів цей показник досягає $0,20–0,30 за кВт·год. Крім того, вартість впровадження батарей ($70–150 за кВт) також є значно нижчою порівняно з генераторами ($250–500 за кВт), що робить батареї привабливим варіантом для довготривалих проєктів.

Скорочення викидів CO_2 є ще однією важливою перевагою вторинних батарей. У порівнянні з дизельними генераторами, які виділяють близько 0,70 кг CO_2 на кожний кВт·год виробленої енергії, батареї виділяють лише 0,02 кг CO_2 на кВт·год. Це забезпечує зменшення викидів більш ніж на 90%, що є суттєвим кроком до досягнення екологічних цілей. Додатково, вторинні батареї мають значно вищий коефіцієнт енергоефективності (88–90%) у порівнянні з дизельними генераторами (40–45%), що також сприяє оптимізації витрат на життєвий цикл.

Таблиця 3. Економічні та екологічні показники використання вторинних батарей та дизельних генераторів

Показник	**Вторинні батареї**	**Дизельні генератори**
Вартість експлуатації ($/кВт·год)	0,05–0,10	0,20–0,30
Викиди CO_2 (кг/кВт·год)	0,02	0,70
Рівень шуму (дБ)	<30	60–90
Залежність від пального	Відсутня	Висока
Життєвий цикл (роки)	5–8	10–15
Енергоефективність (%)	88–90	40–45
Вартість впровадження ($/кВт)	70–150	250–500

Висновки

Вторинні батареї електромобілів мають значний потенціал для забезпечення резервного живлення критичних об'єктів. Завдяки своїм характеристикам, таким як залишкова ємність і гнучкість в адаптації до різних умов, вони можуть забезпечувати безперебійну роботу важливих систем навіть під час тривалих енергетичних перебоїв. У лікарнях такі батареї дозволяють підтримувати роботу життєво необхідного обладнання, зменшуючи ризики для здоров'я пацієнтів. У диспетчерських центрах батареї забезпечують функціонування систем управління та зв'язку, що є необхідним для координації дій в умовах надзвичайних ситуацій.

Особливе перспективним може бути їх застосування на високовольтних підстанціях, які є ключовими елементами енергетичної інфраструктури. Інтеграція вторинних батарей на таких об'єктах може забезпечити резервне живлення систем релейного захисту, моніторингу та автоматизації. Це дозволяє зменшити ризик системних збоїв, особливо під час пікових навантажень чи атак на енергетичну інфраструктуру. Крім того, батареї можуть бути використані для стабілізації частоти та напруги у мережі, що є важливим аспектом підтримання її стабільності в кризових умовах.

Вторинні батареї демонструють значно кращі економічні та екологічні характеристики порівняно з дизельними генераторами. Вони мають нижчу вартість експлуатації та менший рівень викидів CO_2, що відповідає вимогам сталого розвитку. Окрім того, відсутність залежності від пального робить їх більш надійними у кризових умовах, тоді як дизельні генератори потребують регулярного постачання ресурсів, що може бути ускладненим під час надзвичайних ситуацій. Використання вторинних батарей також забезпечує суттєве зниження шумового впливу, що є важливим для об'єктів із підвищеними вимогами до комфорту та безпеки.

1. Zaporozhets, A. et al. (2024). Power System Resilience: An Overview of Current Metrics and Assessment Criteria. In: Systems, Decision and Control in Energy VI.

Studies in Systems, Decision and Control, vol 561. Springer, Cham. https://doi.org/10.1007/978-3-031-68372-5_2.
2. Denysov, V. et al. (2024). Energy System Optimization Potential with Consideration of Technological Limitations. In: Nexus of Sustainability. Studies in Systems, Decision and Control, vol 559. Springer, Cham. https://doi.org/10.1007/978-3-031-66764-0_5.
3. 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.
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. 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.

І.П. Каменева

ІМОВІРНІСНІ ОЦІНКИ РОЗПОДІЛУ НЕБЕЗПЕКИ ДЛЯ ТЕРИТОРІАЛЬНИХ СИСТЕМ В УМОВАХ РИЗИКУ

В останні роки в світі відбувається занадто багато небезпечних та надзвичайних подій, суттєво відмінних від минулого досвіду. Перш за все це неочікувані кліматичні явища або катастрофічні події (землетруси, цунамі, вулканічні виверження, жахливі посухи або масштабні зливи, нетипові для окремих регіонів, що відрізняються суттєво нелінійним характером), Також сюди можна віднести численні техногенні аварії, вибухи та інші небезпечні інциденти, що виникають на фоні військових конфліктів і викликають значні пошкодження енергетичних систем і об'єктів критичної інфраструктури.

На фоні таких подій зростає актуальність теоретичних і прикладних робіт, спрямованих на підвищення безпеки та резильєнтності соціальних, енергетичних і екологічних систем. На системному рівні резильєнтність – це здатність забезпечити можливості для адаптації складної системи до збурень і несприятливих змін, тобто наявність певних механізмів для підтримки або відновлення стабільного стану (балансу основних складових).

Задачі оцінювання резильєнтності мають багато різних вимірів, які необхідно враховувати при моделюванні. Тому на математичному рівні їх можна описати в рамках багатовимірного аналізу даних моніторингу та визначення ризиків щодо виходу системи за межі допустимих значень.

В [1, 2] досліджуються імовірнісні моделі репрезентації знань, де семантичні аспекти складної ситуації можна описати у термінах імовірності небезпеки. Запропоновано також методи перетворення даних екологічного моніторингу (в вигляді таблиць) в семантичний простір ризику, де визначено імовірнісну міру небезпеки (міру ризику), яка вказує належність випадкових подій до відповідних рівнів небезпеки. Семантичний простір ризику можна вважати адекватною та зручною формою репрезентації знань про довкілля, що узагальнює багаторічний досвід екологічних досліджень.

Коротко розглянемо алгоритмічні засоби представлення та візуального аналізу небезпечних тенденцій у вигляді проекцій фазового простору. Для візуальної інтерпретації множини вихідних даних запропоновано методи та засоби побудови простору інформативних показників [2]. Зокрема, можна визначити значення ризиків, в межах яких екосистема зберігає здатність до відновлення (діапазон резильєнтності), тобто описати порушення балансу в системі як імовірність виходу за межі нормальної діяльності.

Загальна схема структурного аналізу даних і виявлення когнітивних патернів (шаблонів небезпечних подій) представлена на рис. 1. Відповідно до цієї методики множина вихідних даних отримує змістовну інтерпретацію та візуальне представлення виявлених шаблонів. Імовірнісний простір знань будується з урахуванням експертних оцінок виділених подій [3]. Розглянемо більш докладно окремі етапи аналізу даних (рис. 1)

1. Матричне представлення даних моніторингу

Якщо вихідні дані представлені у вигляді таблиці з n спостережень, кожне з яких включає m параметрів, то цю множину можна описати як простір подій розмірності m. Вихідні спостереження представлені в цьому просторі як множина точок з координатами, що відповідають числовим значенням відповідних параметрів. Випадковими подіями можна вважати окремі підмножини вихідної множини спостережень.

2. Багатовимірний аналіз та візуалізація простору подій

Для виявлення латентних характеристик вихідних даних (факторів впливу) використовуються відомі методи багатовимірного аналізу, зокрема факторний аналіз і побудова багатовимірних шкал [2, 3].

В результаті обробки сукупність вихідних ознак перетворюється в більш інформативні характеристики (фактори), які дозволяють отримати опис вихідних даних у вигляді точок в новій системі координат. Застосування методів багатовимірного аналізу забезпечує перехід в простір подій меншої розмірності за рахунок виключення менш інформативних показників.

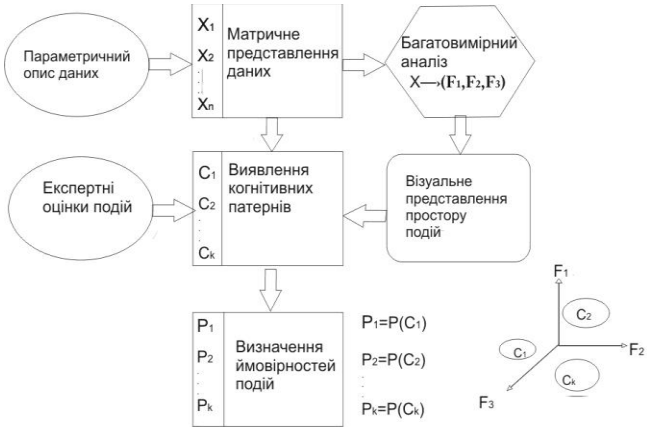


Рисунок 1 – Схема аналізу даних в імовірнісному просторі

Після зниження розмірності простір випадкових подій набуває візуальної інтерпретації (на площині або в тривимірному просторі), набагато зручнішу для візуального аналізу на екрані монітора. Множина подій може виглядати як розмита хмара, окремі скупчення або довільні конфігурації різних форм. Виділені фактори утворюють семантичні шкали, за допомогою яких можна оцінити окремі спостереження. Кожен із чинників включає кілька показників, тобто утворює більш інформативний образ. Він може бути проінтерпретований відповідно до того значення, яке він набуває в даній конкретній ситуації.

Імовірнісні моделі подання знань мають подвійну інтерпретацію. На логічному рівні вони визначаються як імовірнісні оцінки і мають формальне представлення. В той же час вони одержують візуальну інтерпретацію, яка дозволяє скористатися засобами сучасної комп'ютерної графіки.

3. Виявлення інформативних образів (шаблонів).

З усієї сукупності можливих подій виділяємо небезпечні події, які мають певну якісну інтерпретацію. Як правило, на цьому етапі необхідно залучення експертних знань про предметну область, щоб встановити зв'язки між чисельними значеннями показників і тими шаблонами, до яких можна віднести наявні спостереження Кожна група таких спостережень може розглядатись як окреме поняття (певна загроза або рівень небезпеки).

Зокрема, в області екологічної безпеки такі поняття можуть відповідати різним рівням техногенних навантажень або пошкоджень. При аналізі медико-екологічної інформації можна виділити різні ступені порушення здоров'я (захворювання та групи ризику за результатами аналізів).

5. Оцінювання ймовірностей небезпечних подій.

Кожному з виділених шаблонів слід привласнити кількісне значення імовірності, яке характеризує ступінь об'єктивної можливості небезпечної події на основі вже наявних даних моніторингу та експертних оцінок.

Імовірність, пов'язана з небезпечною подією, визначається в рамках вже побудованої системи шаблонів (бази знань). У більшості випадків системи шаблонів (прототипів) будуються на основі наявних ретроспективних даних, які допомагають уточнити зв'язки між значеннями окремих груп показників та імовірністю виникнення певних небезпечних ситуацій.

На основі багатовимірного аналізу та відповідних програмних засобів [2, 3] можна побудувати імовірнісні розподіли для територіальних систем в умовах терористичних загроз, де ризики можливих руйнацій і пошкоджень зростають в залежності від розташування важливих об'єктів інфраструктури, військових частин або енергетичних підприємств.

Для територіальних систем з високими ризиками рекомендується здійснювати додаткові дослідження, спрямовані на оцінювання діапазону резильєнтності екологічних систем в цілому на територіальному рівні та розташованих поблизу об'єктів критичної інфраструктури.

1. Артемчук В.А., Каменева И.П., Яцишин А.В. Специфика применения когнитивного анализа информации в задачах обеспечения экологической безопасности // Электронное моделирование, 2017, **39**, № 6, с. 107–124.
2. Каменева І.П., Артемчук В.О. Проблема інформативності та визначення інформативних структур для підтримки прийняття рішень в галузі екологічної безпеки // Електронне моделювання, 2022, 44, № 3, с. 50-64.
3. Каменева И.П., Артемчук В.А., Яцишин А.В. Вероятностное моделирование экспертных знаний с использованием методов психосемантики // Електронне моделювання, 2019, 41, № 2, с. 81–96.

Д.О. Рибачок

РЕЗИЛЬЄНТНІСТЬ РОЗПОДІЛЕНИХ СИСТЕМ: АРХІТЕКТУРНІ ПІДХОДИ ТА МЕТОДИ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ ДО ЗБОЇВ

Розподілені системи є основою сучасних інформаційних технологій, забезпечуючи високу продуктивність, масштабованість та доступність, які є необхідними для виконання складних завдань у різноманітних галузях. Однак складність, гетерогенність компонентів та географічна розподіленість створюють значні виклики для забезпечення резильєнтності. Збої, що спричинені апаратними, або програмними помилками, мережевими порушеннями чи іншими факторами, можуть призвести до втрати даних, зниження якості обслуговування та переривання функціонування системи. Забезпечення стійкості розподілених систем до таких збоїв є ключовим завданням сучасної комп'ютерної інженерії, що вимагає впровадження відповідних архітектурних підходів та методів, таких як реплікація, балансування навантаження, резервування ресурсів і автоматизоване виявлення збоїв. Представлено огляд існуючих підходів, їхні переваги та обмеження, а також запропоновано напрямки майбутніх досліджень, орієнтованих на вдосконалення системного управління збоями та забезпечення високої надійності й ефективності роботи розподілених середовищ.

Основні види відмовостійкості в розподілених та хмарних обчислювальних системах можна класифікувати на чотири категорії: реактивні, проактивні, адаптивні та гібридні підходи. Реактивні підходи зосереджуються на мінімізації впливу збоїв після їх виникнення. Вони передбачають відновлення системи до робочого стану за допомогою таких методів, як реплікація даних, створення контрольних точок, повторне виконання завдань, журнальне логування, спеціалізована обробка винятків і рятувальні робочі потоки. Ці підходи забезпечують високу доступність і надійність, але можуть викликати значні накладні витрати та проблеми з узгодженістю даних. Проактивні підходи спрямовані на передбачення та запобігання збоїв до їх виникнення. Основними методами є програмне омолодження, самовідновлення, превентивна міграція компонентів і балансування навантаження. Ці підходи дозволяють знизити ризики виникнення збоїв, забезпечуючи стабільну роботу системи, однак потребують складних механізмів прогнозування та управління. Адаптивні підходи поєднують прогнозування та автоматичну адаптацію системи до змін. Вони використовують штучний інтелект та машинне навчання для виявлення та виправлення потенційних збоїв у реальному часі. Ці підходи є більш гнучкими, оскільки система постійно навчається та адаптується до нових умов, але вони можуть бути дорогими та вимагати значних обчислювальних ресурсів. Гібридні підходи інтегрують реактивні, проактивні та адаптивні методи для більш ефективного управління збоями.

Вони поєднують переваги всіх підходів, забезпечуючи максимальну стійкість і ефективність системи навіть у складних середовищах. Гібридні методи дозволяють використовувати кращі рішення для різних типів збоїв, проте їхнє впровадження є складним і вимагає комплексного підходу до проєктування системи.

Типи збоїв у розподілених та хмарних системах класифікуються за природою їх виникнення та впливу на систему. Основними категоріями є такі:

Постійні (перманентні) збої: Ці збої залишаються в системі до тих пір, поки дефектний компонент не буде замінено або відремонтовано. Вони часто виникають через апаратні поломки або повну відмову компонентів системи, таких як сервери чи мережеве обладнання. Постійні збої можуть мати серйозний вплив на продуктивність і доступність системи.

Транзитні (тимчасові) збої: Це короткочасні збої, які зникають самі по собі або після виправлення причини. Наприклад, до таких збоїв належать збої в мережевих з'єднаннях або тимчасові збої процесорів. Вони є менш небезпечними, але можуть створювати затримки чи перерви в роботі системи.

Періодичні (інтермітуючі) збої: Ці збої виникають і зникають випадково та нерегулярно. Вони можуть бути спричинені, наприклад, перегріванням апаратного забезпечення, яке тимчасово втрачає працездатність. Періодичні збої складно діагностувати через їхню нестабільність.

Доброзичливі (benign) збої: Такі збої трапляються, коли один з компонентів системи перестає виконувати свою функцію, але не спричиняє серйозного впливу на решту системи. Наприклад, це може бути вихід із ладу одного з вузлів, який не є критичним для загальної роботи.

Візантійські (byzantine) збої: Це найскладніший тип збоїв, коли компоненти системи поводяться непередбачувано, наприклад, надсилають суперечливі або неправильні дані. Такі збої важко виявити, і вони можуть серйозно вплинути на коректність функціонування системи.

Виклики у забезпеченні відмовостійкості в розподілених і хмарних системах пов’язані зі складністю архітектури та взаємодії компонентів, а також з різноманітними сценаріями відмов. Основні виклики включають:

Гетерогенність системи. Сучасні розподілені системи складаються з різноманітних апаратних і програмних компонентів, часто розташованих у різних географічних регіонах. Ця неоднорідність ускладнює інтеграцію, управління та забезпечення резильєнтності, оскільки різні компоненти можуть мати різні протоколи роботи, рівні надійності та характеристики відмов.

Автоматизація процесів. В умовах зростання масштабів і складності систем забезпечення відмовостійкості вимагає автоматизованих рішень для виявлення, аналізу та усунення збоїв. Однак розробка універсальної платформи для автоматизації таких процесів є складним завданням, оскільки різні сценарії можуть вимагати унікальних підходів.

Призупинення компонентів. Вихід з ладу ключового компонента, наприклад сервера чи вузла в мережі, може спричинити зупинку всього хмарного або розподіленого середовища. Запобігання таким ситуаціям вимагає впровадження резервних механізмів, таких як реплікація або автоматичне перенаправлення робочих процесів.

Навантаження на систему. У хмарних середовищах завдання часто розподіляються між вузлами для оптимального використання ресурсів. Однак у разі відмови одного з вузлів навантаження може бути перерозподілене неправильно, що створює затримки в обробці завдань або їхню недоступність.

Перерви у роботі системи. У великих розподілених системах, таких як хмарні обчислення, збій в одному центрі даних може вплинути на доступність і продуктивність інших центрів через тісну інтеграцію компонентів. Забезпечення безперервності роботи вимагає детально прописаних угод про рівень обслуговування (SLA) та ефективних механізмів відновлення.

Складність забезпечення консистентності даних. У розподілених системах, особливо в географічно розподілених середовищах, забезпечення узгодженості даних є складним завданням. Проблеми виникають через затримки в мережі, порушення зв'язку та асинхронну реплікацію даних.

Масштабованість. Забезпечення відмовостійкості системи, яка динамічно збільшує обсяги даних або кількість користувачів, вимагає адаптивних рішень, здатних підтримувати високу продуктивність без збільшення витрат на обчислення.

Вартість реалізації. Багато механізмів забезпечення відмовостійкості, таких як реплікація даних або балансування навантаження, є ресурсомісткими, що збільшує витрати на впровадження та експлуатацію системи. Пошук оптимального співвідношення між витратами та ефективністю залишається відкритим питанням.

Майбутні напрями досліджень у галузі забезпечення відмовостійкості розподілених і хмарних систем спрямовані на інтеграцію машинного навчання та штучного інтелекту для прогнозування та автоматизованого управління збоями, розробку економічно ефективних і адаптивних методів балансування навантаження, а також впровадження механізмів, які забезпечують узгодженість даних у географічно розподілених середовищах. Особливу увагу приділяють гібридним підходам, що поєднують реактивні, проактивні та адаптивні методи, а також створенню універсальних платформ для автоматизації процесів забезпечення резильєнтності. Дослідження також фокусуються на зменшенні витрат і накладних витрат під час впровадження рішень, а також на підвищенні їхньої ефективності в умовах динамічно змінюваних навантажень і масштабів систем.

1. Mukwevho, M., & Celik, M., *"Taxonomy and trends in fault tolerance approaches in cloud computing"*, IEEE Access.
2. Kalantari, A., & Liu, M., *"Proactive fault tolerance through dynamic software rejuvenation in cloud systems"*, Journal of Cloud Computing.
3. Zhang, L., & Lee, S., *"Hybrid fault-tolerance methods for large-scale distributed systems"*, Distributed Computing Systems Journal.
4. Rajput, S., & Sikka, P., *"Self-healing mechanisms in distributed computing environments"*, IEEE Transactions on Dependable and Secure Computing.
5. Veronese, G. S., & Distler, T., *"Practical Byzantine fault tolerance for distributed systems"*, ACM Transactions on Computer Systems, 2014.
6. Kumari, P., & Kaur, S., *"Proactive and reactive fault tolerance strategies for cloud computing: A comparative study"*, International Journal of Grid Computing, 2018.
7. Eischer, B., & Distler, T., *"Adaptive replication for fault tolerance in geo-distributed systems"*, IEEE Distributed Systems Online, 2020.
8. Lee, K., & Gil, M., *"Replication and checkpointing methods for fault recovery in cloud computing"*, Elsevier Future Computing Journal, 2021.

A. Davydiuk, S. Kulyk

DATA CENTER INFRASTRUCTURE IN THE CONTEXT OF NATIONAL RESILIENCE. EXISTING RISKS, SOLUTIONS, AND PROSPECTS

The use of data centers is becoming increasingly popular due to the constant growth of data, as well as the convenience and accessibility of cloud services for users. Indeed, data centers offer a number of advantages over client-hosted local solutions, as the data center assumes the risks associated with the security of this data and the continuous availability of digital services for the data center's clients. At the same time, the irreversible process of migration to data centers makes them de facto critical infrastructure objects. These facilities must meet heightened requirements for security and operational reliability, as they have a significant impact on national resilience.

The basis for such requirements lies in the risk analysis for data centers. A data center risk is understood as the impact of uncertainty on the goals of the data center. In this context, uncertainty is explained as the lack of sufficient information to prevent a negative event. Thus, the question arises of identifying and classifying the risks associated with data centers. Naturally, data centers, as an organizational and technical system consisting of organizational processes, technical means, and tools, inherit a range of risks typical of standard information and communication systems (hereafter referred to as ICS), such as cyberattacks, physical destruction, and so on. However, due to their unique characteristics, data centers also face a number of specific risks, which are the focus of this publication.

Thus, the purpose of this study is to analyze these unique risks, propose solutions to enhance the resilience of data centers, and explore prospects for their further development.

To identify the specific risks of data centers, it is appropriate to compare them with conventional information and communication systems (ICS). First and foremost, data centers differ in terms of data volumes, the amount of equipment, monitoring challenges [1], energy supply requirements, compatibility issues of virtual machines within a single network [2-4], risks of battery failures [5,6] and equipment breakdowns, as well as failures in ventilation and fire suppression systems. Moreover, data centers face physical risks, such as floods, fires, and terrorist attacks [7]. Unlike conventional systems, relocating a data center to mitigate risks requires significant time and logistical resources, making this process comparable to a full restoration of IT infrastructure.

This study examines existing literature and models related to these issues, including traffic encryption during migration, intelligent monitoring systems, and predictive maintenance of equipment. Alternative approaches, such as hybrid migration strategies—partly physical and partly through data transmission networks—are also analyzed. Particular attention is given to emerging practices, such as mobile data centers and geographically distributed backup strategies.

Thus, the first risk specific to data centers is the lack of adequate conditions for deployment at a new location. The next risk is the insufficiency of logistical resources for relocation. A lack of time for the migration process is also a significant risk. Furthermore, a shortage of competencies necessary for redeploying the data center at the new location may cause substantial delays in restoring operations.

An alternative approach may involve accepting the risk of losing IT equipment while ensuring data preservation. At the same time, the issue arises of the time required to create a complete backup and the availability of storage capacity in a geographically remote backup facility. It should also be noted that migrating a virtual machine is critical for load balancing, server consolidation, and maintenance in virtualized data centers, and can increase security risks. As an alternative, migration traffic should be encrypted, eliminating the need for dedicated management networks while ensuring data security and mutual authentication. The work [8] proposes an architecture that helps create an automated intelligent system, which monitors overloads or underloads and determines when operational migration should occur. Once a virtual machine is selected, encryption is performed using the appropriate security algorithm, ensuring data security, mutual authentication, confidentiality, and integrity.

It is also important to note that a critical factor here is the monitoring of the lifespan of hard drives. Thus, premature failure of a disk and the corresponding data loss can have catastrophic consequences. To reduce the risk of failures, cloud storage providers monitor the health of disks based on their status and replace hard drives before they fail. By assessing the remaining lifespan of hard drives, it is possible to predict the mean time to failure of a specific device and replace it at the appropriate time, ensuring maximum utilization while minimizing operational costs. The work [9] presents an LSTM encoder-decoder model, where the context derived from understanding the sequences of reliability statistics helps predict the output sequence of the number of days remaining until a potential disk failure. The models developed in this work have been trained and validated on a comprehensive dataset of all 10 years of S.M.A.R.T. health data provided by Backblaze, across various disk instances. A hybrid approach, where part of the data is physically moved with the media (disks), and part is transferred via data transmission networks, may also be used as an alternative. However, it is essential to consider the reliability of the data transmission channels, which presents an additional risk.

During military conflicts, the assessment of such risks increases significantly, leading to the emergence of alternative approaches to the placement of data centers in areas that are difficult for the enemy to access. For example, Fortnox in the Swiss mountains [10], Microsoft's underwater data centers [11], and so on. Currently, there are mobile data centers, consisting of several machines (operator and administrator units) [12], as well as space-based data centers [13].

The complexity of finding an optimal solution to overcome the resilience problem of data centers can be seen as a multi-criteria task for determining optimal

decisions regarding the architecture and placement of data centers. For example, the work [14] proposes a strategy for placing a backup data processing center, considering emergencies and evacuation, with a global view of network resources in scenarios defined by software. Specifically, to reduce the risk of backup loss and enable rapid evacuation after a natural disaster, the researchers examine expected losses after the disaster and evacuation delays, formulating a new facility location problem accounting for disaster and evacuation (NP-hard), which is multi-objective. The proposed multi-objective optimization algorithm optimizes multiple goals, with different coefficients in various disaster situations. In particular, data on location, backup evacuation delay, Pareto recommendation degree, and node damage loss are introduced to guide the solution search.

The work [15] investigates the impact of various uncertainties in parameters on energy efficiency and over-provisioning coefficients, such as virtual machine resource requirements, migration-related costs, or the energy consumption model of the servers used. It is demonstrated that allocating additional resources to handle workload uncertainty affects the server over-provisioning ratio and energy consumption. The paper proposes an approach for operators to calculate a more reliable migration schedule, which will lead to higher overall energy consumption. A riskier operator may choose a more favorable schedule, resulting in lower energy consumption but also increasing the risk of SLA violations.

A special case is data evacuation to avoid the consequences of cyberattacks on virtual machines by moving them to quarantine and inspection centers. The work [16] demonstrates an approach to minimizing the damage caused by a cyberattack through the rapid relocation of virtual machines under threat of malware infection to other locations, taking into account alerts provided by intrusion detection mechanisms. Specifically, the problem is formalized into a mathematical model, which is represented as an integer linear programming problem.

An additional risk during migration is the overload of physical machines. The work [17] presents a migration strategy considering workload, called Chameleon, which is focused on recent cloud workloads. Chameleon creates a new indicator and corresponding threshold value for accurately identifying hotspots. It also predicts the resource requirements of a virtual machine under complex workloads to avoid secondary overload of the physical machine to which the virtual machine is migrated.

The main principle of migration remains the geographical distribution of data. For better availability and fault tolerance of data copies in geographically distributed data centers, the process of geo-replication is used. A distinctive feature of geo-replication is the high global latency between data centers, which varies significantly depending on the location of the data centers. Thus, the choice of data centers for deploying a cloud application directly affects the observed response time. The study [18] proposes an optimization system that automatically generates a geo-replication placement plan to minimize latency.

After the migration (copying) is completed, there remains the risk of improper data storage. The work [19] proposes an external auditor, who, on behalf of the users, will periodically check the integrity of the data stored on the cloud server. The user will not experience any online load, and data security will be maintained, as data will not be directly transmitted to the external auditor. A homomorphic encryption scheme is used to encrypt the data that will be transmitted to the Third-Party Auditor.

For continuous monitoring of data security, the authors of the work [20] propose a risk assessment framework to study the security risks of cloud operators between cloud users and two cloud providers. The risk assessment framework uses the National Vulnerability Database [21] to study the vulnerabilities of router operating systems in the cloud operator. This framework provides quantitatively defined security indicators for each cloud operator, enabling cloud users to choose the quality of security services among cloud providers.

Based on the analysis presented above, it becomes possible to classify the risks of data centers (see Table 1).

Table 1. Classification of Data Center Risks

Risk Category	Examples	Description
Cyber Threats	Malware, ransomware, unauthorized access	Vulnerabilities in security systems that can be exploited by hackers.
Physical Risks	Natural disasters, terrorist attacks	Damage to infrastructure caused by external factors.
Equipment Risks	Hard drive failures, ventilation issues	Premature hardware failures requiring monitoring.
Logistical Risks	Insufficient resources for relocation, virtual machine compatibility issues	Challenges in transferring or deploying data centers in new environments.
Energy Risks	Power supply interruptions	Lack of backup power sources or insufficient capacity.
Data Migration Risks	Compatibility issues, security vulnerabilities	Difficulties in transferring data between data centers or securing them.

Although the solutions presented above offer significant improvements, their implementation poses certain challenges. For instance, predictive maintenance models require extensive datasets, which are not always available. Encrypted

migration enhances security but can increase latency and resource requirements. Geo-replication, while highly reliable, causes delays due to network latency and depends on a stable connection between data centers.

In times of war or similar crises, risk assessment becomes more critical, requiring unconventional data center placement strategies, such as remote mountain sites or underwater installations. However, these innovative approaches require significant investment and further technological development.

This research identifies key risks associated with data centers, distinguishing them from traditional ICS. Unique risks, such as relocation challenges, equipment failures, and vulnerabilities in virtual machine migration, were analyzed along with corresponding solutions. Techniques such as predictive maintenance, encrypted migration, and geo-replication have proven effective in improving resilience.

The findings emphasize the importance of developing innovative approaches, including mobile and autonomous data centers, to address evolving challenges. Future research should focus on optimizing algorithms for disaster recovery and exploring new technologies to ensure the resilience and sustainability of data centers under extreme conditions.

1. Verissimo, P., Kreutz, D., Araujo, F., Barbosa, R., Neves, S., Sousa, B., Casimiro, A., Curado, M., Silva, C., Gandhi, R., & Narasimhan, P. (2012). TRONE: Trustworthy and resilient operations in a network environment. У 2012 IEEE/IFIP 42nd international conference on dependable systems and networks workshops (DSN-W). IEEE. https://doi.org/10.1109/dsnw.2012.6264694.
2. Miao, F., Wang, L., & Wu, Z. (2018). A VM placement based approach to proactively mitigate co-resident attacks in cloud. У 2018 IEEE symposium on computers and communications (ISCC). IEEE. https://doi.org/10.1109/iscc.2018.8538543.
3. Almutairi, A., Sarfraz, M. I., & Ghafoor, A. (2018). Risk-Aware management of virtual resources in access controlled service-oriented cloud datacenters. IEEE Transactions on Cloud Computing, 6(1), 168–181. https://doi.org/10.1109/tcc.2015.2453981.
4. Li, H.-C., Liang, P.-H., Yang, J.-M., & Chen, S.-J. (2010). Analysis on cloud-based security vulnerability assessment. У 2010 IEEE 7th International Conference on e-Business Engineering (ICEBE). IEEE. https://doi.org/10.1109/icebe.2010.77.
5. Nasiriani, N., & Kesidis, G. (2018). Optimal peak shaving using batteries at datacenters: Charging risk and degradation model. У 2018 international conference on computing, networking and communications (ICNC). IEEE. https://doi.org/10.1109/iccnc.2018.8390416.
6. Nasiriani, N., Kesidis, G., & Wang, D. (2017). Optimal peak shaving using batteries at datacenters: Characterizing the risks and benefits. У 2017 IEEE 25th international symposium on modeling, analysis and simulation of computer and telecommunication systems (MASCOTS). IEEE. https://doi.org/10.1109/mascots.2017.27.
7. Ceballos, J., DiPasquale, R., & Feldman, R. (2012). Business continuity and security in datacenter interconnection. Bell Labs Technical Journal, 17(3), 147–155. https://doi.org/10.1002/bltj.21565.

8. Sengole Merlin, S., Arunkumar, N. M., & Angela, M. A. (2018). Automated intelligent systems for secure live migration. У 2018 second international conference on inventive communication and computational technologies (ICICCT). IEEE. https://doi.org/10.1109/icicct.2018.8472988.
9. Mohapatra, R., Coursey, A., & Sengupta, S. (2023). Large-scale end-of-life prediction of hard disks in distributed datacenters. У 2023 IEEE international conference on smart computing (SMARTCOMP). IEEE. https://doi.org/10.1109/smartcomp58114.2023.00069.
10. Our datacenter. company.swisscows.com. https://company.swisscows.com/en/about/datacenter.
11. Roach, J. (2020, 14 September). Microsoft finds underwater datacenters are reliable, practical and use energy sustainably. news.microsoft.com. https://news.microsoft.com/source/features/sustainability/project-natick-underwater-datacenter/.
12. Mobile data center. conteg.com. https://www.conteg.com/mobile-data-center.
13. Space data centres. Space Data Centres. https://www.spacedatacentres.co.uk/.
14. Li, X., Wang, H., Yi, S., Liu, S., Zhai, L., & Jiang, C. (2019). Disaster-and-Evacuation-Aware backup datacenter placement based on multi-objective optimization. IEEE Access, 7, 48196–48208. https://doi.org/10.1109/access.2019.2909084.
15. Nasim, R., Zola, E., & Kassler, A. J. (2018). Robust optimization for energy-efficient virtual machine consolidation in modern datacenters. Cluster Computing, 21(3), 1681–1709. https://doi.org/10.1007/s10586-018-2718-6.
16. Karakoc, E., & Dikbiyik, F. (2016). Rapid migration of VMs on a datacenter under cyber attack over optical infrastructure. У 2016 honet-ict. IEEE. https://doi.org/10.1109/honet.2016.7753450.
17. Liu, Y. (2016). Chameleon: Virtual machine migration supporting cascading overload management in cloud. У Green, pervasive, and cloud computing (с. 129–145). Springer International Publishing. https://doi.org/10.1007/978-3-319-39077-2_9.
18. Zakhary, V., Nawab, F., Agrawal, D., & El Abbadi, A. (2016). DB-Risk. У SIGMOD/PODS'16: International conference on management of data. ACM. https://doi.org/10.1145/2882903.2899405.
19. Rewadkar, D. N., & Ghatage, S. Y. (2014). Cloud storage system enabling secure privacy preserving third party audit. У 2014 international conference on control, instrumentation, communication and computational technologies (ICCICCT). IEEE. https://doi.org/10.1109/iccicct.2014.6993049.
20. Lenkala, S. R., Shetty, S., & Kaiqi Xiong. (2013). Security risk assessment of cloud carrier. У 2013 13th IEEE/ACM international symposium on cluster, cloud and grid computing (ccgrid). IEEE. https://doi.org/10.1109/ccgrid.2013.28.
21. National vulnerability database. nvd.nist.gov. https://nvd.nist.gov/.

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

ВИКОРИСТАННЯ ПЛІС В ТЕХНІЧНИХ СИСТЕМАХ ДРОБОВОГО ПОРЯДКУ: ПЕРЕВАГИ ТА ВИКЛИКИ

Математичний опис технічних систем, в якому кількість операцій диференціювання або інтегрування не є цілою величиною, надає певні переваги під час вирішення багатьох прикладних задач, таких як низькочастотна фільтрація сигналів, стиснення інформації, динамічне шифрування, виділення сигналу на тлі перешкод, ідентифікація параметрів динамічних систем тощо [1]. На жаль, використання систем нецілого порядку вимагає за інших рівних умов більшої кількості обчислень, що може стати проблемою, наприклад, в мобільних та безпілотних застосуваннях.

Програмовані логічні інтегральні схеми (ПЛІС) є відомим засобом підвищення резильєнтності та зниження енергоспоживання технічних систем. В данному дослідженні проаналізовано можливості їх використання в якості платформи для побудови пристроїв, що використовують математичний апарат дробового порядку. Приклади практичних розробок обчислювачів нецілого порядку на ПЛІС можна знайти, наприклад, в роботах [2, 3]. В якості алгоритмічної основи для побудови апаратної схеми в даних дослідженнях використано оператор Грюнвальда–Летнікова. В роботі [4] наведено обчислювальну структуру реалізації на ПЛІС цього оператора.

Підсумовуючи отриманий досвід, можна зробити наступні висновки стосовно можливостей використання ПЛІС для побудови систем дробового порядку. Такі риси програмованої логіки, як висока енергоефективність та безпрецедентна гнучкість стають безумовними перевагами. До потенційно проблемних моментів слід віднести, по-перше, обмежені можливості реконфігуровних пристроїв виконувати операції з плаваючою комою. По-друге, ускладнюється реалізація ще однієї важливої переваги ПЛІС – значних здібностей щодо розпаралелювання розрахунків. Саме від того, наскільки успішно вдасться подолати згадані виклики, залежить ступень поширення програмованої логіки в якості апаратної бази для систем нецілого порядку.

1. Васильев В. В., Симак Л. А., Васильев А. В. Обработка сигналов и моделирование динамических систем дробного порядка на основе операционного исчисления аппроксимационного типа. *Електронне моделювання*. 2016. Том 38, № 4. С. 13-34.
2. A unified FPGA realization for fractional-order integrator and differentiator / M. S. Monir et al. *Electronics*. 2022. Vol. 11, no. 13:2052.
3. Fractional order integrator/differentiator: FPGA implementation and FOPID controller application / M. F. Tolba et al. *AEU – international journal of electronics and communications*. 2019. Vol. 98. P. 220–229.
4. Васильєв О.В., Васильєв В.В., Чьочь В.В., Гільгурт С.Я. Реалізація технічних систем нецілого порядку з використанням програмованої логіки. *Електронне моделювання*. 2024. Том 46, № 6. С. 64-71.

Ю.О. Гарбуз

РЕЗИЛЬЄНТНІСТЬ МІСЬКИХ СИСТЕМ ЖИТТЄЗАБЕЗПЕЧЕННЯ ПІД ЧАС ВОЄННОГО СТАНУ

Військові дії в Україні стали масштабним випробуванням для міської інфраструктури, яка ще до їх початку зазнавала впливу кліматичних змін, надзвичайних подій і техногенних аварій. Підвищення резильєнтності міських систем життєзабезпечення (МСЖ) є ключовим завданням для збереження працездатності інфраструктури в умовах багатовекторних загроз. При цьому, якщо деякі впливи можливо прорахувати (наприклад, кліматичні), то вплив військових подій спрогнозувати практично неможливо. Яскравий приклад – неможливість постачання води з р. Дніпро в м. Миколаїв з квітня 2022 року через руйнування водогону та окупацію територій. Лише в травні 2022 р. водопостачання відновилось, але вода подавалась з іншої річки - Південного Бугу і відповідала санітарним нормам не «питної», а «технічної» води [1, 2]. Дотепер ця проблема повністю не вирішена.

Основними викликами для резильєнтності МСЖ під час військових дій є атаки на критичну інфраструктуру, посилення кліматичних ризиків, через неможливість оперативно реагувати на них з різних чинників, та соціальні ризики. Атаки на критичну інфраструктуру спричиняють масштабні руйнування енергосистем, систем водопостачання, тепломереж та іншої цивільної інфраструктури. Як наслідок - відключення електро- та водопостачання, перебої з теплопостачанням, зупинка міського електротранспорту, обмеження в наданні медичної допомоги цивільному населенню тощо. До цього додаються кліматичні та соціальні ризики, перші - є наслідком ускладнення реагування на них через військові дії, другі спричинені вимушеною міграцією та збільшенням навантаження на міські системи у відносно безпечних регіонах держави.

Сучасні МСЖ в Україні не були пристосовані до умов війни, тому є лише два шляхи розв'язання цієї проблеми: пристосовувати вже існуючі системи до сучасних умов або будувати нові, які будуть враховувати обставини воєнного часу. Враховуючи досвід практично 3-х років активних бойових дій в Україні, можна зробити висновок, що резильєнтність МСЖ найвища в тих регіонах, де є альтернативні джерела енергії, інфраструктуру вдалось забезпечить захистом та вплив військових дій мінімальний.

Тому, щоб збільшити резильєнтність інфраструктури потрібно захистити критичні об'єкти та розвивати альтернативні системи. Прикладом захисту може бути фізичне укріплення об’єктів водо-, електро-, теплопостачання та комунікацій, використання підземних мереж для зменшення вразливості від обстрілів, захист насосних станцій, ТЕЦ і очисних споруд. Розвитком альтернативних систем можна вважати: для води - мобільні очисні установки, резервуари для зберігання води, системи збору

дощової води, буріння свердловин; для електроенергії – сонячні панелі, вітрові турбіни, різні генератори, та системи накопичення; для комунікації – резервні канали зв'язку, супутникові технології.

Класичним прикладом таких заходів може служити м. Миколаїв, де йде процес введення в експлуатацію двох когенераційних установок потужністю 1,5 МВт кожна, які будуть здатні забезпечити теплом понад 200 багатоквартирних житлових будинків, 5 медичних та 24 освітніх закладів [3].

Кліматичні зміни, як правило, не залежать від бойових дій та різняться від регіону до регіону. Так, через глобальне потепління та зміни у кліматі, кількість сонячних днів в Україні стає все більшою, а також збільшується і середньорічна температура повітря [4]. Тому є можливість та потреба використати ці фактори для збільшення резильєнтності МСЖ, а також адоптувати цивільну інфраструктуру до таких змін. Прикладом є встановлення сонячних панелей на дахах багатоповерхівок, утеплення стін будинків. Наразі існує багато інноваційних технологій, які можна використати як під час військових дій, так і в мирний час: розбудова розумних міст (smart cities), де використаються інтелектуальні системи управління енергоспоживанням, а також розвиток мікромереж (microgrids), які можуть функціонувати незалежно від центральної енергосистеми. Резильєнтність міських систем життєзабезпечення в умовах війни потребує інтегрованого підходу, що поєднує інфраструктурні, соціальні, екологічні та технологічні рішення. Це дасть можливість забезпечення життєдіяльності міста навіть у кризових умовах і буде сприяти швидкому відновленню після надзвичайних подій. На додаток, після закінчення військових дій на території України буде багато практичних кейсів, а не теоретичних моделей, які можуть бути використані іншими країнами для підвищення резильєнтності МСЖ до кліматичних змін, надзвичайних подій та техногенних аварій, які були впроваджені у воєнний час, тому з великою ймовірність будуть успішні і в мирний час.

1. Забезпечення водопостачання в м. Миколаїв, офіційний сайт Національного університету водогосподарства та природокористування URL: https://nuwm.edu.ua/university/news/zabezpechennia-vodopostachannia-m-mykolaiv?utm_source=chatgpt.com.
2. Протягом наступного тижня в місті буде відновлено централізоване водопостачання 07.05.2022, сайт Миколаївводоканалу, URL: https://www.vodokanal.mk.ua/uk/noviny/novini/protiagom-nastupnogo-tizhnia-v-misti-bude-vidnovleno-tcentralizovane-vodopostachannia-686.
3. Продовжуємо активну роботу з посилення захисту енергооб'єктів, — Прем'єр-міністр під час робочої поїздки на Миколаївщину, Урядовий портал, URL: https://www.kmu.gov.ua/news/prodovzhuiemo-aktyvnu-robotu-z-posylennia-zakhystu-enerhoobiektiv-premier-ministr-pid-chas-robochoi-poizdky-na-mykolaivshchynu.
4. Wilson, L., New, S., Daron, J., Golding, N. (2021). Climate Change Impacts for Ukraine. Met Office, URL: https://mepr.gov.ua/wp-content/uploads/2023/07/2_Vplyv-zminy-klimatu-v-Ukrayini.pdf.

В.О. Дерій, О.В. Згуровець

ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ POWER-TO-HEAT ДЛЯ ПІДВИЩЕННЯ РЕЗИЛЬЄНТНОСТІ ЦЕНТРАЛІЗОВАНОГО ТЕПЛОПОСТАЧАННЯ

Вступ

Різке зростання частки відновлюваних джерел енергії (ВДЕ), таких як сонячні та вітрові електростанції, у структурі генерації енергосистеми України створює суттєві виклики для її стабільної роботи. Стохастичний характер генерації ВДЕ призводить до періодичного профіциту електроенергії, що ускладнює балансування потужності та регулювання частоти в енергомережі. З іншого боку, у пікові періоди споживання виникає дефіцит, що загрожує стабільності постачання.

Технологія Power-to-Heat (PtH) пропонує перспективне рішення цих проблем. Вона дозволяє перетворювати надлишкову електроенергію на теплову, яку можна використовувати для забезпечення систем централізованого теплопостачання (СЦТ) [1,2].

Застосування такого підходу технології PtH не лише допомагає утилізувати надлишкову енергію, але й знижує залежність від викопного палива, сприяючи декарбонізації енергетичного сектора.

Основні принципи технології Power-to-Heat

Технологія PtH базується на використанні електричних теплогенераторів, таких як електричні котли чи теплові насоси, які здатні ефективно перетворювати електроенергію на теплову. Крім того, система включає акумулятори теплової енергії, які дозволяють зберігати отриману теплоту для подальшого використання у періоди підвищеного попиту.

Важливим аспектом є інтеграція PtH у СЦТ, що створює можливості для скорочення використання викопного палива та зниження викидів парникових газів в цьому секторі.

Ефективність впровадження PtH залежить від грамотного вибору потужності електричних теплогенераторів та ємності акумуляторів. Важливу роль також відіграє розробка стратегії управління, яка враховує специфіку роботи міських СЦТ України, що пов’язана з їх високою централізацією та потребує адаптації існуючих підходів до впровадження новітніх технологій.

Виклики та рішення для впровадження PtH

Використання ВДЕ в енергосистемі супроводжується природною нестабільністю, яка ускладнює балансування між виробництвом і споживанням електроенергії. Для України це є серйозним викликом, враховуючи застаріле енергетичне обладнання та недостатню кількість маневрених потужностей на фоні руйнувань інфраструктури, що викликані агресією росії. Початкові інвестиції у впровадження PtH також можуть бути значними через високу вартість обладнання та необхідність модернізації інфраструктури.

Однак варто зазначити, що перспективи застосування технології Power-to-Heat досить широкі. Так, використання теплових насосів дозволяє утилізувати низькопотенційне тепло, що значно підвищує ефективність системи. В той же час, інтеграція PtH із акумуляторами теплової енергії відкриває можливість балансування пікових навантажень, а розробка математичних моделей дозволяє прогнозувати роботу систем із урахуванням динаміки генерації ВДЕ та споживання енергії. Таким чином, PtH може стати ключовим елементом підвищення стійкості енергосистеми України.

Економічні та екологічні переваги використання PtH

Втрати від обмеження генерації ВДЕ через профіцит електроенергії дуже значні. Зокрема, у 2021 році ці втрати в Україні оцінювалися у 17,2 млн євро [3]. Технологія PtH здатна мінімізувати такі збитки, забезпечуючи ефективну утилізацію надлишкової електроенергії. Більше того, впровадження цієї технології сприяє зниженню витрат на імпорт викопного палива, що є критично важливим для енергетичної незалежності країни.

З екологічної точки зору, PtH сприяє істотному скороченню викидів парникових газів. Зменшення обсягів використання викопного палива узгоджується з кліматичними цілями України, гармонізуючи її енергетичну політику з європейськими стандартами. Це робить PtH важливим кроком на шляху до декарбонізації енергетичного сектора.

Перспективи впровадження PtH в Україні

Україна має унікальні можливості для адаптації міжнародного досвіду у сфері Power-to-Heat. У багатьох країнах ЄС, зокрема Данії та Німеччині, PtH вже інтегровано у гібридні системи теплопостачання, які довели свою ефективність у скороченні паливних витрат та зниженні викидів парникових газів [4-7]. Для успішного впровадження технології PtH в Україні необхідно створювати пілотні проєкти у великих містах, які дозволять оцінити її економічну та технічну доцільність.

Крім того, модернізація існуючих СЦТ може стати базою для інтеграції PtH. Фінансова підтримка, зокрема через державні програми та міжнародні гранти, сприятиме подоланню інвестиційних бар'єрів. Впровадження PtH може стати прикладом успішної трансформації енергетичного сектора України.

Висновки

Технологія Power-to-Heat є перспективним рішенням для підвищення резильєнтності енергосистем України. Вона дозволяє ефективно утилізувати надлишкову електроенергію, знижує залежність від викопного палива та сприяє скороченню викидів парникових газів. Економічна вигода від цієї технології включає зменшення витрат на регулювання енергосистеми та зниження залежності від імпортованих ресурсів.

Для успішної реалізації PtH необхідно забезпечити поєднання міжнародного досвіду з локальними особливостями енергетичної системи України. Інвестиції в інфраструктуру, впровадження інноваційних підходів до управління та співпраця з міжнародними партнерами є ключовими чинниками, які визначатимуть успіх цієї технології у майбутньому.

1. International Renewable Energy Agency (IRENA). (2019). Renewable power-to-heat: Innovation landscape brief. Retrieved from https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2019/Sep/IRENA_Power-to-heat_2019.pdf?la=en&hash=524C1BFD59EC03FD44508F8D7CFB84CEC317A299 (accessed December 10, 2024).
2. Federal Ministry for Economic Affairs and Climate Action (BMWK). (2016, April 22). What exactly is meant by 'power-to-heat'? Energiewende Direct. Retrieved from https://www.bmwk-energiewende.de/EWD/Redaktion/EN/Newsletter/2016/07/Meldung/direkt-answers.html (accessed February 6, 2024).
3. Укренерго. (2020). Інтеграція ВДЕ в енергосистему України. Retrieved from https://ua.energy/zagalni-novyny/u-2020-rotsi-vstanovlena-potuzhnist-ves-ta-ses-zrosla-na-41-a-yihnya-chastka-u-strukturi-vyrobnytstva-elektroenergiyi-vdvichi/ (accessed June 3, 2020).
4. Interreg Baltic Sea Region, European Union, European Regional Development Fund. (2021). Power-to-Heat & Power-to-Gas in district heating systems. Retrieved from https://www.lowtemp.eu/wp-content/uploads/2021/01/BackgroundInfo_Power-to-Heat-and-Power-to-X_LowTEMP.pdf (accessed June 7, 2023).
5. Hers, S., Afman, M., Cherif, S., & Rooijers, F. (2021). Potential for Power-to-Heat in the Netherlands. Retrieved from https://cedelft.eu/wp-content/uploads/sites/2/2021/04/CE_Delft_3E04_Potential_for_P2H_in_Netherlands_DEF.pdf (accessed June 7, 2023).
6. Schweiger, G., Rantzer, J., Ericsson, K., & Lauenburg, P. (2017). The potential of power-to-heat in Swedish district heating systems. Energy, 137, 661–669. https://doi.org/10.1016/j.energy.2017.02.075
7. Bloess, A., Schill, W.-P., & Zerrahn, A. (2018). Power-to-heat for renewable energy integration: A review of technologies, modeling approaches, and flexibility potentials. Applied Energy. Retrieved from https://www.sciencedirect.com/science/article/pii/S0306261917317889 (accessed June 9, 2023).

В.В. Шкарупило, В.В. Душеба, Т.А. Зайко, В.В. Шкарупило

ПІДХІД ДО ЗАБЕЗПЕЧЕННЯ РЕЗИЛІЄНТНОСТІ ЗГІДНО ПРИНЦИПІВ БАГАТОВИМІРНОЇ ВЕРИФІКАЦІЇ

У відповідності до концепції багатовимірної верифікації [1], згідно якої опрацьованими мають бути показники як функціональних (ФХ), так і нефункціональних характеристик (НФХ) розроблюваної програмної системи, у межах представленого підходу пропонується розглядати засади забезпечення резилієнтності вже на етапі проєктування у складі етапів процесу розроблення [2]. Специфіку запропонованого підходу графічно представлено на рисунку 1, із застосуванням виразних засобів UML (Unified Modeling Language).

Рисунок 1 – Графічне подання підходу

На рисунку 1 фігурують умовні позначення, що представляють відповідні типи артефактів: ПА – первинні артефакти; ВА – вихідні; РА – результуючі. У вигляді коментарів зведено форми подання представників вказаних типів. Тип ПА охоплює артефакти, що, у загальному випадку, є неформалізованими, і призначеними для опосередкованого їх опрацювання на предмет контролю за показниками і ФХ, і НФХ. Опосередкованість, у свою чергу, реалізовано шляхом поступального застосування розроблених правил перетворення неформалізованих подань у формалізовані: у артефакти типу ВА [3, 4]; наступним кроком – у артефакти типу РА. Представники типів ВА і РА – похідні формалізовані подання – як засоби уможливлення проведення контролю, відповідно, за показниками ФХ і НФХ.

У якості показника ФХ пропонується опрацьовувати несуперечливість програмно-алгоритмічної складової, шляхом проведення формальної верифікації методом перевірки на моделі TLC (TLA Checker) [5]; у якості показника НФХ – супутні часові витрати.

Результати проведеного аналізу праць у напрямі забезпечення резилієнтності енергетичної інфраструктури надають підстави вважати доцільним застосування представленого підходу у частині опрацювання кібернетичної складової вказаної інфраструктури, при розробленні або дослідженні відповідного програмно-алгоритмічного забезпечення [6].

Дослідження проведено в рамках вирішення задач наступних науково-дослідних робіт, виконуваних в Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України: НДР № 0120U102683 «Розроблення спеціалізованих комп'ютерних технологій моделювання та опрацювання оперативної інформації в задачах енергетики»; «Кіберризики та кіберзахищеність топології розподілених інформаційних систем в глобальному кіберпросторі», за договором з МОН України № РН/15 – 2023 від 24.05.2023; W911NF-22-2-0153 research work, funded by the US Army Engineer Research and Development Center (ERDC).

1. Jenihhin, M., Lai, X., Ghasempouri, T., & Raik, J. (2018). Towards multidimensional verification: where functional meets non-functional. *NORCHIP and International Symposium of System-on-Chip (SoC): 2018 IEEE Nordic Circuits and Systems Conference*, Tallinn, Estonia, 30-31 Oct. 2018. 1–7. https://arxiv.org/ftp/arxiv/papers/1908/1908.00314.pdf.
2. Шкарупило, В.В., & Душеба, В.В. (2022). Спадковість артефактів у контексті багатовимірної верифікації. *Тиждень науки-2022: науково-практ. конф., 18–22 квітня 2022 р.: тези доп. Запоріжжя: НУ "Запорізька політехніка"*, 789–791.
3. Шкарупило, В.В., Чемерис, О.А., Душеба, В.В., Кудерметов, Р.К., & Польська, О.В. (2020). Метод синтезу формальних специфікацій на основі трійок Хоара. *Наукові праці ДонНТУ, Серія "Інформатика, кібернетика та обчислювальна техніка"*, 1(30), 49–57. https://iktv.donntu.edu.ua/wp-content/uploads/2021/01/07_Shkarupylo.pdf.
4. 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.
5. 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.
6. Shkarupylo, V., Chemerys, O., Artemchuk, V., Alsayaydeh, J., Kudermetov, R., & Polska, O. (2024). Comprehensive stratified approach to energy resilience solutions taxonomy: a Ukraine scenario. Proc. *14th International Conference on Dependable Systems, Services and Technologies*, Greece, Athens, October 11-13, 2024. (in press).

В.В. Шкарупило, В.В. Душеба

НАПРЯМИ РОЗВИНЕННЯ РЕЗИЛІЄНТНОСТІ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ

Пропонується застосовувати комплексний підхід до охоплення аспектів забезпечення резилієнтності енергетичної інфраструктури, у відповідності до раніше представленої тривимірної концепції [1].

Комплексність вказаного підходу полягає у послідовному опрацюванні трьох виокремлених концептуальних площин: стосовно основоположного принципу у напрямі забезпечення резилієнтності; у контексті варіювання рівня деталізації сприйняття енергетичної інфраструктури розробником / дослідником; у частині концептуальної спрямованості окремого рішення при розгляді зазначеної інфраструктури як кіберфізичної системи [2, 3]. Представлений підхід побудовано у відповідності до згаданої концепції (рис. 1) [1].

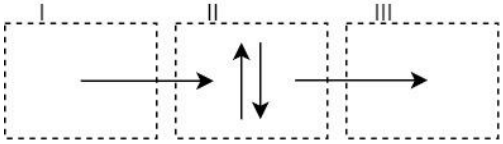


Рисунок 1 – Графічне представлення розробленого підходу

На рисунку 1 прямокутними пунктирними областями зображено озвучені вище виокремлені концептуальні площини, пронумеровані зліва направо. Стрілками подано напрям і специфіку виконуваних кроків:

1. На початковому кроці опрацьовуються засади площини I. Означено класифікацію рішень, спрямованих на забезпечення резилієнтності, – за аналогією до підходу, застосованого для групування шаблонів проєктування, використовуваних розробниками програмних систем [4]. За основоположним принципом виокремлюються рішення, у межах яких забезпечення резилієнтності реалізується або шляхом впровадження відповідних державних політик та / або стратегій, або шляхом розвинення архітектурної складової досліджуваної енергосистеми. Я якості «архітектури» при цьому розглядається сукупне поняття, що охоплює поняття «структури» і «зв'язків».

2. На другому кроці розглядаються компоненти площини II. За рахунок зміщення між ієрархічними рівнями (стратами) як засобами варіювання рівня деталізації, окреслюється масштаб енергосистеми, на який орієнтоване певне рішення у частині забезпечення резилієнтності.

3. За умови розгляду енергетичної інфраструктури як кіберфізичної системи [5], для обраного на попередньому кроці масштабу енергосистеми опрацьовується відповідна концептуальна площина (фізична та / або кібернетична), у межах якої забезпечується резилієнтність.

Результати проведених досліджень, організованих у відповідності до представленого підходу (рис. 1), дали підстави вважати, що серед перспективних напрямів забезпечення резилієнтності енергетичної інфраструктури, є, у тому числі, наступні: реалізовані шляхом розвинення архітектурної складової (площина I), із акцентом на опрацюванні кібернетичної складової (площина III) [6].

Дослідження проведено в рамках вирішення задач наступних науково-дослідних робіт, виконуваних в Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України: НДР № 0120U102683 «Розроблення спеціалізованих комп'ютерних технологій моделювання та опрацювання оперативної інформації в задачах енергетики»; «Кіберризики та кіберзахищеність топології розподілених інформаційних систем в глобальному кіберпросторі», за договором з МОН України № РН/15 – 2023 від 24.05.2023; W911NF-22-2-0153 research work, funded by the US Army Engineer Research and Development Center (ERDC).

1. Шкарупило, В.В., Душеба, В.В., & Чемерис, О.А. (2024). Щодо тривимірної концепції опрацювання резилієнтності енергетичної інфраструктури. *Безпека енергетики в епоху цифрової трансформації: Шоста науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України*, Київ, Україна, 13 грудня, 2024 р. Київ : ІПМЕ ім. Г.Є. Пухова НАН України. 176-177. https://ipme.kiev.ua/konferencii/naukovo-praktichna-konferenciya-bevect-2024/.
2. Шкарупило, В.В., Чемерис, О.А., & Душеба, В.В. (2024). Стратифікований підхід до опрацювання резилієнтності у галузі енергетики. *Збірник матеріалів XLII Науково-технічної конференції молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України*, м. Київ, 15 травня 2024 р., 54-55. https://ipme.kiev.ua/konferencii/konferenciya-molodix-vchenix-2024/.
3. Шкарупило, В.В., Душеба, В.В., & Тіменко, А.В. (2023). Огляд рівнів забезпечення резилієнтності у галузі енергетики. Survivability & Resilience – 2023: collection of materials of the international scientific and practical conference, Kyiv, October 19, 2023, PIMEE of NAS of Ukraine, 33-34. https://ipme.kiev.ua/konferencii/zhivuchist-ta-rezilyentnist-2023/.
4. Gamma, E., Helm, R., Johnson, R., & Vlissides, J. (1993). Design patterns: abstraction and reuse of object-oriented design. In: Nierstrasz, O.M. (Eds.) ECOOP' 93 – Object-Oriented Programming. ECOOP 1993. *Lecture Notes in Computer Science*, 707. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-47910-4_21
5. Shkarupylo, V.V., Kudermetov, R.K., & Polska, O.V. (2018). On the approaches to cyber-physical systems simulation. *Advances in Cyber-Physical Systems (ACPS)*, 3(1), 51-54. https://doi.org/10.23939/acps2018.01.051.
6. Shkarupylo, V., Chemerys, O., Artemchuk, V., Alsayaydeh, J., Kudermetov, R., & Polska, O. (2024). Comprehensive stratified approach to energy resilience solutions taxonomy: a Ukraine scenario. Proc. *14th International Conference on Dependable Systems, Services and Technologies*, Greece, Athens, October 11-13, 2024. (in press).

Ю.О. Кириленко

ПИТАННЯ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ В КОНТЕКСТІ ГОТОВНОСТІ ДО ПОТЕНЦІЙНИХ ПОДІЙ НА ТИМЧАСОВО ОКУПОВАНОМУ ЯДЕРНОМУ ОБ'ЄКТІ

З початку повномасштабного вторгнення, перед системою аварійної готовності та реагування постала низка викликів, які продовжують доповнюватися з кожним днем російської агресії проти України. У світлі тимчасової окупації Запорізької АЕС – ядерної установки категорії аварійної готовності І в термінах МАГАТЕ [1], – прогностичні можливості кризових центрів та наукових установ по всьому світу відіграють все більшу роль в аналізі ситуації та репрезентації актуального рівня ризику навколо окупованого майданчика АЕС.

У світлі суттєвих невизначеностей щодо можливих вихідних подій та перебігу аварійних процесів, які можуть мати місце на Запорізькій АЕС, напрацювання джерел аварійних викидів для ряду кінцевих станів енергоблоків Запорізької АЕС можуть доповнити існуючу бібліотеку аварійних джерел для подальшого використання в задачах, пов'язаних з аварійною готовністю та реагуванням на надзвичайні ситуації. Актуалізація бібліотек джерел аварійних викидів та регулярне проведення розрахунків атмосферної дисперсії дають важливе розуміння очікуваних масштабів наслідків ситуацій, які можуть скластися на АЕС під час особливого періоду.

Додаткові дослідження, пов'язані з потенційними впливами військового характеру, можуть розширити перелік референтних подій, що розглядаються в практиці аварійної готовності та реагування [2], а також, можуть бути застосовані з метою інформування громадськості задля зменшення занепокоєння громадськості шляхом встановлення обґрунтованих очікувань щодо потенційних наслідків можливих подій. Результати оцінки радіаційних наслідків потенційних подій на Запорізькій АЕС можуть стати важливим підґрунтям для прийняття рішень з фізичного захисту та Збройними силами України з метою радіаційного захисту та планування.

Готовність до події, яка може виникнути в результаті військових дій навколо ядерної установки, вимагає розуміння реакції систем і елементів станції на потенційні військові загрози. В той же час, діапазон потенційних радіологічних наслідків для населення має бути визначеним на основі експертних припущень, поточної ситуації та потенційного характеру впливу на ядерну установку. Опитування ключових експертів за певним напрямком ядерної та радіаційної безпеки може стати основою для ранжування аварій сценаріїв.

Оцінки ізотопного складу ядерного матеріалу, що міститься на захопленому об'єкті повинні бути підготовлені для різних умов тривалої зупинки. Зокрема, слід розглянути декілька експлуатаційних станів ядерної

установки (наприклад, «холодний» зупин, «гарячий» зупин, мінімально-контрольований рівень потужності, пуск і робота реактора на проміжних рівнях потужності). Така підготовка може вимагати проведення додаткових нейтронно-фізичних розрахунків.

Очікувані частки викиду можуть бути обрані на основі наявних даних, розглянутих для відповідних типів установок, що розміщені на майданчику об'єкта. Цілісність фізичних бар'єрів відіграватиме чи не найважливішу роль в оцінці джерела викиду, моделюванні атмосферного розсіювання і результатах прогнозування дози опромінення репрезентативної особи з населення. Орієнтовне джерело викиду має бути уточнене на основі перших доступних радіаційного моніторингу.

Якщо фактична інформація про статус об'єкта залишається недоступною, конкретні рівні дій можуть бути визначені, наприклад, в термінах потужності дози гамма-випромінювання для стаціонарних постів радіаційного моніторингу на підконтрольних державі територіях. Їх перевищення може надати уявлення про розвиток аварії на об'єкті. Асиміляція даних моніторингу до системи підтримки прийняття рішень повинна бути організована для поточної конфігурації мережі радіаційного моніторингу та інструменту прогнозування дози, що використовується.

Допоміжні організаційні процедури та ресурси можуть бути підготовлені до фази реагування, однак, більшість з них може бути заснована на процедурах, призначених для використання в мирний час, але адаптованих до умов воєнного часу. Наприклад, існуючі механізми і процедури реагування, такі як визначення розмірів та меж зон аварійного планування на випадок надзвичайних ситуацій, повинні бути доповнені спеціальними процедурами реагування в умовах війни.

Разом з тривалою агресією російської федерації, Україна продовжує переживати важливий етап розвитку та вдосконалення процедур готовності та реагування на можливі події на захопленому ядерному об’єкті. Отриманий досвід може стати запорукою високого рівня готовності як під час війни, так і в післявоєнний період.

1. General Safety Requirements. Part 7. Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards, IAEA, 2015. https://www-pub.iaea.org/MTCD/Publications/PDF/P_1708_web.pdf.
2. IAEA-TECDOC-955 Generic assessment procedures for determining protective actions during a reactor accident, 1997 https://www-pub.iaea.org/MTCD/Publications/PDF/te_955_prn.pdf.

I.O. Dubovkina

ALTERNATING IMPULSES OF PRESSURE for TREATMENT of LIQUID NUTRIENT SOLUTION

Now we can see as soil degradation continues and freshwater supplies become scarce, development of farming approaches that use both land and water more efficiently and productively to grow food is essential. That's why this need has created a niche for scientists and farmers to develop techniques to improve either land productivity or to use alternative agricultural techniques [1].

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

Regrettably, farming is also believed to be the main cause of climate change, biodiversity loss, and degradation of land and clean water. as a consequence, it is important to consider other methods and processes of plant cultivation to continue the environment and support global population growth.

The use of greenhouses, vertical farms, aquaponics, hydroponics, and other plant growing methods have thus been studied and implemented over the years[3].

Plants growing under greenhouses can grow protected from severe weather conditions such as hail, snow, extreme low temperatures or excessive high temperature; while at the same time can allow cultivations of out-of-season variety.

Non-soil based production systems have emerged as sustainable options for food production. Among other agricultural systems, the opportunities soilness systems present are becoming more evident.

In hydroponic systems, the potential of hydrogen is constantly changing as the plant grows. Therefore pH control is a requirement in hydroponic solutions, because the plant growth depends on this.

The pH range from 5,5 to 7,5 is most favorable for the availability of nutrients from most water nutrient solutions.

The method of alternating impulses of pressure is one of the methods of controlled energy impact with many hydrodynamic effects, such as power of pressure of shift, cavitations, the effect of explosive boiling, collective effects in assembly of vials, crossness of an interphase surface in gas-liquid bubbly medium, action of hydrodynamic oscillations, alternating impulses of pressure, effects which associated with acceleration of movement of a continuous phase.

The most important effects of the alternating impulses of pressure are allied with increase of velocity of association of a continuous phase of medium.

The analytical chemistry and chemical methods were used for the researches physical and chemical parameters of the aquatic solutions.There are different types of hydroponic systems[4].

The aim of this scientific work is to investigate the influence of the application of alternating impulses of pressure all through processing in foodstuff

production by the modification physical and chemical properties of the liquid nutrient solutions and mediums for hydroponic systems.

The hydroponic system from recirculation technological mode of greenhouse in the technological processes of the growing crops is exceptionally multiple constituent elements complex organic organization which includes many types of biotic organisms [5].

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

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

Through researches increases pH of the pure water on 15.5% have been established, thus the hydrogen potential of the water prepared on technology for hydroponic system has raised on 15-20%.

Experimental investigations of the testing growing crops are demonstrated increasing the the productivity of the growing crops yield of green biomass on 32.8-34%. Growth rate for testing growing crops was arising on 20.5-24.4%.

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

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

1. Chadwick J.J., Witteveen A., Zhang P., Lynch I. (2023), Hydroponics and alternative forms ofagriculture: opportunities from nanotechnology. *Nano-Enabled Sustainable and Precision Agriculture*, pp. 259-272, https://doi.org/10.1016/B978-0-323-91233-4.00018-1.
2. Foley J. A., Ramankutty N., Brauman K. A. (2011), Solutions for a cultivated planet, *Nature*, vol. 478, №. 7369, pp. 337-342, doi:10.1038/nature10452.
3. Asiabanpour B., Estrada A., Ramirez R., Downey M. S. (2018), Optimizing Natural Light Distribution for Indoor Plant GrowthUsing PMMA Optical Fiber: Simulation and Empirical Study Hindawi *Journal of Renewable Energy*, V. 18, Article ID 9429867, 10 pages .https://doi.org/10.1155/2018/942986.7.
4. Edited by Kenneth I.Ozomwna (2007), Recent Advances in Analitycal Electrochemistry, *Transword Research Network*, 300 p. Available at: Network.http://www.ressign.com/UserBookDetail.aspx?bkid=605&catid=160.
5. Mamta D. Sardare, Shraddha V. Admane (2013), A Review on Plant without Soil – Hydroponics. International Journal of Research in Engineering and Technology Volume 2, Issure 3, 299-304 https://www.ijret.org.

К.В. Васильєв

ІДЕНТИФІКАЦІЯ ЕЛЕКТРОТЕХНІЧНИХ СИСТЕМ ТА ПРИСТРОЇВ НА ОСНОВІ КЛАСИФІКАЦІЙНИХ МОДЕЛЕЙ ШТУЧНОГО ІНТЕЛЕКТУ

Кібербезпека для комп'ютерних систем реального часу має критичне значення, оскільки такі системи функціонують у середовищах, де помилки або затримки можуть мати серйозні наслідки, включаючи шкоду для людей, втрати ресурсів чи компрометацію систем. Основні аспекти значення кібербезпеки для таких систем наведені нижче:

Ідентифікація електричних систем та пристроїв за допомогою класифікаційних моделей штучного інтелекту є значним досягненням сучасної інженерії. Використовуючи алгоритми машинного навчання, ці моделі аналізують закономірності в електричних сигналах для точного розпізнавання пристроїв і моніторингу стану системи. Такий підхід підвищує ефективність, підтримує профілактичне обслуговування та забезпечує безперебійну роботу складних систем, таких як інтелектуальні мережі так і IoT-мережі. Оскільки технологія штучного інтелекту продовжує розвиватися, її інтеграція в електричні системи обіцяє ще більше інновацій в автоматизації та управлінні системами.

Для ефективного вирішення задач керування електротехнічними об'єктами (ЕТО), діагностики їхніх внутрішніх параметрів і станів, важливо створити математичну модель, яка максимально відповідає поставленій меті, будь то управління, прогнозування чи діагностика. Це завдання вирішується за допомогою теорії ідентифікації — математичного підходу до пізнання властивостей і поведінки об'єктів реального світу, включаючи ЕТО.

Одним із ключових інструментів для вирішення подібних задач є системний підхід, де система ідентифікації розглядається як частина багаторівневої структури, що базується на принципах декомпозиції, композиції та оптимізації. Стан системи при цьому виступає окремим об'єктом ідентифікації, що вивчається із використанням статистичних методів. Для первинного аналізу причинно-наслідкових зв'язків у ЕТО застосовується регресійний аналіз. Однак у реальних умовах статистичні методи можуть бути неоптимальними через вплив неточностей, які виникають не лише у вимірюванні результатів, але й у визначенні причинних факторів. Тому доцільно використовувати додаткові підходи, здатні враховувати ці похибки [1].

Моделі класифікації на основі ШІ використовують алгоритми машинного навчання для аналізу електричних сигналів, таких як струм, напруга і гармоніки, щоб ідентифікувати унікальні підписи пристроїв. Такі методи, як глибокі нейронні мережі, машини опорних векторів і дерева рішень, дозволяють точно розпізнавати підключені пристрої, прогнозувати

несправності та оптимізувати розподіл енергії. Ця методологія не тільки підвищує ефективність системи, але й підвищує відмовостійкість [2].

Застосування штучного інтелекту в цій галузі охоплює кілька критично важливих сфер. Наприклад, у «розумних» мережах AI-моделі використовуються для балансування навантаження та мінімізації втрат енергії. У промисловому контексті ШІ підтримує превентивне технічне обслуговування, виявляючи несправності обладнання на ранніх стадіях. Тим часом в екосистемах Інтернету речей ці моделі забезпечують безпечну та ефективну ідентифікацію та управління пристроями [3].

Незважаючи на свої переваги, інтеграція штучного інтелекту в електричні системи пов'язана з певними проблемами, зокрема з необхідністю отримання високоякісних даних, обчислювальної масштабованості для великомасштабних систем і надійних заходів кібербезпеки для захисту від потенційних загроз. Вирішення цих питань має вирішальне значення для широкого впровадження [4,5].

Майбутні розробки в цій галузі зосереджені на периферійних обчисленнях для обробки даних у реальному часі, підвищенні точності моделей за допомогою передових методів глибокого навчання та подальшій інтеграції з відновлюваними джерелами енергії. Потенціал моделей класифікації на основі ШІ для революції в управлінні енергією та автоматизації залишається значним.

1. Сильвестров А. Н. Идентификация и оптимизация автоматических систем / А. Н. Сильвестров, П. И. Чинаев. — М. : Энергоатомиздат, 1987. — 200 с.
2. Vamvakas, D.; Michailidis, P.; Korkas, C.; Kosmatopoulos, E. Review and Evaluation of Reinforcement Learning Frameworks on Smart Grid Applications. Energies 2023, 16, 5326. https://doi.org/10.3390/en16145326.
3. W. Villegas-Ch, J. García-Ortiz and S. Sánchez-Viteri, "Toward Intelligent Monitoring in IoT: AI Applications for Real-Time Analysis and Prediction," in IEEE Access, vol. 12, pp. 40368-40386, 2024, doi: 10.1109/ACCESS.2024.3376707.
4. Geo-Intelligent Architecture for Smart Grid Evolution: Addressing Contemporary Challenges through Spatial AI and Knowledge Integration. In Proceedings of the 2023 4th Asia Service Sciences and Software Engineering Conference (ASSE '23). Association for Computing Machinery, New York, NY, USA, 171–180. https://doi.org/10.1145/3634814.3634838.
5. Amiri, M.M., Jalilian, A., Abdi, H., Rezaei, M., Nazari-Heris, M. (2024). New Trends for Machine Learning Applications in Future Power Systems. In: Azad, S., Nazari-Heris, M. (eds) Artificial Intelligence in the Operation and Control of Digitalized Power Systems. Power Systems. Springer, Cham. https://doi.org/10.1007/978-3-031-69358-8_4.

А.М. Давиденко, С.Я. Гільгурт, О.Г. Кіслов, В.М. Попова

ВИЯВЛЕННЯ АТАК НА SCADA-СИСТЕМИ ЦИФРОВИХ ПІДСТАНЦІЇ

Цифровізація систем автоматики та АСУ ТП привносить в роботу промислових систем ризики інформаційної безпеки, які можуть бути більш катастрофічними порівняно з традиційними галузями застосування інформаційних технологій [1]. Засоби технічного захисту таких критичних об'єктів, як цифрові електричні підстанції (ЦПС), побудовані згідно стандарту МЕК 61850, успадковують більшість рис традиційних для IT інструментів кіберзахисту, але мають і певну специфіку. Метою даного дослідження було виявити специфічні відмінності систем виявлення вторгнень (СВВ), спрямованих на захист SCADA-систем для ЦПС.

Відповідно до стандарту МЕК 61850 система автоматизації інформаційного обміну на енергооб'єкті за схемою ЦПС складається з трьох рівнів: станційний (Station Level) – найвищій рівень, рівень приєднання (Bay Level) та рівень процесу (Process Level) або "польовий" (Field Level) – найнижчий рівень [2]. Кожен рівень виконує притаманні йому функції, за які відповідають певні типи пристроїв. Комунікації можливі як всередині рівнів (горизонтальні), так і між рівнями (вертикальні).

Специфіка та відмінності функціонування ЦПС (на базі стандарту МЕК 61850) від традиційних об’єктів IT-галузі обумовлює й особливості СВВ, що створюються для їх захисту [3]. Розуміння потенційних вразливостей мереж і пристроїв цифрових підстанцій, які можуть погіршити конфіденційність, доступність і цілісність даних, має вирішальне значення для розробки відповідних контрзаходів безпеки та механізмів виявлення вторгнень. Несанкціонований віддалений доступ до мереж підстанції дозволяє зловмиснику обходити фізичний захист і завдавати ЦПС катастрофічної шкоди [4].

Розслідування відомих атак на енергооб'єкти дозволяють проаналізувати поведінку зловмисника, який вже отримав несанкціонований доступ до мережі SCADA-системи ЦПС. При цьому важливо враховувати максимум чинників, починаючи з відомостей про логіку поведінки системи на фізичному рівні (включаючи засоби живлення) й до сучасних підходів створення засобів IT-безпеки [5]. Дотримуючись такого підходу можна виділити чотири підходи до виявлення вторгнень:

1) на рівні контролю доступу – Access-Control Detection (ACD);

2) з використанням білого списку протоколів – Protocol Whitelisting Detection (PWD);

3) на основі моделі – Model-based Detection (MBD);

4) багатопараметричне виявлення вторгнень – Multi-Parameter based Detection (MPD).

Напрям ACD реалізує стратегією, схожу на білий список стосовно

контролю доступу, яка охоплює MAC-адреси на рівні Ethernet, IP-адреси на мережевому рівні та TCP-порти на транспортному рівні (для мережевого трафіку згідно МЕК 61850 використовується TCP порт номер 102).

Підхід PWD працює на всіх рівнях моделі OSI крім фізичного та крім типових для IT-галузі протоколів має справу зі специфічними протоколами ЦПС: MMS, COTP, TPKT, SNTP, GOOSE, SMV та IEEE 1588. Детектор СВВ налаштовується таким чином, щоб дозволяти роботу лише припустимих на відповідному рівні протоколів.

Підхід MBD аналізує файли опису конфігурації ЦПС та зміст поточного трафіку з протоколів МЕК 61850, визначає штатну поведінку, порівнює її профілі з реальним трафіком та виявляє відхилення. При цьому враховуються такі відмінності мережі SCADA-систем ЦПС, як регулярні потоки трафіку й передбачуваність поведінки. Таким чином, підхід MBD демонструє потенціал для ідентифікації як зловмисних атак, так і ненавмисних аномалій – на станційному рівні та на рівні процесу.

Ідея багатопараметричного напряму MPD полягає у виявленні можливих загроз для SCADA-системи, що є результатом або внутрішнього ненавмисного використання, або зовнішніх зловмисних атак шляхом моніторингу найбільш чутливих параметрів ЦПС. Ці багатовимірні параметри пов'язані з безпечною та стабільною роботою інтелектуальної підстанції, наприклад дані дистанційного вимірювання та дистанційної сигналізації від станційної шини та шини процесу згідно МЕК 61850. Стратегії багатопараметричного виявлення, такі як критична кореляція сигналу перемикання та порівняння ключового аналогового сигналу, використовують фізичні знання та досвіду експлуатації цифрових підстанцій.

Отримані в данному дослідженні результати дозволяють забезпечити перевагу перед іншими рішеннями стосовно побудови СВВ для ЦПС на базі стандарту МЕК 61850 за рахунок більш суттєвого застосування специфічних властивостей даних об'єктів.

1. Sanger D.E. Cyberattack Forces a Shutdown of a Top U.S. Pipeline / D.E. Sanger, C. Krauss, N. Perlroth // The New York Times (May 8, 2021) URL: https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html.
2. Communication Networks and Systems in Substations. IEC Std. 61850.
3. Quincozes S.E., Albuquerque C., Passos D., Mossé D. A survey on intrusion detection and prevention systems in digital substations // Computer Networks. – 2021. – Vol. 184. – Article 107683.
4. P.I. Radoglou-Grammatikis, P.G. Sarigiannidis Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems, IEEE Access 7 (2019) 46595–46620.
5. Yang Y., Xu H.-Q., Gao L., Yuan Y.-B., Sezer S. Multidimensional intrusion detection system for IEC 61850-based SCADA networks // IEEE Trans. Power Deliv, 2017. – Vol. 32, № 2. – P. 1068-1078.

А.М. Давиденко, С.Я. Гільгурт

ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ІНФОРМАЦІЇ В КІБЕРФІЗИЧНИХ СИСТЕМАХ З ВИКОРИСТАННЯМ ПЛІС

Програмовані логічні інтегральні схеми (ПЛІС) завдяки своїй безпрецедентній гнучкості дозволяють підвищувати резильєнтність промислових підприємств критичної інфраструктури [1]. Однією з проблем, які виникають в кіберфізичних системах на таких об'єктах, є забезпечення цілісності інформації в каналах обміну даними між їх компонентами [2].

Найбільш відомим рішенням щодо протидії завадам, які порушують цілісність даних під час передачі каналами зв'язку, є використання коригуючих кодів, що виправляють помилки [3]. При цьому ключовим моментом, що визначає ефективність підходу, є наявність породжувальної матриці, яка формує код з потрібними властивостями. Повний перебір всіх комбінацій рядків, що складають породжувальну матрицю, забирає неприйнятно багато часу. Зменшити часові витрати на пошук матриць дозволяє використання певних методів та технік прискорення обчислень [3]. Але крім власне пошуку породжувальної матриці (який здійснюється на високопродуктивних обчислювальних засобах) необхідно також організувати процес синтезу апаратної схеми обчислювача, що реалізує завадостійке кодування, кінцевим результатом якого є файли з конфігураційними послідовностями (bitstream) для завантаження в ПЛІС.

В дослідженні розглядається сервіс, який не тільки спрощує поводження з породжувальними матрицями лінійних блокових коригуючих кодів (для довільних значень як інформативних, так і надлишкових бітів), але також дозволяє автоматизувати процедуру формування bitstream-файлів.

Отримані в дослідженні результати здатні підвищити резильєнтність кіберфізичних систем на об’єктах критичної інфраструктури.

1. Гільгурт С.Я. НРС та реконфігуровні засоби підвищення резильєнтності кіберфізичних систем // Живучість та резильєнтність критичної інфраструктури – 2023: Матеріали міжнародної науково-практичної конференції, м. Київ, 19 жовтня 2023. – К.: ІПМЕ ім. Г.Є. Пухова НАН України, 2023. – С. 11-14.
2. Євдокимов В.Ф., Давиденко А.М., Гільгурт С.Я. Сервіс централізованого синтезу апаратних засобів забезпечення цілісності інформації в кіберфізичних системах // Безпека енергетики в епоху цифрової трансформації: Матеріали наук.-практ. конф. Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, м. Київ, 22 грудня 2021. – К.: ІПМЕ ім. Г.Є. Пухова НАН України, 2021. – С. 51-53.
3. Давиденко А.М., Гільгурт С.Я., Потенко О.С., Кіслов О.Г. Поводження з породжувальними матрицями завадостійкого кодування інформації в кіберфізичних системах // XLI Щорічна науково-технічна конференція молодих вчених і спеціалістів: Тези доп., м. Київ, 17 травня 2023. – К.: Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, 2023. – С. 66-68.

С.Я. Гільгурт, О.Г. Кіслов

ВИКОРИСТАННЯ ФІЛЬТРІВ БЛУМА З ЛІЧИЛЬНИКАМИ ДЛЯ ПОБУДОВИ РЕКОНФІГУРОВНИХ ЗАСОБІВ КІБЕРЗАХИСТУ ІНФОРМАЦІЇ

Реконфігуровні пристрої на базі програмованих логічних інтегральних схем (ПЛІС) типу Field-Programmable Gate Array (FPGA) завдяки своїй безпрецедентній гнучкості є перспективною платформою для створення резильєнтних технічних систем. В галузі технічного захисту інформації при побудові мережевих систем виявлення вторгнень (МСВВ) сигнатурного типу програмована логіка успішно використовується для створення схем розпізнавання, суттєво прискорюючи виконання ресурсоємної задачі множинного розпізнавання патернів (multi-pattern matching) [1].

Одним з найбільш ефективних рішень для побудови апаратних схем множинного розпізнавання на ПЛІС є так званий фільтр Блума (ФБ), англомовна назва – Bloom Filter [2, 3]. В роботі [4] докладно розглянуто властивості даної схеми в сенсі застосування в системах МСВВ, а також особливості її реалізації на ПЛІС. Одним з недоліків класичної схеми ФБ є його нездатність вилучати патерни, які були додані в схему на етапі його програмування. Це позбавляє МСВВ, побудованих на базі ФБ, такого важливого функціонального показника, як здатність до динамічного переналаштування без переконфігурації ПЛІС (в роботі [5] докладно розглянуто показники ефективності реконфігуровних засобів кіберзахисту). Рішення проблеми полягає у використанні фільтрів Блума з лічильниками. Але додавання в схему великої кількості апаратно синтезованих лічильних схем збільшує загальні апаратні витрати. Для ефективного поводження з такими схемами потрібно мати інструмент для швидкої оцінки кількісних характеристик реконфігуровної схеми ФБ.

В роботі [6] запропоновано метод прискореної кількісної оцінки компонентів реконфігуровних сигнатурних систем кіберзахисту, який за допомогою так званих функцій оцінки (ФО) дозволяє знаходити в тому числі апаратні витрати для схем розпізнавання. В цьому ж дослідженні наведено вираз для ФО класичної схеми фільтра Блума.

Метою даної роботи є побудова ФО для ФБ з лічильниками. Для її досягнення докладно розглянуто особливості побудови ФБ на програмованій логіці, зокрема, проблему одночасного доступу множині геш-функцій до комірок бітового регістру, який у випадку реконфігуровної реалізації синтезується з використанням блокової пам'яті ПЛІС, на базі блоків BRAM. Запропоновано схему побудови реверсивних асинхронних лічильників – також з використанням запам'ятовуючих модулів BRAM. Використовуючи такий саме підхід, як в роботі [6], виконується підрахунок потрібних ресурсів та, як результат, знаходиться формула питомої функції оцінки:

$$R_{\text{SCBF}} = EG\left(\left\lceil\frac{8j}{x}\right\rceil + (\alpha+1)\left\lceil\frac{\left\lceil\frac{8j}{x}\right\rceil - 1}{x-1}\right\rceil - \alpha\right) + \alpha q(G+4) +$$

$$+ q\left(\left\lceil\frac{2(C-1)}{x}\right\rceil + 2\left\lceil\frac{G}{\left\lfloor\frac{x-1}{2}\right\rfloor}\right\rceil + 4C + \beta(1+C)\right) + \left\lceil\frac{q-1}{x-1}\right\rceil,$$

де $E = -\lfloor \log_2 \rho_{дозв.} \rfloor$, де $\rho_{дозв.}$ – дозволена вірогідність хибного розпізнавання;

G – розрядність геш-функцій;

j – довжина патернів, які розпізнає даний ФБ;

x – число входів логічних таблиць (LUT) використаної мікросхеми ПЛІС;

α – коефіцієнти нормалізації кількості тригерів відносно LUT;

$q = \lceil E / p \rceil$ – кількість часткових ФБ в складі повного ФБ, де p – число портів блокової пам'яті BRAM використаної мікросхеми ПЛІС;

C – кількість розрядів лічильників;

β – коефіцієнти нормалізації числа блоків BRAM відносно LUT.

Отримані в даному дослідженні результати дозволять розробникам цифрових пристроїв створювати більш ефективні реконфігуровні засоби інформаційної безпеки, в тому числі для підвищення резильєнтності об'єктів критичної інфраструктури за рахунок підвищення гнучкості та адаптивності.

1. С. Я. Гільгурт, “Метод прискореної кількісної оцінки компонентів реконфігуровних сигнатурних систем кіберзахисту”, Електронне моделювання, т. 44, № 5, с. 3-24, 2022. doi: 10.15407/emodel.44.05.003.
2. B. H. Bloom, “Space/Time Trade-offs in Hash Coding with Allowable Errors”, *Communications of the ACM*, Article vol. 13, no. 7, pp. 422-426, 1970, doi: 10.1145/362686.362692.
3. R. Patgiri, S. Nayak, and N. B. Muppalaneni, “Is Bloom Filter a Bad Choice for Security and Privacy? ”, *2021 International Conference on Information Networking (ICOIN)*, Jeju Island, Korea (South), pp. 648-653, 2021, doi: 10.1109/ICOIN50884.2021.9333950.
4. С. Гільгурт, “Побудова фільтрів Блума реконфігуровними засобами для вирішення задач інформаційної безпеки”, Безпека інформації, т. 25, № 1, с. 53-58, 2019, doi: 10.18372/2225-5036.25.13594.
5. С. Я. Гільгурт, “Порівняльний аналіз підходів до побудови компонентів реконфігуровних засобів технічного захисту інформації”, Проблеми інформатизації та управління, т. 2, № 66, с. 17-26, 2021, doi: 10.18372/2073-4751.66.15712.
6. S. Y. Hilgurt, A. M. Davydenko, T. V. Matovka, and M. P. Prygara, “Tools for Analyzing Signature-Based Hardware Solutions for Cyber Security Systems”, *JCSANDM*, vol. 12, no. 03, pp. 339–366, 2023, doi: 10.13052/jcsm2245-1439.123.5.

С.Я. Гільгурт

ПІДВИЩЕННЯ КІБЕРРЕЗИЛЬЄНТНОСТІ ЦИФРОВИХ ПІДСТАНЦІЙ ЗА МЕК 61850 З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Головним призначенням стандарту побудові електричних цифрових підстанцій (ЦПС) МЕК 61850 "Мережі та системи зв'язку на підстанціях" є створення єдиних специфікації, які дозволили б, з одного боку, захистити фінансові вкладення в енергетичні підприємства, з іншого – використовувати передові обчислювальні та мережеві технології, яки на відміну від енергетичного обладнання морально старіють набагато швидше [1]. На жаль, одночасно з вирішенням проблеми забезпечення сумісності обладнання різних рівнів ЦПС цифрові технології привносять в роботу систем автоматики ризики безпеки інформації. притаманні традиційній галузі їх застосування, а саме інформаційно-комунікаційним системам, чим суттєво зніжують рівень кіберрезильєнтності цифрових підстанцій [2].

В данному дослідженні проаналізовано найбільш перспективні підходи з використанням технологій штучного інтелекту, спрямованих на підвищення кіберрезильєнтності промислових інформаційних мереж підприємств та систем АСУ ТП, включаючи ЦПС [3-7]. При цьому основний акцент зроблено на такі засоби кібербезпеки, як мережеві системи виявлення та запобігання вторгнень [8].

Сигнатурний підхід виявляє атаки, порівнюючи заздалегідь зібрану інформацію з ознаками атаки, наприклад, шляхом відшукування конкретних патернів в мережевих пакетах. Але не виявляє принципово нові типи атак. Підхід на основі знань використовує знання про конкретні атаки, щоб ідентифікувати відповідні загрози. Реалізується на основі правил, логіки тощо. Базується на даних спостереження за набором попередньо визначених правил. Підхід на основі аномалій аналізує поточний стан системи на відхилення поведінки нормального стану, опис якого згенеровано заздалегідь, від такого, що виникає внаслідок вторгнення. Нормальний трафік використовується для навчання моделі ідентифікації штатного режиму. Профілі трафіку створюються за допомогою системних індикаторів, таких як завантаження процесора, помилки входу тощо з прив'язкою до часу доби та дня тижня. Повідомлення генерується коли поточні дані про трафік не відповідають заданим показникам. Підхід на основі статистики використовує логічні тести для перевірки відповідності даних певній статистичній моделі мережевого трафіку, яка характеризує стохастичну поведінку мережі. Підхід на основі контрольованого машинного навчання створює математичні моделі, які навчаються та вдосконалюються з часом, щоб виявляти вторгнення. Може використовувати нейронні мережі або статистичні моделі (класифікація, кластеризація). Використовує встановлену модель для перевірки шаблонів на основі даних, зібраних раніше в процесі

навчання. Зазвичай застосовує методи класифікації. Підхід на основі неконтрольованого машинного навчання на відміну від попередніх не потребує навчальних даних. Зазвичай використовують статистичні методи, такі як кластеризація.

Розглянуті вище підходи на базі методів штучного інтелекту найбільш прийнятні для застосування в електричних цифрових підстанціях, побудованих за стандартом МЕК 61850 з метою підвищення рівня їх кіберрезильєнтності. Деякі приклади реалізацій систем кіберзахисту для ЦПС можна знайти в роботах [9-11].

1. International Electrotechnical Commission. IEC 61850-1 ed. 2.0 Communication Networks and Systems for Power Utility Automation – Part 1. Introduction and Overview; IEC: Geneva, Switzerland, 2013.
2. Гільгурт С.Я. Підходи до побудови систем виявлення атак на протоколи цифрових електричних підстанцій / С.Я. Гільгурт // Кібербезпека енергетики: Матеріали наук.-практ. конф. Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, м. Київ, 28 травня 2021. – К.: ІПМЕ ім. Г.Є. Пухова НАН України, 2021. – С. 34-42.
3. J.E. Rubio, C. Alcaraz, R. Roman, J. Lopez, "Analysis of intrusion detection systems in industrial ecosystems," in SECRYPT, 2017, Conference Proceedings, pp. 116-128.
4. L. Tomlin, M.R. Farnam, S. Pan, "A clustering approach to industrial network intrusion detection," in Proceedings of the 2016 Information Security Research and Education (INSuRE) Conference (INSuRECon-16), 2016, Conference Proceedings.
5. L. Zhou, H. Guo, "Anomaly detection methods for IIOT networks," in 2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI). IEEE, 2018, Conference Proceedings, pp. 214-219.
6. A. Javaid, Q. Niyaz, W. Sun, M. Alam, "A deep learning approach for network intrusion detection system," in Proceedings of the 9th EAI International Conference on Bioinspired Information and Communications Technologies (formerly BIONETICS), 2016, Conference Proceedings, pp. 21-26.
7. W. Liang, K.C. Li, J. Long, X. Kui, A.Y. Zomaya An industrial network intrusion detection algorithm based on multifeature data clustering optimization model, IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 2063-2071, 2020.
8. Quincozes S.E., Albuquerque C., Passos D., Mossé D. A survey on intrusion detection and prevention systems in digital substations // Computer Networks. – 2021. – Vol. 184. – Article 107683.
9. Yang Y., Xu H.-Q., Gao L., Yuan Y.-B., Sezer S. Multidimensional intrusion detection system for IEC 61850-based SCADA networks // IEEE Trans. Power Deliv, 2017. – Vol. 32, № 2. – pp. 1068-1078.
10. Hariri M.E., Youssef T.A., Habib H.F., Mohammed O. Online false data detection and lost packet forecasting system using time series neural networks for IEC 61850 sampled measured values. IEEE conf. on Innovative Smart Grid Technologies (ISGT), IEEE: 2017. – pp. 1-5.
11. Rouget P., Badrignans B., Benoit P., Torres L. FPGA Implementation of Pattern Matching for Industrial Control Systems // 2018 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW), Vancouver, BC, Canada, 2018. – pp. 210-213.

Д.В. Федоренко

ВИЯВЛЕННЯ ДЕЗІНФОРМАЦІЇ ЯК МЕТОД ПІДВИЩЕННЯ РЕЗИЛЬЄНТНОСТІ СОЦІАЛЬНИХ СИСТЕМ

Соціальні системи в умовах цифровізації зазнають значного впливу дезінформації, що поширюється через соціальні мережі, медіа-платформи та інші канали комунікації. Це знижує здатність суспільства до ефективного реагування на виклики, породжує паніку, соціальну поляризацію та підриває довіру до інституцій. Своєчасне виявлення та протидія дезінформації є важливими компонентами забезпечення резильєнтності соціальних систем.

Сучасні інструменти для виявлення дезінформації:

Botometer – це веб-інструмент, що використовує методи машинного навчання для класифікації акаунтів у Twitter як ботів або людей. Система аналізує характеристики профілю, включаючи список друзів, структуру соціальної мережі, часову активність, мову та емоційний зміст повідомлень. Botometer надає загальний бот-складник (0–5), який оцінює ймовірність того, що акаунт є ботом, а також додаткові показники для більш детального аналізу.

ClaimBuster – це автоматизований онлайн-інструмент для перевірки фактів, розроблений в Університеті Техасу в Арлінгтоні. Він використовує методи обробки природної мови та контрольованого навчання на основі попередньо кодованих людських даних для ідентифікації правдивої або хибної інформації. ClaimBuster також доступний як застосунок для Slack, що полегшує інтеграцію в робочі процеси.

Bot Sentinel – це безкоштовна платформа, призначена для виявлення та моніторингу тролів, ботів і ненадійних акаунтів у Twitter. Інструмент використовує методи машинного навчання для класифікації акаунтів як надійних або ненадійних, а також для виявлення ботів. Усі такі акаунти заносяться до бази даних для щоденного моніторингу. Платформа також проводить ручний аналіз: оцінюються сотні твітів та ретвітів. Якщо акаунт має багато підписників і високий відсоток маніпулятивних або неправдивих повідомлень, він класифікується як ненадійний. Інструмент допомагає досліджувати вплив ботів на дискурс і пошук шляхів протидії поширенню дезінформації.

Вплив ШІ на резильєнтність соціальних систем:

- Зменшення впливу дезінформації: інструменти дозволяють оперативно виявляти маніпулятивні повідомлення.
- Підвищення критичного мислення: технології сприяють розумінню громадянами ризиків інформаційного впливу.
- Забезпечення стійкості до інформаційних атак: системи раннього попередження мінімізують наслідки.

Застосування ШІ для виявлення дезінформації є ключовим елементом підвищення резильєнтності соціальних систем. Впровадження сучасних інструментів, таких як Botometer, ClaimBuster та Bot Sentinel, дозволяє не лише ефективно ідентифікувати загрози, але й формувати стратегії для запобігання деструктивним інформаційним впливам. Однак їх інтеграція в систему управління інформаційною безпекою потребує вирішення етичних, правових та технічних питань.

1. Університет Індіани. (б. д.). *Botometer*. https://botometer.osome.iu.edu.
2. Університет Техасу в Арлінгтоні. (б. д.). *ClaimBuster*. https://idir.uta.edu/claimbuster/.
3. Bot Sentinel Inc. (б. д.). *Bot Sentinel*. https://botsentinel.com.

А.В. Бойченко, В.Р. Сенченко

ВРАХУВАННЯ ІНФОРМАЦІЙНИХ ВПЛИВІВ ПРИ АНАЛІЗІ КАСКАДНИХ ЕФЕКТІВ

Аналіз каскадних ефектів, спричинених впливами на функціонування об'єктів критичної інфраструктури, в умовах російської збройної агресії набуває все більшої актуальності. Традиційно при дослідженні каскадних ефектів у критичній інфраструктурі розглядаються наступні типи взаємозалежностей між об'єктами [1,2]:

– фізичні – характеризують зв'язки, пов'язані з передачею певних ресурсів (електроенергії, сировини, пального, тощо);

– комунікаційні – характеризують канали, пов'язані з інформаційним обміном;

– геопросторові – враховують відстань між елементами критичної інфраструктури та ймовірність того, що порушення роботи одного об'єкта може вплинути на інші, розташовані поблизу.

– управлінські – відображають зв'язки у прийнятті рішень на різних рівнях критичної інфраструктури.

Проте слід враховувати і інформаційні впливи, які відіграють вирішальну роль у формуванні суспільних настроїв та прийнятті рішень, і внаслідок цього впливають на резильєнтність критичної структури в цілому [3].

Для моделювання поширення каскадних ефектів у інформаційному просторі пропонується застосувати епідеміологічну модель. При цьому будемо вважати що розповсюдження інформації є подібним до процесу поширення епідемії[4, 5].

Розглянемо інформаційний простір як множину об'єктів, частина з яких отримала інформацію про пошкодження інфраструктури (заражені), тих, які потенційно можуть її отримати (сприйнятливі до зараження) та тих хто вже втратив інтерес до інформації (виробив імунітет). Патоген здатен поширюватися від заражених об'єктів до сприйнятливих об'єктів. У термінах класичної моделі [6] заражені позначаються I (infected), сприйнятливі – S (susceptible) а об'єкти з імунітетом – R (recovered).

Розглянемо наступні варіанти розповсюдження.

Найпростіший тип поширення (модель SI):

$$\begin{aligned} &\frac{di}{dt} = \lambda i(1-i), \\ &i(0) = i_0. \end{aligned} \qquad (1)$$

де i(t) – це частка інфікованих у момент часу.

Поширення з урахуванням повторного інфікування (модель SIS):

$$\begin{aligned} \frac{di}{dt} &= \lambda i(1-i) - \mu i, \\ i(0) &= i_0. \end{aligned} \tag{2}$$

де μ – це частка об'єктів, які «одужали».

Поширення з урахуванням здобуття імунітету (модель SIR):

$$\begin{aligned} \frac{ds}{dt} &= -\lambda si, \\ \frac{di}{dt} &= \lambda i(1-i) - \mu i, \\ \frac{dr}{dt} &= \mu i. \end{aligned} \tag{3}$$

де R – це частка об'єктів, які отримали «імунітет», який полягає у тому що об'єкт не може знову заразитися.

Поширення з урахуванням повторного зараження об'єктів з імунітетом (модель SIRS):

$$\begin{aligned} \frac{ds}{dt} &= -\lambda si + \alpha r, \\ \frac{di}{dt} &= \lambda i(1-i) - \mu i, \\ \frac{dr}{dt} &= \mu i - \alpha r. \end{aligned} \tag{4}$$

де α – ймовірність інфікуватися для об'єктів, які отримали «імунітет».

На рисунку представлено відображення вищенаведених типів розповсюдження інформаційних каскадних ефектів засобами графічної бази Neo4j моделюючого комплексу [7].

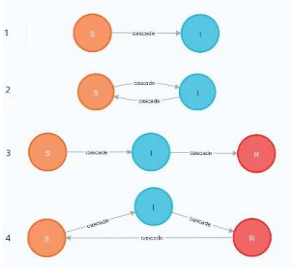


Рисунок 1 – Типи розповсюдження інформаційного каскадного ефекту

Включення інформаційних впливів в аналіз КЕ покращує розуміння того, як каскади поширюється мережами під час надзвичайних ситуацій. Вивчаючи цю динаміку, зацікавлені сторони можуть розробити більш ефективні стратегії пом'якшення негативних наслідків КЕ та підвищення резильєнтності критичних інфраструктур.

Використання даного підходу дозволить підвищити якість аналізу та прогнозування наслідків впливу на об'єкти критичної інфраструктури за рахунок врахування ширшого спектру ймовірних наслідків.

1. De Oliveira, A. K. B., Battemarco, B. P., Barbaro, G., Gomes, M. V. R., Cabral, F. M., de Oliveira Pereira Bez-erra, R., ... & Miguez, M. G. (2022). Evaluating the role of urban drainage flaws in triggering cascading effects on critical infrastructure, affecting urban resilience. Infrastructures, 7(11), 153.
2. Бойченко А.В., Сенченко В.Р. Дослідження взаємозв'язків об'єктів критичної інфраструктури. Міжнародна науково-практична конференція «Живучість та резильєнтність – 2023». Збірник матеріалів конференції. Київ. 2023. – с. 102-103.
3. Pescaroli, G., & Alexander, D. (2015). A definition of cascading disasters and cascading effects: Going beyond the "toppling dominos" metaphor. Planet@ risk, 3(1), 58-67.
4. Mizrahi, S. (2020). Cascading disasters, information cascades and continuous time models of domino effects. International journal of disaster risk reduction, 49, 101672.
5. Kabir, K. A., Kuga, K., & Tanimoto, J. (2019). Analysis of SIR epidemic model with information spreading of awareness. Chaos, Solitons & Fractals, 119, 118-125.
6. W.O. Kermack and A.G. McKendrick, A contribution to the mathematical theory of epidemics, Proc. R. Soc. Lond. Ser. A 115 (1927), pp. 700–721.
7. Бойченко, А. В., & Сенченко, В. Р. (2023). Підхід до моделювання геопросторових каскадних ефектів критичних інфраструктур. Інформаційні технології та безпека. 56(7). – с. 35-40.

О.С. Потенко

АНАЛІЗ ТА ФОРМАЛІЗАЦІЯ КРИТЕРІЇВ ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ НД ТЗІ 2.5-004-99

Інформаційні технології проникають у всі сфери діяльності, включаючи технологічні об'єкти. Безперебійне функціонування кібероб'єктів неможливе без вирішення питань безпеки, таких як створення захищених комп'ютерних систем і засобів захисту від несанкціонованого доступу, а також оцінка їх здатності обробляти критичну інформацію. Основою для визначення вимог захисту інформації є формальні критерії, зокрема: "Помаранчева книга" Міністерства оборони США, європейські критерії ITSEC, федеральні та канадські критерії безпеки інформаційних технологій, а також загальні критерії оцінки захищеності (Common Criteria) та НД ТЗІ 2.5-004-99.

Основне призначення критеріїв полягає в тому, щоб створити порівняльну шкалу для оцінки ефективності механізмів захисту інформації від несанкціонованого доступу, що реалізовані в комп'ютерних системах. Це дозволяє оцінювати рівень безпеки цих систем та гарантувати їх здатність захищати важливу інформацію від потенційних загроз. Крім того, критерії слугують орієнтирами для розробки нових комп'ютерних систем, в яких повинні бути реалізовані відповідні функції захисту інформації, що відповідають високим стандартам безпеки.

Хоча кожен критерій має свої специфічні області застосування в залежності від конкретних потреб і вимог, всі вони тісно пов'язані з кібербезпекою, оскільки спрямовані на забезпечення захищеності інформації в умовах сучасних технологій. Подібність предметної області цих критеріїв визначає їх схожу архітектуру, яка зазвичай включає набір вимог і стандартів, що повинні виконуватись для досягнення належного рівня безпеки (1).

$$МКБ = \{M_{КБ1}, M_{КБ2}, ..., M_{КБN}\} \quad (1)$$

яка включає кортежи (2)

$$M_{КБi} = \{ФПБ_1, ФПБ_2, ..., ФПБ_{Ki}\} \quad (2)$$

Розглянемо більш докладно НД ТЗІ 2.5-004-99 та визначимо вимоги критичні з точки зору сталого функціонування кібероб'єктів, що реалізують базові технології

Прикладом вітчизняних критеріїв є нормативний документ НД ТЗІ 2.5-004-99 [1], які визначають вимоги та стандарти для технічного захисту інформації в Україні та є основою для створення захищених систем, засобів захисту від несанкціонованого доступу та оцінки їх здатності обробляти критичну інформацію. Ці критерії надають порівняльну шкалу для оцінки надійності механізмів захисту і використовуються як основа для розробки захищених комп'ютерних систем. Вони можуть бути застосовані до

різноманітних типів систем, таких як однорідні системи, бази даних, вбудовані системи, мережі тощо.

Множина критеріїв безпеки визначається згідно з (3) як сукупність вимог або параметрів, що забезпечують необхідний рівень захисту інформаційних систем і даних від потенційних загроз та ризиків [1, 3].

$$МКБ(НДТЗІ) = \{K_{конф}, K_{ціл}, K_{дост}, K_{спост}, K_{гар}\} \quad (3)$$

де кортежі відповідних критеріїв мають вигляд (4-8)

$$K_{конф} = \{K_{КД}, K_{КА}, K_{КО}, K_{КК}, K_{КВ}\} \quad (4)$$

$$K_{ціл} = \{K_{ЦД}, K_{ЦА}, K_{ЦО}, K_{ЦВ}\} \quad (5)$$

$$K_{дост} = \{K_{ДР}, K_{ДС}, K_{ДЗ}, K_{ДВ}\} \quad (6)$$

$$K_{спост} = \{K_{НР}, K_{НК}, K_{НЦ}, K_{НТ}, K_{НА}, K_{НІ}, K_{НО}, K_{НВ}, K_{НП}\} \quad (7)$$

$$K_{гар} = \{Г1, Г2, Г3, Г4, Г5\} \quad (8)$$

В НД ТЗІ 2.5-004-99, окрім функціональних критеріїв, що оцінюють наявність послуг безпеки в комп'ютерній системі, наведені також критерії гарантій, які дозволяють оцінити правильність реалізації цих послуг. Вони охоплюють вимоги щодо архітектури засобів захисту, середовища розробки, етапів розробки, випробувань комплексу засобів захисту, середовища функціонування та експлуатаційної документації. Ці критерії визначають сім рівнів гарантій (Г-1, ..., Г-7), що мають ієрархічну структуру [2, 4].

1. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу.
2. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу.
3. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.
4. НД ТЗІ 2.7-010-09. Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.

А.В. Ковилін, С.Я. Гільгурт

АНАЛІЗ АНОМАЛІЙ КІБЕРБЕЗПЕКИ В ЕНЕРГЕТИЧНИХ СИСТЕМАХ З ВИКОРИСТАННЯМ ГРАФОВИХ МОДЕЛЕЙ

Енергетичні системи відносяться до ключових об'єктів критичної інфраструктури, від яких залежить надійне функціонування виробничих підприємств, транспорту, закладів охорони здоров'я та багатьох інших важливих для економіки та суспільства об'єктів. Сучасні енергосистеми відрізняються високою складністю, включаючи багато компонентів, таких як генератори, розподільчі станції, контролери, сенсори, комутатори та інтелектуальні пристрої, які функціонують у тісній взаємодії. Інтенсивний обмін інформацією між цими елементами в реальному часі забезпечує ефективність системи, але водночас створює кібербезпекові ризики.

Особливість енергетичного сектору полягає у його динамічній природі [1]. Зв'язки між вузлами змінюється, обсяги даних, що обробляються, швидко зростають, інтелектуальні технології, такі як інтернет речей (IoT), додають ще більше складності. Узагальнюючи, можна віднести до характерних рис енергетичних систем в сенсі динамічної поведінки наступні аспекти:

– часті зміни топології мережі у вигляді підключення нових пристроїв, змінення потоків енергії та даних;

– часові залежності: активність системи залежить від часових факторів, таких як добові піки споживання чи аварійні ситуації;

– гетерогенність інформаційних джерел (сенсори, пристрої IoT, контролери), розмаїття стандартів та форматів даних, а також швидкість їх оновлення.

Динамічний характер енергетичних систем ускладнює в тому числі застосування традиційних методів кіберзахисту. Типові загрози для них включають атаки на SCADA-системи, які порушують процес управління критично важливими об'єктами; DDoS-атаки на вузли управління, що можуть призвести до збоїв у передачі даних та прийнятті рішень; маніпуляції даними сенсорів, що можуть спровокувати неправильні дії в системі, включаючи аварійне відключення обладнання або розбалансування електроенергетичної мережі. Традиційні методи кіберзахисту, такі як сигнатурний аналіз або правила контролю трафіку на основі статичних моделей в подібних умовах стають недостатньо ефективними. Причинами є: нездатність враховувати зв'язки між вузлами, обмеженість у виявленні складних патернів поведінки, вимога реакції в реальному часі.

Ефективним інструментом для аналізу складних взаємодій в системі, здатним забезпечувати можливість виявлення аномалій та потенційних загроз виявляються графові моделі, використання яких дозволяє моделювати поведінку динамічних енергосистем у реальному часі, підвищуючи їхню

стійкість до сучасних кіберзагроз. Зокрема, графові моделі можуть стати універсальним засобом для виявлення прихованих залежностей і аномалій у складних енергетичних системах [3]. Вони дозволяють врахувати як статичні аспекти (топологію), так і динамічну поведінку (зміни зв'язків у часі), забезпечуючи більш глибокий аналіз і прогнозування. При цьому вузли графа представляють елементи системи, а ребра – взаємодії між ними, включаючи обмін даними, комунікації та потоки енергії. Подібний підхід дозволяє не тільки описати структуру системи, але й проаналізувати її поведінку в різних сценаріях, забезпечуючи глибше розуміння залежностей між компонентами. Як наслідок, використання графових моделей дозволяє підвищити стійкість енергосистем до сучасних кіберзагроз.

Особливу увагу в аналізі графів приділяють виявленню аномалій. Кластеризація вузлів дозволяє групувати компоненти системи за схожими характеристиками, що сприяє ідентифікації відхилень, таких як аномальні дані від сенсорів. Аналіз центральності вузлів допомагає визначити найважливіші елементи системи, які можуть стати потенційними цілями атак. Також значну роль відіграє аналіз поведінки зв'язків, який дозволяє виявляти незвичайні взаємодії, наприклад, несанкціоновані комунікації між сенсорами та підстанціями.

Забезпечуючи комплексний підхід до аналізу енергетичних систем, враховуючи як їхню структуру, так і динамічну поведінку, графові моделі дозволяють виявляти приховані залежності, оцінювати стійкість системи та оперативно реагувати на сучасні кіберзагрози, що є критично важливим для забезпечення безпеки й стабільності енергетичної інфраструктури. Графові нейронні мережі (Graph Neural Networks, GNN) є сучасним інструментом машинного навчання, розробленим для аналізу складних залежностей у графових структурах. Вони дозволяють моделювати взаємодії між вузлами та ребрами графа, враховуючи як топологічні, так і атрибутивні особливості системи. У контексті енергетичних систем GNN надають можливість аналізувати зв'язки між генераторами, сенсорами, вузлами керування та іншими компонентами, що критично важливо для виявлення прихованих аномалій або порушень у роботі системи.

Однією з ключових переваг GNN є здатність інтегрувати інформацію про сусідні вузли та ребра для кожного вузла у графі. Наприклад, в енергетичних системах це дозволяє враховувати залежності між сенсорами, контролерами та генераторами, виявляючи відхилення в поведінці. Якщо сенсор починає генерувати дані, які не відповідають очікуваній поведінці щодо взаємодії з іншими вузлами, GNN може сигналізувати про можливу аномалію.

Процес виявлення аномалій за допомогою GNN базується на порівнянні поточної структури графа та його атрибутів із очікуваною моделлю [4]. Наприклад, нормальна робота системи може бути описана як граф із певними характеристиками зв'язків і атрибутів вузлів. GNN навчається на

цій моделі, а потім порівнює поточний стан системи зі збереженим шаблоном. Будь-які значні відхилення, такі як поява нових зв’язків, зміна ваги ребер або аномальна поведінка вузлів, можуть бути автоматично ідентифіковані.

Для ефективного виявлення аномалій, GNN дозволяють проводити класифікацію вузлів, прогнозування властивостей ребер і навіть генерацію нових графів для моделювання можливих сценаріїв розвитку подій [5]. Це відкриває широкі можливості для аналізу енергетичних систем, включаючи прогнозування збоїв, оцінку впливу атак на ключові вузли та оптимізацію роботи системи. Таким чином, GNN стають невід'ємним інструментом для підвищення кібербезпеки й стійкості критичної інфраструктури, а їх аналіз є ключовим методом для виявлення аномалій у складних системах, таких як енергетичні мережі.

На рис. 1 наведено приклад виявлення одночасно кількох аномалій в системі:

1. Sensor_3 → Substation_1: Пряме з’єднання сенсора з підстанцією, що може свідчити про несанкціонований доступ.
2. Sensor_5 → Generator_2: Сенсор безпосередньо впливає на генератор, минаючи контролери.
3. Controller_2 → Control_Center: Несподіваний прямий зв'язок контролера з центром управління.
4. Generator_1 → Substation_2: Генератор взаємодіє з неправильною підстанцією.

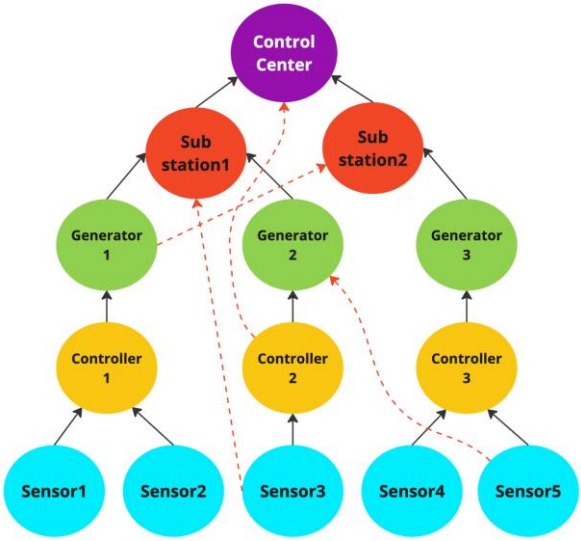


Рисунок 1 – Граф представлення енергетичної системи з виділеними аномаліями

Описані вище аномальні зв'язки порушують типову структуру системи. Це допомагає швидко ідентифікувати потенційні вразливості та проблеми в енергетичній мережі.

Висновок. Енергетичні системи є складними динамічними системами, що забезпечують життєдіяльність сучасного суспільства. Їхня складність та висока взаємопов'язаність створюють нові виклики в контексті кібербезпеки. Традиційні методи виявлення загроз часто не здатні ефективно реагувати на нові типи атак, особливо в умовах динамічного розвитку енергетичних систем. У таких випадках графові моделі та графові нейронні мережі стають потужним інструментом для аналізу складних взаємодій, виявлення аномалій та забезпечення стійкості системи. Використання графових моделей дозволяє не лише репрезентувати взаємозв'язки між компонентами системи, а й аналізувати поведінкові патерни вузлів у реальному часі. Це відкриває можливості для ефективного виявлення відхилень, кластеризації вузлів за схожими характеристиками, прогнозування загроз і швидкого реагування на потенційні атаки. Крім того, динамічні графи дозволяють враховувати часові залежності та адаптуватися до змін у структурі системи. Таким чином, впровадження графових підходів у кібербезпеку енергетичних систем дозволяє не лише підвищувати рівень захисту, але й створювати умови для проактивного управління ризиками. Це робить енергосистеми більш резильєнтними, забезпечуючи їх стабільну й безпечну роботу у найскладніших умовах.

1. Laimon, M., Mai, T., Goh, S., & Yusaf, T. (2019). Energy sector development: System dynamics analysis. *Applied Sciences*, 10(1):134. https://doi.org/10.3390/pp10010134.
2. Venayagamoorthy, G. K., Sharma, R. K., Gautam, P. K., & Ahmadi, A. (2016). Dynamic energy management system for a smart microgrid. *IEEE Transactions on Neural Networks and Learning Systems*, 27(8), 1643–1656. https://doi.org/10.1109/nnls.2016.2514358.
3. Ma, X., Wu, J., Xue, S., Yang, J., Zhou, C., Sheng, Q. Z., Xiong, H., & Akoglu, L. (2021). A comprehensive survey on graph anomaly detection with deep learning. *IEEE Transactions on Knowledge and Data Engineering*, 1. https://doi.org/10.1109/kde.2021.3118815.
4. Wang, H., Hooi, B., He, D., Liu, J., & Xiao, X. (2024). EGNN-AD: An Effective Graph Neural Network-Based Approach for Anomaly Detection on Edge-Attributed Graphs. In *Database Systems for Advanced Applications* pp. 321–331. https://doi.org/0.1007/978-981-97-5572-1_21.
5. Xiao, S., Wang, S., Dai, Y., & Guo, W. (2021). Graph neural networks in node classification: Survey and evaluation. *Machine Vision and Applications*, 33(1), art. number 4. https://doi.org/10.1007/s00138-021-01251-0.

О.С. Потенко А.М. Давиденко О.А. Суліма

АВТОМАТИЗАЦІЯ ЗАПИТІВ ДО БАЗ ДАНИХ ВРАЗЛИВОСТЕЙ ПРИ РОЗРОБЦІ СИСТЕМ МОНІТОРИНГУ ТА УПРАВЛІННЯ РИЗИКАМИ

Щороку кількість нових вразливостей в програмному та апаратному забезпеченні невпинно зростає, що ставить під загрозу безпеку інформаційних систем. Це створює додаткові труднощі для організацій, які змушені постійно адаптувати свої системи захисту до нових загроз. Для ефективної боротьби з такими викликами необхідно не тільки регулярно проводити моніторинг і виявляти нові вразливості, але й оперативно реагувати на зміни у загрозах. Важливими складовими цього процесу є своєчасне оновлення програмного забезпечення, використання сучасних технологій захисту, а також інтеграція спеціалізованих засобів для автоматичного виявлення і нейтралізації загроз. В іншому випадку, відсутність адекватного захисту може призвести до серйозних наслідків для цілісності та конфіденційності даних.

CVE (Common Vulnerabilities and Exposures) — це система, яка забезпечує стандартизований підхід до ідентифікації та реєстрації вразливостей у програмному та апаратному забезпеченні. CVE була створена для того, щоб об'єднати інформацію про вразливості в єдину, уніфіковану базу даних, що дозволяє фахівцям з безпеки та розробникам програмного забезпечення легше відслідковувати, обмінюватися і усувати ці вразливості. Кожній вразливості у CVE присвоюється унікальний ідентифікатор, який має формат "CVE-Рік-Номер", наприклад, CVE-2024-7658. Цей номер є ключем для швидкого пошуку та ідентифікації. В CVE надається базова інформація про вразливість, наприклад, її опис та потенційні наслідки, але без детальних технічних даних або рекомендацій щодо виправлення [1, 2].

NVD (National Vulnerability Database) — це розширена база даних, яка працює на основі ідентифікаторів CVE і надає додаткову інформацію про кожну зареєстровану вразливість. Вона розроблена Національним інститутом стандартів і технологій США (NIST) і дозволяє користувачам отримувати більш детальну інформацію, зокрема оцінки ризику уразливості. NVD надає такі додаткові дані, такі як оцінка вразливості за допомогою CVSS (Common Vulnerability Scoring System), що дає можливість визначити рівень серйозності проблеми. Також NVD містить інформацію про те, як вразливість може вплинути на різні аспекти системи, наприклад, конфіденційність, цілісність і доступність даних. Крім того, National Vulnerability Database надає рекомендації щодо протидії вразливості або послабленню її впливу, що робить її важливим інструментом для системних адміністраторів і спеціалістів з безпеки[1, 3].

Для автоматизації запитів до бази даних NVD можна використовувати NVD API

NVD API — це інтерфейс програмування додатків (Application Programming Interface, API), який надає доступ до бази даних Національної бази вразливостей (National Vulnerability Database, NVD). Що дозволяє користувачам отримувати інформацію про зареєстровані в базі даних вразливості за допомогою програмних запитів. NVD API надає дані у зручному форматі JSON, що дозволяє інтегрувати інформацію про вразливості в різні системи моніторингу, аналізу безпеки та управління ризиками. NVD API надає доступ до даних про вразливості, зареєстровані в базі даних NVD, включаючи інформацію про CVE (Common Vulnerabilities and Exposures), CVSS (Common Vulnerability Scoring System), а також оцінки впливу та інші метадані. Це може бути корисним для організацій або експертів яким потрібно автоматично відслідковувати, аналізувати і управляти вразливостями. NVD API дозволяє проводити пошук за унікальними ідентифікаторами CVE, пошук за датою. Можна фільтрувати вразливості за рівнем ризику, використовуючи оцінку CVSS. Є можливість шукати вразливості за категоріями, наприклад, за типами атак чи категоріями програмного забезпечення[4].

Прикладом запиту до NVD є *https://services.nvd.nist.gov/rest/json/cves/2.0?cpeName=cpe:2.3:o:microsoft:windows_10: 1809:*:*:*:*:*:*:**

CPE Name це унікальний ідентифікатор, який використовується для опису конкретного продукту чи платформи в системах, що допомагає визначити, на які версії продуктів або операційних систем вразливість може впливати вразливість[4].

Це надає можливість для інтеграції даних про вразливості в різні інформаційні системи. Наприклад, можна використовувати NVD API при розробці систем для моніторингу і сповіщення про нові вразливості, оцінки та аналізу ризиків на основі даних CVSS, автоматичного оновлення систем безпеки і їх захисту від нових загроз. А також є важливим інструментом для фахівців з безпеки, оскільки дозволяє інтегрувати дані про вразливості у власні системи моніторингу та управління ризиками.

1. Потенко О.С. Аналіз сучасних баз даних вразливостей інформаційної безпеки // XLI Науково-технічна конференція молодих вчених та спеціалістів інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. Збірник тез конференції (17 травня 2023 р). – Київ, 2023. – С. 34.
2. CVE Website https://www.cve.org/.
3. National Vulnerability Database Main page https://nvd.nist.gov/.
4. Vulnerability APIs https://nvd.nist.gov/developers/vulnerabilities.

О.М. Дибач

РЕЗИЛЬЄНТНІСТЬ АТОМНИХ ЕЛЕКТРОСТАНЦІЙ ДО ЗОВНІШНІХ ПРИРОДНІХ ЕКСТРЕМАЛЬНИХ ВПЛИВІВ У КОНТЕКСТІ ЗМІНИ КЛІМАТУ

Зміна клімату є одним із найбільших викликів, з якими стикається людство сьогодні. Досягнення кліматичних цілей, спрямованих на обмеження викидів парникових газів, вимагає декарбонізації енергетичного сектору. Одним із ключових елементів цього процесу є розширення використання низьковуглецевих джерел енергії, серед яких важливу роль відіграють атомні електростанції (АЕС).

Зважаючи на тривалий строк експлуатації АЕС, що може складати до 80 років (із урахуванням довготермінової експлуатації за результатами періодичної переоцінки безпеки), необхідно вивчити та врахувати можливий вплив зміни клімату на безпеку та експлуатацію АЕС.

Вплив зміни клімату на АЕС в цій роботі розглядається якісно в парадигмі поняття «резильєність», що набуває поширення в галузі атомної енергетики. Актуальність проблеми підтверджується тематикою конференції МАГАТЕ «Резильєність ядерних установок до зовнішніх подій з точки зору безпеки – фокус на зміні клімату» (2025) 1.

Природні екстремальні впливи та їх наслідки для АЕС

Відповідно до 2, кількість випадків природних екстремальних впливів, які спричинили розвантаження АЕС, збільшилась майже у 5 разів за останні 30 років, із значним прискоренням після 2009 року (рис.1). Попри частіші випадки виникнення, втрати у виробництві електроенергії на АЕС внаслідок природніх екстремальних впливів залишаються помірними - менше 50 ТВт·год з 1990 року (тобто менше 0,1% від обсягу електроенергії виробленої на АЕС за той самий період). Для порівняння недовироблення електроенергії на АЕС внаслідок втрати зовнішньої мережі є у тричі більшим.

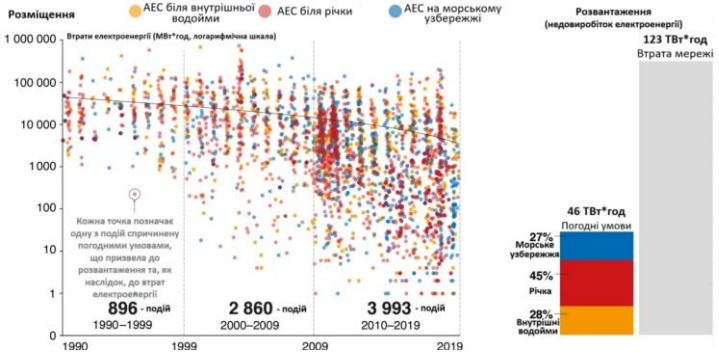


Рисунок 1 – Розвантаження АЕС (недовироблення електроенергії) внаслідок природних екстремальних впливів 2

Аналіз експлуатаційних подій на АЕС 3, свідчить що наступні впливи (та їх наслідки), імовірно можуть бути викликані зміною клімату:

– затоплення;

– пошкодження елементів систем (зокрема, цифрових) через високу температуру;

– лісові пожежі, що впливають на доступ до майданчика та експлуатацію АЕС;

– вплив піщаних бурь на майданчик та системи АЕС;

– вплив соляних аерозолів на фільтри;

– ускладнення доступу транспортних засобів на майданчик, в тому числі для реалізації протиаварійних заходів;

– втрата/недоступність кінцевого поглинача тепла;

– втрата зовнішньої електромережі.

Наслідки зміни клімату, важливі для безпеки та експлуатації АЕС

За результатами огляду міжнародних публікацій, зокрема 4, можна виділити наступні наслідки зміни клімату, що є важливими для безпеки та надійної експлуатації АЕС:

– збільшення частоти та інтенсивності екстремальних впливів (граничні значення екстремальних впливів можуть перевищувати консервативні значення враховані у проектних основах АЕС із урахуванням запасів безпеки);

– типи екстремальних впливів (окремі екстремальні впливи могли бути раніше відсіяні та відповідно невраховані в проекті АЕС з урахуванням регіону розміщення АЕС, наприклад, піщані бурі, посухи та ін.);

– нові джерела впливів (окремі джерела впливів могли бути раніше виключені з розгляду із урахуванням кліматичної зони розміщення АЕС, наприклад джерела затоплення);

– нові комбінації впливів (сильний дощ + землетрус + зсуви, повінь + замерзання та ін.)

– характеристики впливів, що раніше вважалися «нефізичними» (наприклад, швидкість і інтенсивність великого урагану).

Резильєність АЕС до зміни клімату

У матеріалах МАГАТЕ 1 резильєнтність визначено як «здатність готуватися та планувати, поглинати, відновлюватися та більш успішно адаптуватися до несприятливих подій». Що стосується безпеки АЕС, резильєнтність розглядається як міра здатності АЕС відновлюватися до безпечного стану після інциденту. Зазначається, що в проектних основах АЕС постулюються вихідні події на основі яких розробляються відповідні

проектні рішення із використанням консервативного підходу та із забезпеченням запасів безпеки.

Для визначення переліку цих вихідних подій застосовуються наявні статичні дані (історичні спостереження), аналітичні методи та узагальнені переліки із досвіду експлуатації. Як правило, історичні дані, що використовуються в цих оцінках, не враховують зміну клімату. Слід додатково зазначити, що для HILP-подій, тобто подій з низькою імовірністю та високим впливом, загалом відсутні історичні дані спостережень. Таким чином в термінах складових резильєнтності реагування на такі події зміщується на фази «поглинання» «відновлення» та «адаптація».

Довід експлуатації АЕС свідчить що конструкції, системи та елементи АЕС здатні витримати природні екстремальні впливи вищої інтенсивності ніж електричні мережі та інші об'єкти критичної інфраструктури. Враховуючи зворотній вплив енергосистеми на безпеку АЕС, у роботі 4 пропонується розглядати аспекти резильєнтності АЕС до змін клімату у складі енергосистеми (рис. 2).

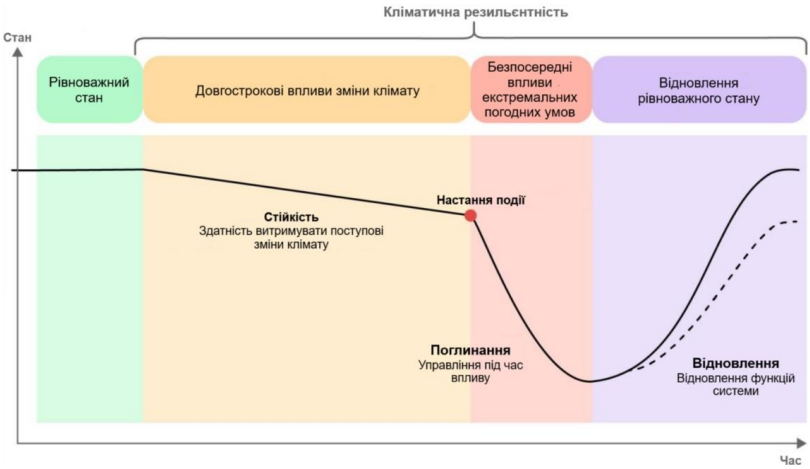


Рисунок 2 – Крива резильєнтності до змін клімату 4

З урахуванням проведеного аналізу, можна сформувати наступні складові для підвищення резильєнтності АЕС до зміни клімату:

1. Визначення природних екстремальних впливів, майбутніх тенденцій і екстремальних змін клімату на території розміщення АЕС.
2. Ідентифікація конструкцій, систем та елементів АЕС, що можуть зазнати впливу від зміни клімату.
3. Аналіз вразливості і ризику, що виникають через зміни клімату (внаслідок відмови конструкцій, систем та елементів АЕС).

4. Розробка плану адаптації до зміни клімату для підвищення резильєнтності АЕС.

Зазначені складові підвищення резильєнтності АЕС до зміни клімату потребують подальшого опрацювання та розробки теоретичних основ для їх реалізації.

1. IAEA, International Conference on Resilience of Nuclear Installations against External Events from a Safety Perspective – Focus on Climate Change, Announcement and Call for Papers. .https://www.iaea.org/sites/default/files/24/11/cn-337_announcement_and_call_for_papers.pdf.
2. IAEA, Climate Change and Nuclear Power 2022. Securing Clean Energy for Climate Resilience, https://www.iaea.org/sites/default/files/iaea-ccnp2022-body-web.pdf
3. P. Contri, Climate change impact on the safety of nuclear installations. USNRC RIC 2022, TH21 -Are We Observing More Extreme Weather Events that Affect the Risk of Nuclear Power Plants? March 8-10, 2022.
4. Investigating Natural Disaster-Related External Events at Nuclear Power Plants: Towards Climate Change Resilience, International Journal of Energy Research, Volume 2024, Article ID 3921093, https://doi.org/10.1155/2024/3921093.
5. C.Hart, IEA, Climate Resilience, J.Lim, 2021, https://iea.blob.core.windows.net/assets/e6962b75-103d-4567-b11a-94eac0c01daf/ClimateResilience_JinsunLIMandCraigHart.pdf.

В.В. Мохор, О.В. Цуркан, Р.П. Герасимов,
В.П. Яшенков, І.М. Демченко, О.О. Михайлова

КУБ РЕЗИЛЬЄНТНОСТІ ПРАЦІВНИКІВ ОРГАНІЗАЦІЙ ДО АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Здатність організацій реагувати на мінливі як внутрішні, так і зовнішні обставини визначається її резильєнтністю [1]. Насамперед це важливо в умовах існування негативної тенденції до збільшення кількості кібератак. Серед них до того ж уже понад десять років однією з актуальних залишається соціальна інженерія [2, 3]. Основним об'єктом такого різновиду кібератак є працівники організації. Оскільки здебільшого людина є найбільш уразливою у процесі забезпечення інформаційної безпеки та кібербезпеки зокрема [3, 4]. Тож встановлення основних напрямів протидії таким проявам і, як наслідок, формування кубу резильєнтності працівників організацій до атак соціальної інженерії є актуальним завданням.

З урахуванням [5, 6], куб резильєнтності формується з огляду на роль працівника в організації, уразливості працівника з визначеною роллю та методи протидії реалізуванню загроз через його уразливості (рис. 1). Основою такого представлення є направленість заходів на підвищення обізнаності щодо атак соціальної інженерії. Це насамперед узгоджується з діяльністю у межах розробляння і впроваджування систем управління інформаційною безпекою [7]. Так, підрозділом 6.3 «Обізнаність з інформаційною безпекою. Освіта та навчання» обумовлюється необхідність володіння працівниками відповідною інформацією з огляду на визначені для них в організації ролі. Наприклад [6, 7]:

- керівник;
- заступник керівника;
- начальних відділу;
- бухгалтер;
- адміністратор.

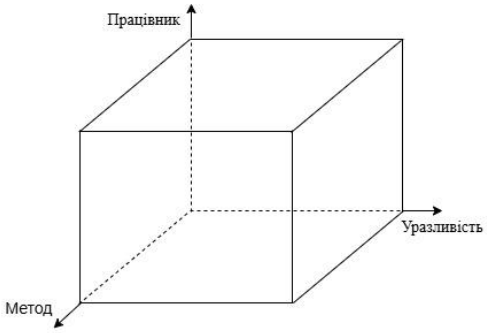


Рисунок 1 – Приклад представлення кубу резильєнтності працівників організації до атак соціальної інженерії [5, 6]

Незалежно від ролі працівників в організації атаки соціальної інженерії направлені на їхню свідомість [6]. Цим визначаються вибір форми маніпулювання (наприклад, обман, афера, інтрига, містифікація) і, як наслідок, методу протидії її використанню. При цьому обирання кожного з них може залежати від ролі працівника: або керівник, або бухгалтер, або адміністратор. Тому вибір методу протидії направлений на забезпечення їхньої резильєнтності до атак соціальної інженерії (рис. 1). Результативність таких дій обумовлюється досвідом і готовністю до отримання нових знань працівників організації. До того ж залежить від шаблонності поведінки залежно від типовості/нетиповості умов виконання поставлених завдань. У даному випадку доцільно також враховувати прояв емоцій працівників організації (наприклад, страх повідомити про перехід з цікавості за підозрілим посиланням з листа електронної пошти). І, що не менш важливо, впливання, зокрема, моделей поведінки.

Отже, направленість протидії атакам соціальної інженерії визначається насамперед з огляду на підвищення обізнаності працівників організації. Це узгоджується з реалізуванням заходів у межах розробляння і впроваджування систем управління інформаційною безпекою. З огляду на це куб резильєнтності формується за трьома напрямами: уразливість працівника з визначеною роллю в організації – метод протидії реалізуванню загрози соціальної інженерії через уразливість – працівник з визначеною роллю в організації. На його представлення впливають внутрішні та зовнішні психічні фактори.

1. Мохор, В.В., Бакалинський, О.О., Дорогий, Я.Ю., Цуркан, В.В. (2024). Парадигма нових ризиків кібербезпеки. *Кібербезпека енергетики* (с. 116, 117). ІПМЕ ім. Г.Є. Пухова НАН України.
2. International Organization for Standardization. (2012). *Information technology. Security techniques. Guidelines for cybersecurity* (ISO/IEC Standard No. 27032: 2012). https://www.iso.org/standard/44375.html.
3. International Organization for Standardization. (2023). *Cybersecurity. Guidelines for Internet security* (ISO/IEC Standard No. 27032:2023). https://www.iso.org/standard/ 76070.html.
4. Almutairi, B., Alghamdi, A. (2022). The Role of Social Engineering in Cybersecurity and Its Impact. *Journal of Information Security*. 13, 363-379. https://doi.org/ 10.4236/jis.2022.134020.
5. Feng, Q., Liu, M., Dui, H., Cai, B., Fan, D., Ren, Y., Wang, Z. (2024). A general design-oriented resilience measurement and evaluation method for engineering systems: Resilience cube. *Reliability Engineering & System Safety*, 245, 110038. https://doi.org/10.1016/j.ress.2024.110038.
6. Mokhor, V.V., Tsurkan, O.V., Herasymov, R.P., Tsurkan, V.V. (2017). Information security assessment of computer systems by socio-engineering approach. *Information Technologies and Security* (p. 92–98). CEUR Workshop Proceedings. http://ceur-ws.org/Vol-2067/paper13.pdf.
7. International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection. Information security management systems. Requirements* (ISO/IEC Standard No. 27001:2022). https://www.iso.org/standard/27001.

Д.П. Сінько, Г.О. Кравцов

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ПАРТИЦІЮВАННЯ КІБЕРНЕТИЧНОЇ СКЛАДОВОЇ ДЛЯ ЗАБЕЗПЕЧЕННЯ РЕЗИЛЬЄНТНОСТІ ІНДУСТРІАЛЬНИХ КІБЕРФІЗИЧНИХ СИСТЕМ В ЕЛЕКТРОЕНЕРГЕТИЦІ

Кіберфізичні системи електроенергетичних інтелектуальних систем мають скадну фізичну та кібернетичну структуру. Скалдність структури пояснюється географічна розгалуженість фізичних компонентів (генерація, підстанції різних рівнів, споживання), що в свою чергу обумовлює розподілену у просторі структуру кібернетичної складової (далі - КС) [1].

Архітектура розподілених інформаційних систем на поточний момент розвивається у напрямку домінування мікросервісного підходу, який пропонує гнучкість в горизонтальному масштабуванні програмного додатку та значно вищий за інші підходи рівень керованості та надійності застосунку під час її технічного обслуговування (релізи, патчі тощо) [2]. У відповідності до принципів мікросервісної архітектури застосунок складається з сукупності самостійних домен-орієнтованих застосунків, які, як правило, розташовані на окремих фізичних або логічних (віртуальних) серверах і мають назву “ноди”, а сукупність нод утворює кластер. Розміри кластерів варіюються від кількох нод до декількох тисяч нод, які можуть знаходитися в одному або декількох дата-центрах, які, в свою чергу, можуть перебувати в одній або декількох географічних локаціях.

Припустимо, що кожен вузол у кластері є критично важливим для безперебійної та якісної роботи застосунку. Будь-яке порушення зв'язку між цими вузлами може призвести до зниження продуктивності кластеру, а в найгіршому випадку – до його повної зупинки. Такий стан, коли застосунок не спроможний обробляти бізнес-транзакції і не може самостійно відновити свою роботу, називається партиціюванням кластеру або проблемою split brain [3]. Ця проблема є однією з ключових для забезпечення стійкості розумних енергетичних мереж (SmartGrid) і досі не має повністю задовільного розв'язку.

Саме тому розробка математичної моделі, яка б дозволяла прогнозувати стани кластеру, близькі до партиціювання або повного відмови, є надзвичайно важливою як з наукової, так і з практичної точки зору. Це дозволить вживати проактивних заходів для запобігання критичним збоям в роботі системи.

Параметрами математичного моделювання є :

1. Кількість датацентрів, що забезпечують функціонування нод кластеру дорівнює D.

2. Кількість фізичних серверів, на яких розміщено ноди кластеру, дорівнює S.

3. Бінарна матриця розподілу (плейсменту) фізичних серверів по датацентрам P розміром $S \times D$, де $p_{i,j} = \{0,1\}$ означає, що i-го сервер розташовано в j-ому датацентрі. Вочевидь, $S = \sum_{i=1}^{S} \sum_{j=1}^{D} p_{i,j}$.

4. Кількість мікросервісів (домен-орієнтованих аплікацій) дорівнює M.

5. Конфігурація аплікації описується як $n_{i,j,k} \in \{0,1\}$ присутності (або відсутності) ноди i-го мікросервісу на j-ому фізичному сервері в k-ому датацентрі. Загальна кількість нод в кластері визначається як $T = \sum_{i=1}^{M} \sum_{j=1}^{S} \sum_{k=1}^{D} n_{i,j,k}$.

6. Бінарна матриця з'єднань мікросервісів C розміром $M \times M$. Матриця з'єднань визначає функціональну залежність мікросервісів, де $c_{i,i} = 1$ означає реплікацію.

7. Функція доступності може бути представлена як бінарна функція $A: \big((i,j,k),(l,m,n)\big) \rightarrow \{0,1\}$, що описує здатність i-го мікросервісу на j-ому фізичному сервері в k-ому датацентрі викликати функцію на l-го мікросервісі на m-ому фізичному сервері в n-ому датацентрі.

Наведені параметри надають можливість описати split brain problem [3] та «смерть кластера», яка визначається як сегментація пласкої матриці з'єднань мікросервісів C, де кожен з заявлених станів може бути ефективно валідований за допомогою обходу графу в ширину, представленого сукупністю ребер, що формально описуються як $n_{i,j,k} \cdot n_{l,m,n} \cdot A\big((i,j,k),(l,m,n)\big) \rightarrow \{0,1\}$.

Підсумаємо, що запропонована формалізація ребер графу кластеру дозволяє методами комбінаторного аналізу попередити критичні стани кібернетичної складової кіберфізичної системи.

1. Nikolas Flourentzou (2022) .Cyber-physical systems modelling and simulation / Nikolas Flourentzou, Stella Hadjistassou, and Irina Ciornei // RTU Press. - 239 p.
2. Mark Richards (2015). Software Architecture Patterns / O'Reilly Media, Inc. - 47 p.
3. Davidson, Susan; Garcia-Molina, Hector; Skeen, Dale (1985). "Consistency In A Partitioned Network: A Survey". ACM Computing Surveys. 17 (3): 341–370.

Д.Р. Федоренко

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ МОНІТОРИНГУ РЕЗИЛЬЄНТНОСТІ КРИТИЧНИХ СИСТЕМ

У сучасному світі критично важливі системи, такі як енергетичні мережі, транспортна інфраструктура та фінансові установи, стають дедалі більш вразливими до широкого спектра загроз, включно з кібератаками, технічними збоями та природними катаклізмами. Забезпечення їхньої резильєнтності, тобто здатності протистояти, адаптуватися до змін та оперативно відновлювати функціонування після негативних впливів, є ключовим завданням для національної безпеки й сталого розвитку суспільства.

Штучний інтелект (ШІ) займає центральне місце в підвищенні стійкості критичних систем завдяки своїм потужним можливостям у сферах автоматизованого моніторингу, аналізу великих даних та прогнозування потенційних загроз. Зокрема, технології машинного навчання й нейронні мережі дозволяють ідентифікувати аномалії у функціонуванні систем, виявляти підозрілу активність у мережах і оперативно реагувати на потенційні загрози. Такі підходи значно покращують ефективність управління ризиками та зменшують ймовірність критичних збоїв.

У системах кібербезпеки впровадження ШІ сприяє автоматизації процесів моніторингу, виявлення загроз та їхньої нейтралізації, знижуючи залежність від людського фактора. Це забезпечує можливість швидшої та точнішої реакції на нові типи атак, зокрема розподілені атаки типу DDoS чи спроби несанкціонованого доступу до мережі. Штучний інтелект здатен не лише виявляти загрози в режимі реального часу, але й адаптувати захисні механізми до змін у характері атак.

Однак поряд із численними перевагами використання ШІ у критичних системах супроводжується низкою викликів. Зокрема, постає необхідність гарантування надійності та безпеки самих систем ШІ, які можуть бути об'єктами атак. Додатково виникають етичні питання, пов'язані з прозорістю прийняття рішень алгоритмами ШІ та їхньою відповідністю суспільним інтересам. У зв’язку з цим актуальним є розроблення комплексних підходів, що враховують не лише технічні аспекти впровадження ШІ, але й потенційні ризики та правові рамки.

У цій роботі аналізуються основні напрями застосування ШІ для моніторингу резильєнтності критичних систем, розглядаються сучасні технології та методи їхньої інтеграції, а також обговорюються перспективи подальшого розвитку та виклики, пов’язані з впровадженням цих рішень.

Поняття резильєнтності критичних систем можна визначити як їхню здатність зберігати функціональність, адаптуватися до нових умов і швидко відновлюватися після впливу природних, техногенних чи антропогенних загроз. Воно охоплює не лише здатність систем до опору негативним подіям, але й їхню спроможність до трансформації в умовах динамічних змін середовища [1].

Критично важливі системи, серед яких енергетичні мережі, транспортна інфраструктура та інформаційні технології, постійно перебувають під загрозою з боку природних (землетруси, повені), техногенних (аварії, технічні збої) та антропогенних (кібератаки, терористичні акти) чинників. Наслідки таких загроз можуть призвести до значних порушень у їхньому функціонуванні, створюючи серйозні ризики для безпеки та стабільності суспільства. Таким чином, підвищення стійкості цих систем є фундаментальним завданням у забезпеченні національної безпеки та сталого розвитку.

Моніторинг виступає ключовою складовою забезпечення резильєнтності критичних систем. Регулярний збір, обробка та аналіз даних про стан таких систем дозволяють своєчасно виявляти потенційні загрози, оцінювати їхній вплив та формувати дієві стратегії протидії. Це не лише сприяє запобіганню кризовим ситуаціям, але й зменшує наслідки вже виниклих подій, підтримуючи безперервність функціонування інфраструктури.

Інтеграція технологій штучного інтелекту (ШІ) — таких як машинне навчання, нейронні мережі та експертні системи — суттєво посилює ефективність процесів моніторингу. Обробляючи великі обсяги даних, ці інструменти дозволяють ідентифікувати приховані закономірності та аномалії, що дає змогу своєчасно реагувати на загрози. Наприклад, у сфері кібербезпеки алгоритми ШІ ефективно виявляють нетипову поведінку в мережах, що часто сигналізує про підготовку кібератаки [2].

Методи аналізу даних, які застосовуються в контексті машинного навчання, відіграють важливу роль у розумінні структурних та функціональних аспектів критичних систем. Так, аналіз кліматичних даних дозволяє моделювати сценарії можливих природних катастроф, а моделі на основі нейронних мереж здатні виявляти потенційні точки відмови у складних транспортних мережах. Нейронні мережі забезпечують імітацію багатофакторних взаємодій у системах, дозволяючи адаптувати їхню роботу до змінних умов [3].

Експертні системи доповнюють традиційні підходи, автоматизуючи процес прийняття рішень. Наприклад, у енергетичних мережах вони дозволяють запобігати перевантаженням або технічним збоям, використовуючи інтегровані бази знань для діагностики проблем на ранніх етапах. Завдяки оперативному аналізу даних та прийняттю оптимальних рішень в реальному часі, експертні системи мінімізують час реакції на критичні інциденти, забезпечуючи високу надійність роботи систем [4].

У сфері енергетики впровадження штучного інтелекту (ШІ) відкриває нові можливості для оптимізації управління енергетичними потоками та підвищення безпеки інфраструктури. Одним із прикладів є використання інтелектуальних лічильників другого покоління з функцією in-home display, які дозволяють споживачам відстежувати енергоспоживання в реальному часі. Ці технології не лише інформують про можливості зменшення витрат

на електроенергію, але й сприяють оптимізації енергетичних систем шляхом збалансування попиту і пропозиції [5]. Таке інтегрування ШІ в енергетику підвищує ефективність систем, зменшує витрати енергії та посилює стійкість до зовнішніх викликів.

У транспортному секторі технології ШІ активно використовуються для забезпечення безпеки дорожнього руху та оптимізації перевезень. Інноваційні системи, такі як технології запобігання зіткненням і допомоги водієві, зменшують ризик аварій, заздалегідь попереджаючи про небезпеки або здійснюючи коригувальні дії. Значний інтерес викликають автономні транспортні засоби, які, використовуючи алгоритми машинного навчання, забезпечують навігацію та управління транспортними засобами без участі людини. Безпілотні автомобілі та вантажівки, інтегровані в транспортні системи, мають потенціал для кардинальних змін у сфері міської мобільності та логістики [6].

ШІ також знаходить своє застосування в інших критичних секторах. У будівельній галузі інтелектуальні системи на основі ШІ допомагають виявляти небезпечні ситуації на будівельних майданчиках, що дозволяє зменшувати ризики травматизму. У логістиці штучний інтелект активно використовується для прогнозування попиту на перевезення, оптимізації маршрутів і зменшення транспортних заторів, що сприяє підвищенню ефективності транспортних потоків і зниженню витрат [7].

Застосування ШІ для моніторингу резильєнтності критичних систем демонструє значний потенціал у підвищенні здатності цих систем до адаптації, протистояння зовнішнім загрозам і швидкого відновлення після інцидентів. Зокрема, інтелектуальні системи моніторингу технічного стану об’єктів транспортної інфраструктури дозволяють виявляти дефекти на ранніх етапах і планувати заходи з їх усунення. Це значно знижує ризики аварійності та забезпечує довготривалу функціональність об’єктів.

Подальший розвиток цієї сфери охоплює кілька ключових напрямів. Вдосконалення алгоритмів машинного навчання має на меті підвищення точності виявлення аномалій, прогнозування можливих сценаріїв розвитку кризових ситуацій і забезпечення адаптивного реагування систем. Інтеграція ШІ з такими технологіями, як Інтернет речей (IoT) та обробка великих даних, сприятиме створенню комплексних систем моніторингу в реальному часі, здатних враховувати багатофакторні впливи.

Однак важливими залишаються питання правового й етичного регулювання використання ШІ в критичних системах. Необхідно розробити нормативну базу, яка забезпечить прозорість, відповідальність і безпечність таких технологій. Водночас актуальною є підготовка кваліфікованих фахівців, здатних ефективно впроваджувати та обслуговувати інноваційні рішення. Комплексний підхід до інтеграції ШІ в критичні сектори сприятиме підвищенню їхньої стійкості до сучасних викликів, забезпечуючи безпеку та стабільність функціонування в умовах динамічних змін.

1. Філатов В.В., Попко О.В. Резильєнтність критичної інфраструктури України на ринку електротехнічного обладнання // Резильєнтність критичної інфраструктури – 2023 : зб. матеріалів наук.-практ. конф., м. Київ, 21 червня 2023 р. / ІПМЕ ім. Г.Є. Пухова НАН України. Київ, 2023. 104 с. URL: https://ipme.kiev.ua/wp-content/uploads/2023/06/Mat-Critical-Infrastructure-Resilience-%E2%80%93-2023.pdf.
2. МакФарланд А. Машинне навчання та штучний інтелект: ключові відмінності. Unite.ai, 9 грудня 2022. URL: https://www.unite.ai/uk/machine-learning-vs-artificial-intelligence-key-differences/.
3. Шаркаді М.М., Роботишин М.В., Маляр М.М. Моделі і методи машинного навчання для завдань передбачення // Науковий вісник Ужгородського університету. Серія «Математика і інформатика». 2020. № 1(36). С. 112–122. DOI: https://doi.org/10.24144/2616-7700.2020.1(36).112-122.
4. Фратавчан В.Г., Фратавчан Т.М., Лукашів Т.О., Літвінчук Ю.А. Методи та системи штучного інтелекту: навч. посібник. Чернівці: ЧНУ, 2023. 114 с. URL: https://archer.chnu.edu.ua/bitstream/handle/123456789/6778/%D1%88%D1%82%D1%83%D1%87%D0%BD%D0%B8%D0%B9-%D1%96%D0%BD%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D1%82.pdf.
5. Суходоля О.М. Штучний інтелект в енергетиці: аналіт. доп. Київ: НІСД, 2022. 72 с. URL: https://www.libr.dp.ua/student_notes_it_suhodolya.html.
6. ШІ в транспорті: революція в майбутньому мобільності. URL: https://julienflorkin.com/uk/%D0%B1%D1%96%D0%B7%D0%BD%D0%B5%D1%81/%D1%82%D1%80%D0%B0%D0%BD%D1%81%D0%BF%D0%BE%D1%80%D1%82/ai-%D0%B2-%D1%82%D1%80%D0%B0%D0%BD%D1%81%D0%BF%D0%BE%D1%80%D1%82%D1%96/.
7. Мироненко О. Використання штучного інтелекту в управлінні транспортними потоками та логістичними реакціями. URL: https://cargofy.ua/uk/blog/vikoristannya-shtuchnogo-intelektu-v-upravlinni-transportnimi-potokami-ta-logistichnimi-reakciyami.

О.А. Владимирський, С.А. Недосєка, В.М. Зварич, О.В. Артемчук,
І.А. Владимирський, І.П. Криворучко, М.А. Яременко

КОМПЛЕКСНА ТЕХНІЧНА ДІАГНОСТИКА ЯК ЗАСІБ ВИРІШЕННЯ ПРОБЛЕМ РЕЗИЛЬЄНТНОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Питання резильєнтності критичної інфраструктури, до якої слід віднести як потенційно небезпечні виробництва, об'єкти, що постійно несуть підвищене навантаження, можна вирішувати різними, принципово відмінними способами.

Перший, активний, стосується стадії проєктування. При цьому задаються такі параметри об'єкту, які б забезпечили чіткі кількісні показники резильєнтності навіть для найкритичніших умов. Другий, пасивний, якій розглядається у даній роботі, є таким, що відповідає на пошкодження навіть на початковій стадії їх розвитку, і дозволяє запобігти ситуаціям, коли реагування на шкідливі впливи стає вже запізнім.

Оптимальним засобом забезпечення безпечного функціонування інфраструктури, яка має потенційні ризики, є встановлення систем безперервного моніторингу, які б відслідковували виникнення потенційних ризиків ще на ранніх стадіях та сигналізували б про них. Ще краще, якщо такі системи мають засоби кількісної оцінки стану контрольованого об'єкту, отримані на основі аналізу комплексу вхідних параметрів.

Якщо ж об'єкт не забезпечений заздалегідь системою постійного моніторингу його стану, виникає необхідність розробки засобів оперативного отримання інформативних параметрів, на основі яких можна про цей стан судити.

Таким чином, річ іде про застосування засобів технічної діагностики, яка, як наука, розвивається в Україні вже кілька десятиліть і має суттєвий досвід як створення та експлуатації систем безперервного моніторингу, так і застосування засобів мобільних лабораторій, які, умовно кажучи, «з коліс» дозволяють швидке розгортання діагностичних приладів, проведення вимірювань за відносно короткий час і, приймати рішення щодо стану контрольованого об'єкту. У кращому випадку таке прийняття рішення приймається автоматизованими засобами контролю безпосередньо під час проведення вимірів. У інших випадках час прийняття рішення залежить від складності аналізу накопиченої інформації та відповідних розрахунків, якщо вони потрібні.

У разі, коли проводиться саме оперативне діагностування об'єктів інфраструктури, які не оснащені засобами безперервного моніторингу, слід рекомендувати комплексну діагностику, яка б включала використання декількох вимірювальних методів, кожний з яких має певні переваги і стає основним у прийнятті рішення щодо стану об'єкту контролю в залежності

від умов. Ці умови визначаються як конструктивними особливостями об'єкту, так і рядом чинників, які можна визначити лише на стадії проведення контролю.

Наведемо приклад розробки системи такого діагностування на базі створюваного в Україні акустичного комплексу, який має на меті оперативний контроль і визначення небезпеки однієї з найбільш проблемних інфраструктур в Україні, а саме мереж тепло- та водопостачання. Необхідність підходів до оперативного контролю і швидкої оцінки стану даної інфраструктури визначається як її суттєвим зносом внаслідок складних умов роботи та відпрацювання заданого ресурсу, так і мілітарними впливами.

Обстріли критичної інфраструктури, обмеженість оперативного персоналу, різке зменшення об'ємів перекладання найбільш пошкоджених ділянок трубопроводів, інші чинники вимагають від приладового діагностичного обладнання, що застосовується зараз, підвищеної ефективності стосовно визначення місць витоків та критичних пошкоджень трубопроводів. У рамках проекту 2023.04/0022 «Розроблення апаратно-програмного комплексу та методики оперативного виявлення пошкоджень систем тепло- та водопостачання з врахуванням їх зношеності та мілітарних впливів», ІПМЕ ім. Г.Є .Пухова НАН України запропоновано суттєві вдосконалення існуючих, найбільш ефективних на сьогодні, акустичних методів та приладів діагностування трубопроводів. Ці вдосконалення стосуються підвищення оперативності визначення витоків в умовах малого відношення сигнал-завада, подолання потужних акустичних завад, врахування спотворень сигналів від пошкоджень при їхньому поширенні, визначення параметрів цього поширення і т.і. Для практичного відпрацювання запропонованих нововведень створюється відповідний випробувальний апаратно-програмний комплекс. Загальний склад апаратно-програмного комплексу (АПК) ілюструється рис.1.

Рисунок 1 – Структура АПК виявлення пошкоджень трубопроводів

Акустико емісійні системи ЕМА кількох поколінь протягом багатьох років використовують у ІЕЗ ім. Є.О. Патона НАН України. Виробництво та поставку приладів на замовлення і за технічним завданням ІЕЗ здійснюють похідні від добре відомого у світі колишнього угорського підприємства Videoton компанії Gereb as Tarsa та 2VD. Технологія оцінки стану матеріалу за даними АЕ, програмне забезпечення для реалізації цієї технології розроблено за участю д.т.н. С.А. Недосєки.

Низькочастотна система акустичного зондування трубопроводу та пошуку витоків РАСТР-2В є модернізованим варіантом системи акустичного моніторингу трубопроводів РАСТР-1 розробки ІПМЕ ім. Г.Є. Пухова НАН України [1]. Пасивний термо-акустичний течешукач А-10Т3 є комбінованим пристроєм, пристосованим для пошуку пошкоджених витоками ділянок трубопроводів та місць витоків за акустичною та тепловою ознаками пошкодження. Пристрій розроблено у ІПМЕ ім. Г.Є. Пухова НАН України [2] та використовується у підприємствах тепло- та водопостачання України.

Прилади ЕМА добре зарекомендували себе як у мобільних АЕ системах, так і у промислових комплексах постійного АЕ моніторингу.

В даному проекті пропонується використовувати 4-каналний прилад, як найбільш компактний. Його можливостей достатньо для виконання поставлених завдань.

Основне завдання випробувань – визначити поточну пошкодженість матеріалу, а далі за відомою номограмою (розробка д.т.н. С.А. Недосєки) перерахувати пошкодженість у залишковий ресурс. Таким чином, доступна кількісна оцінка пошкодженості і ресурсу матеріалів.

Загальна схема АЕ випробувань пропонується наступна.

1. На базі технічного завдання на контроль певного об’єкта та його креслень вибираються оптимальні схеми розташування датчиків АЕ.

2. Запропонована схема розташування датчиків АЕ аналізується спеціальним ПЗ на предмет похибок визначення координат.

3. Запропонована схема розташування датчиків АЕ тестується на об’єкті контролю. При наявності акустичного зв’язку між датчиками у локаційній схемі формується так звана антена для визначення координат джерел АЕ. При відсутності такого зв’язку вибирається схема зонної локації.

4. Випробування можна проводити трьома методами:

- При постійному навантаженні об’єкта контролю тиском або іншим чинником;

- При підйомі та скиді робочого тиску до рівня випробувального, відповідно до технічної документації на об’єкт;

- При відсутності акустичної активності у перших двох випадках виконується АЕ сканування, при якому один з датчиків АЕ виступає у ролі випромінювача, а інші – приймачів згенерованих сигналів. Пошкодженість матеріалу при цьому визначається за затуханням амплітуди сигналів та рядом додаткових параметрів (за потреби);

- При неможливості отримати дані попередніми способами пошкодженість об'єкта контролю може бути визначена шляхом використання методу LM – твердості. Метод заснований на визначенні коефіцієнта гомогенності при вимірюванні твердості у достатній (бажано близько 20) кількості точок, розташованих поблизу. Далі за відомими формулами розраховується пошкодженість матеріалу.

Надалі на основі автоматизованої оцінки руйнівного навантаження, отриманого при АЕ випробуваннях [3], або на основі визначення пошкодженості підраховується залишковий ресурс об'єкта контролю [4, 5].

Система РАСТР-2В містить генератор зондуючих сигналів трубопроводів, акустичні випромінювачі, три 3-х канальні реєстратори, мобільний комп'ютер. Генератор з випромінювачами використовуються для зондування трубопроводу з метою визначення параметрів хвильової структури домінуючих на ділянці трубопроводу акустичних сигналів. Ця інформація використовується для з'ясування групової швидкості сигналів від витоків, що є необхідним при обчисленні точних координат пошкоджень. Також генератор використовується для контролю заповнення ділянки трубопроводу водою та відсутності повітряних міхурів, які виникають при заповненні відключеної ділянки та приводять до похибок. Реєстратори акустичних сигналів трубопроводів призначені для реєстрації як сигналів витоків у пасивному режимі роботи системи, так і для реєстрації штучних зондувальних сигналів. Обробка зареєстрованих сигналів виконується на потужному мобільному комп'ютері. Застосування у АПК системи РАСТР-2В дозволяє реалізувати нові, складні алгоритми обробки акустичних даних про витоки та завади і відпрацювати роботу цих алгоритмів при оперативному пошуку витоків.

Термо-акустичний течешукач А-10Т3 пристосований для пошуку витоків саме на розгалужених підземних трубопроводах централізованого тепло- та водопостачання в умовах зносу запірної арматури та інших ускладнень. Це досягається, зокрема, завдяки можливості зручного порівняння рівнів вібрації трубопроводу у потрібному, великому динамічному діапазоні, що перевищує 60 дБ, у сукупності з достатньою чутливістю.

Вибір для створення АПК саме зазначених складових обумовлений:

- Перевіреною ефективністю окремого застосування складових АПК;

- Взаємним доповненням функціональних можливостей складових для досягнення мети проекту;

- Апаратно-програмною гнучкістю кожної складової, можливості їх подальшого розвитку при виконанні проекту для створення єдиної діагностичної системи з новими функціями.

Таким чином, запропонований комплекс являє приклад втілюваного у практику засобу вирішення проблем резильєнтності критичної інфраструктури.

Робота проводиться за проектом 2023.04/0022 «Розроблення апаратно-програмного комплексу та методики оперативного виявлення пошкоджень систем тепло- та водопостачання з врахуванням їх зношеності та мілітарних впливів», що виконується за рахунок грантової підтримки Національного фонду досліджень України (НФДУ). Автори висловлюють щиру подяку Фонду за підтримку виконання цієї витребуваної роботи.

1. Владимирский А. А., Владимирский И. А., Криворучко И. П., Савчук Н. П. Разработка модернизированной системы низкочастотного диагностирования состояния трубопроводов РАСТР-1М. *Моделювання та інформаційні технології* (збірник наукових праць ІПМЕ ім. Г. Є. Пухова НАН України). 2017. Вип. 78. С. 40-45.
2. Владимирский А.А., Владимирский ИА., Криворучко И.П. Термоакустический течеискатель А-10Т3. XXXVIII науково-технічна конференція молодих вчених та спеціалістів інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. Збірник тез конференції. Київ. 15 травня 2020р. – С 72.
3. Испытание сосудов давления международной группой специалистов / А. Я. Недосека, С. А. Недосека, М. А. Овсиенко [и др.] // Технічна. діагностика та неруйнівний контроль. – 2016. – № 3. – С. 3–10.
4. Недосека С.А., Недосека А.Я. Комплексная оценка поврежденности и остаточного ресурса металлов с эксплуатационной наработкой // Технічна. діагностика та неруйнівний контроль. – 2010. – № 1. – С. 9-16.
5. Stanislav Nedoseka (2024) Continuous monitoring of potentially dangerous equipment, "EMA" monitoring systems. Ecotechnology Day R&I networking event on Ecotechnology International Meetup, 23rd April 2024, online event. https://docs.google.com/document/d/1OqebdZq645dd84BVS4omPCjJ95suODMa/edit.

ЗМІСТ

МАТЕРІАЛИ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
«РЕЗИЛЬЄНТНІСТЬ ДИНАМІЧНИХ СИСТЕМ»

27 грудня 2024 року
м. Київ

Інститут проблем моделювання в енергетиці
ім. Г.Є. Пухова Національної академії наук України,
Україна, 03164, Київ, вул. Олега Мудрака
(колишня Генерала Наумова), 15,
тел.: +38 044 424 10 63
https://ipme.kiev.ua/, ipme@ipme.kiev.ua