

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



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

ПРИСВЯЧЕНА ДНЮ НАУКИ В УКРАЇНІ



Збірник матеріалів конференції
17 травня 2023 р.

Київ – 2023

УДК 621.3 + 004 + 519.6 : 620.9

Рекомендовано до друку Вченою радою
Інституту проблем моделювання в енергетиці
ім. Г.Є. Пухова НАН України
(протокол №3 від 20 квітня 2023 р.)

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

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

Відповідальний за випуск:
В.О. Артемчук

Collection of materials of the XLI Scientific and technical conference of young scientists and specialists of G.E. Pukhov Institute for Modelling in Energy Engineering of National Academy of Sciences of Ukraine, Kyiv, May 17, 2023 / PIMEE of NAS of Ukraine. - 2023. - 191 p.

Зб. матеріалів XLI Науково-технічної конференції молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, м. Київ, 17 травня 2023 р. / ПІМЕ ім. Г.Є. Пухова НАН України. – 2023. – 191 с.

© Автори публікацій, 2023

© Інститут проблем моделювання в енергетиці
ім. Г.Є. Пухова НАН України, 2023

ЗМІСТ

M. Chaikin

PROBLEMS AND PROSPECTS OF IMPLEMENTING ASSESSMENT OF THE LEVEL OF MATURITY OF CYBER SECURITY PROCESSES OF CRITICAL INFRASTRUCTURE OBJECTS OF THE ENERGY SECTOR OF UKRAINE IN ACCORDANCE WITH THE NIST CYBERSECURITY FRAMEWORK..... 8

D. Levkin

IMPROVEMENT OF THE CONTROLLING SYSTEM TO ENSURE ENERGY MANAGEMENT OF TECHNICAL SYSTEMS 12

I. Furtat, Yu. Furtat

METHODS FOR EXPERIMENTAL STUDIES OF HEAT AND MASS TRANSFER PROCESSES DURING DYEING OF TEXTILE MATERIALS 13

S. Grechko

VERIFYING MODELS WITH CO₂..... 14

O. Dzhyhun, A. Onyskova

DEVELOPMENT OF RENEWABLE ENERGY SOURCES IN UKRAINE..... 16

О.В. Лисак

АНАЛІЗ ЗМІН В КЛАСИФІКАЦІЇ ГЛИБОКИХ ГЕОТЕРМАЛЬНИХ СИСТЕМ ЧЕРЕЗ ПОЯВУ НОВИХ РІШЕНЬ В СФЕРІ БУРІННЯ..... 18

В.В. Шкарупило, І.В. Бінов, В.В. Душеба

ДОСЛІДЖЕННЯ МЕТОДУ ВЕРИФІКАЦІЇ TLC ПРИ ВИРІШЕННІ ЗАДАЧ ЕНЕРГЕТИКИ..... 21

Д.П. Сінько

ПАРАМЕТРИ МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ ПАРТИЦІОНУВАННЯ КІБЕРНЕТИЧНОЇ СКЛАДОВОЇ В ІНДУСТРІАЛЬНИХ КІБЕРФІЗИЧНИХ СИСТЕМАХ ЕЛЕКТРОЕНЕРГЕТИЧНИХ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ 23

С.М. Дяченко, І.В. Голомолзін

МОДЕЛЮВАННЯ ЗБІРНОГО УЛЬТРАЗВУКОВОГО СОНОТРОДУ З ВІБРУЮЧОЮ ЄМНІСТЮ 25

М.В. Антонішин, В.В. Цуркан

ФОРМУВАННЯ СЦЕНАРІВ ТЕСТУВАННЯ УРАЗЛИВОСТЕЙ МОБІЛЬНИХ ПРОГРАМНИХ ЗАСТОСУНКІВ МЕТОДОМ ТОПОЛОГІЧНОГО СОРТУВАННЯ..... 28

Г.П. Костенко, О.В. Згуровець

ПЕРСПЕКТИВИ УЧАСТІ СИСТЕМ НАКОПИЧЕННЯ ЕНЕРГІЇ В РИНКУ ДОПОМІЖНИХ ПОСЛУГ..... 29

О.І. Ключко

МОДЕЛІ ОПТИМІЗАЦІЇ ПОРТФЕЛЮ ТА МЕТОДИ МОДЕЛЮВАННЯ ЗАДАЧ КУПІВЛІ-ПРОДАЖУ ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ КОМПАНІЯМИ-ПОСТАЧАЛЬНИКАМИ 31

О.С. Потенко

АНАЛІЗ СУЧАСНИХ БАЗ ДАНИХ ВРАЗЛИВОСТЕЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ... 34

Д.О. Манюлюк

ІНТУЇЦІЯ ОБЧИСЛЮВАЛЬНИХ СИСТЕМ..... 35

Є.В. Болтов ПРОГНОЗУВАННЯ ТРАЄКТОРІЇ РУХОМИХ ОБ'ЄКТІВ У НЕДЕТЕРМІНОВАНОМУ СЕРЕДОВИЩІ В РЕАЛЬНОМУ ЧАСІ НА ВБУДОВАНИХ СИСТЕМАХ.....	37
В.В. Ткаченко, С.Ф. Гончар АКТУАЛЬНІСТЬ ОЦІНЮВАННЯ РИЗИКІВ КІБЕРБЕЗПЕКИ ПРИ КАСКАДНИХ АВАРІЯХ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ	41
В.В. Ткаченко, С.Ф. Гончар АНАЛІЗ РОЛІ ЛЮДСЬКОГО ЧИННИКА НА СТАН ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ АСУ ТП	42
А.В. Яцишин, В.О. Ковач, М.Л. Миронцов, М.М. Дівізіюк, Т.О. Шевченко ПЕРСПЕКТИВИ РОЗВИТКУ АТОМНОЇ ЕНЕРГЕТИКИ РІЗНИХ КРАЇН СВІТУ	43
О.О. Попов, С.І. Скуратівський, А.О. Запорожець, О.В. Фаррахов, Є.В. Пилипчук, В.О. Куценко, І.Д. Мартинюк, Є.Б. Краснов, О.М. Коваленко ПРО РОЗВ'ЯЗАННЯ ЗАДАЧІ ВИЗНАЧЕННЯ ЩІЛЬНОСТІ РОЗПОДІЛУ РАДІАЦІЙНОГО ЗАБРУДНЕННЯ ТЕРИТОРІЇ ЗА ДАНИМИ ДИСТАНЦІЙНОГО МОНІТОРИНГУ	47
О.О. Попов, С.В. Купріяничук, А.В. Яцишин, О.В. Фаррахов, Є.В. Пилипчук АНАЛІЗ ІСНУЮЧОГО ДОСВІДУ ПРИ ЗБЕРІГАННІ ВИСОКОАКТИВНИХ ВІДХОДІВ, ЩО МІСТЯТЬ ЯДЕРНІ МАТЕРІАЛИ.....	49
Є.В. Пилипчук, В.О. Ковач, В.О. Куценко, Є.Б. Краснов ПРО ПІДХІД ДО СТВОРЕННЯ GD-ВМІСНИХ НАНОКОМПОЗИТІВ НА ОСНОВІ КОНЦЕПЦІЇ «SAFE BY DESIGN» ДЛЯ ЗАХИСТУ ВІД НЕЙТРОННОГО ВИПРОМІНЮВАННЯ РІЗНИХ ДЖЕРЕЛ.....	55
О.О. Попов, В.О. Артемчук, Т.М. Яцишин, О.О. Вовк, С.П. Тараненко, А.М. Лагойко, А.П. Сулима ПРО ДЕЯКІ ПИТАННЯ ОЦІНКИ РИЗИКУ ХІМІЧНОЇ НЕБЕЗПЕКИ НАСЛІДКІВ АВАРІЙ ПРИ ПЕРЕВЕЗЕННІ НЕБЕЗПЕЧНИХ РЕЧОВИН НА АВТОМОБІЛЬНОМУ ТРАНСПОРТІ	59
С.Я. Гільгурт, О.Г. Кіслов, В.М. Попова АПАРАТНЕ ПРИСКОРЕННЯ ВИЯВЛЕННЯ АТАК НА ЦИФРОВІ ПІДСТАНЦІЇ	63
А.М. Давиденко, С.Я. Гільгурт, О.С. Потенко, О.Г.Кіслов ПОВОДЖЕННЯ З ПОРОДЖУВАЛЬНИМИ МАТРИЦЯМИ ЗАВАДОСТІЙКОГО КОДУВАННЯ ІНФОРМАЦІЇ В КІБЕРФІЗИЧНИХ СИСТЕМАХ.....	66
А.М. Примушко КОНКУРЕНТНЕ УКЛАДАННЯ ТА ВИКОНАННЯ УМОВ СМАРТ КОНТРАКТІВ ПРЕДСТАВЛЕНИХ У ВИГЛЯДІ ВИСОКОРІВНЕВИХ ФУНКЦІЙ ПЕРЕХОДУ МІЖ СТАНАМИ КОНТРАКТУ ЗА ДОПОМОГОЮ ДЕНОТАЦІЙНОЇ СЕМАНТИКИ.....	69
О.А. Кравчук РОЗПОДІЛЕНИЙ АНАЛІЗ ДАНИХ АВТОНОМНОГО РОЮ	73
Я.П. Лукашевич ДОСЛІДЖЕННЯ РОЗВИТКУ ОБ'ЄКТІВ АЛЬТЕРНАТИВНОЇ ЕНЕРГЕТИКИ В УКРАЇНІ З УРАХУВАННЯМ ЇХ ПРИЄДНАННЯ ДО МЕРЕЖ ПЕРЕДАЧІ ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ.....	76

В.В. Сичова, Г.С. Белоха

ЗАСТОСУВАННЯ АНСАМБЛІВ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ ДЛЯ ПРОГНОЗУВАННЯ НЕБАЛАНСІВ ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ В ОЕС УКРАЇНИ 82

М.О. Александров

ГРУПОВА СИНХРОНИЗАЦІЯ ДЕРЕВОПОДІБНИХ МАШИН ПАРНОСТІ 85

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

ЄВРОПЕЙСЬКІ ПІДХОДИ БІОКОНВЕРСІЇ ОРГАНІЧНИХ ВІДХОДІВ У ДИГЕСТАТ ТА БІОВОДЕНЬ ІЗ ЗАСТОСУВАННЯМ СУЧАСНИХ БІОТЕХНОЛОГІЙ . 88

Р.І. Драгунцов

ПІДХОДИ ДО МОДЕЛЮВАННЯ ЗАГРОЗ КІБЕРБЕЗПЕЦИ У ЗВ'ЯЗКУ З МАСОВИМИ ВІДКЛЮЧЕННЯМИ ЕЛЕКТРОПОСТАЧАННЯ ТА ПОТЕНЦІЙНІ ЗАХОДИ ПРОТИДІЇ 91

П.В. Шиманок

ЗАСТОСУВАННЯ МЕТОДІВ ПРОГНОЗУВАННЯ ДЛЯ ВИЗНАЧЕННЯ ОЧІКУВАНИХ ЗНАЧЕНЬ ВТРАТ В РОЗПОДІЛЬНИХ МЕРЕЖАХ 94

О.О. Бакалинський, Д.В. Пахольченко, Д.О. Нагорний

МЕТОДИКА ВИЗНАЧЕННЯ КАТЕГОРІЇ (РІВНЯ) КРИТИЧНОСТІ КІБЕРІНЦИДЕНТУ/КІБЕРАТАКИ 97

В.С. Подгуренко, О.М. Гетманець, В.Є. Терехов

ДОСЛІДЖЕННЯ МЕЖІ МАКСИМАЛЬНОЇ ЕФЕКТИВНОСТІ РОБОТИ ВІТРОЕЛЕКТРИЧНИХ УСТАНОВОК У ЗАДАНИХ ВІТРОКЛІМАТИЧНИХ УМОВАХ 101

А.О. Нікітенко

НАБОРИ ДАНИХ ДЛЯ СТВОРЕННЯ СИСТЕМ ВІЯВЛЕННЯ МЕРЕЖЕВИХ ВТОРГНЕНЬ З ВИКОРИСТАННЯМ НЕЙРОННИХ МЕРЕЖ 104

А.О. Лєпатєєв

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РОЗРОБКИ ТРЕНАЖЕРНИХ ЗАНЯТЬ ЗА РАХУНОК ЗАСТОСУВАННЯ ФУНКЦІОНАЛЬНО-ВАРТІСНОГО АНАЛІЗУ 107

В.В. Аскеров, О.С. Засорнов

ВИКОРИСТАННЯ БЛОКЧЕЙН ТЕХНОЛОГІЇ ДЛЯ КЕРУВАННЯ ДАНИМИ СОНЯЧНОЇ ЕЛЕКТРОСТАНЦІЇ ХМЕЛЬНИЦЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ 110

О.В. Александрова

СТВОРЕННЯ 3D-МОДЕЛІ ОБЛИЧЧЯ ЛЮДИНИ ЗА ДОПОМОГОЮ ПІДХОДУ НА ОСНОВІ НЕЙРОМЕРЕЖІ 113

О.А. Владимирський, В.О. Артемчук, В.А. Дюков

РОЗРОБКА СТРУКТУРИ СИСТЕМИ ВИМІРЮВАННЯ ГЕОМЕТРІЇ ВИГОРОДКИ РЕАКТОРІВ ВВЕР-1000 116

О.А. Владимирський, І.А. Владимирський, В.В. Папазов, Г.В. Анфімова

АВТОМАТИЗАЦІЯ ПРОЦЕСУ ВИЗНАЧЕННЯ КОЕФІЦІЄНТА КОРИСНОЇ ДІЇ ГАЗОВИХ КОТЛІВ 118

О.А. Владимирський, І.А. Владимирський РОЗРОБКА ГЕНЕРАТОРА ДЛЯ АКУСТИЧНОГО ЗОНДУВАННЯ ТРУБОПРОВІДІВ	120
О.А. Владимирський, І.А. Владимирський, А.П. Іващенко, І.П. Криворучко НИЗЬКОЧАСТОТНА ВІБРОКАЛІБРУВАЛЬНА УСТАНОВКА	122
В.А. Дюков ДОСВІД РОЗРОБКИ КОНСТРУКЦІЇ СИСТЕМИ КОНТРОЛЮ РОЗМІРІВ ВИГОРОДКИ ЯДЕРНОГО РЕАКТОРА.....	124
Д.М. Семенюк ВИЯВЛЕННЯ ПРИХОВАНИХ МІКРОВИТОКІВ В ТРУБОПРОВОДАХ ВНУТРІШНЬО БУДИНКОВИХ МЕРЕЖАХ ЗА ДОПОМОГОЮ УДОСКОНАЛЕНОГО ТЕРМОАКУСТИЧНОГО ТЕЧЕШУКАЧА А-10ТЗ.....	127
В.В. Станиціна, А.О. Підручна ДОЦІЛЬНІСТЬ ВИКОРИСТАННЯ ЗАКОНСЕРВОВАНИХ СВЕРДЛОВИН ДЛЯ ТЕПЛОПОСТАЧАННЯ	130
В.В. Станиціна, В.О. Артемчук ПРОБЛЕМА ДЕКАРБОНІЗАЦІЇ СИСТЕМ ТЕПЛОПОСТАЧАННЯ УКРАЇНИ З ВРАХУВАННЯМ ОСОБЛИВОСТЕЙ НАЦІОНАЛЬНОЇ ЕКОНОМІКИ.....	132
І.П. Криворучко ОСОБЛИВОСТІ ФОРМУВАННЯ СИГНАЛІВ УПРАВЛІННЯ КРОКОВОГО ДВИГУНА У МІКРОКРОКОВОМУ РЕЖИМІ.....	134
С.С. Саух КОНЦЕПЦІЯ ПОБУДОВИ ЖОРСТКО РЕЗИЛЬЄНТНОЇ ЕЛЕКТРОЕНЕРГЕТИЧНОЇ СИСТЕМИ УКРАЇНИ.....	137
А.В. Давидюк ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДАНИХ ДАТАЦЕНТРІВ В УМОВАХ ВОЄННОГО СТАНУ	139
М.С. Ярошинський ЗАХИСТ ВІД АТАК ПІДРОБКИ ТА ПЕРЕХОПЛЕННЯ ЗА ДОПОМОГОЮ JWT ДЛЯ НЕКОНФІДЕЦІЙНОЇ ІНФОРМАЦІЇ.....	141
Ф.О. Коробейніков АНАЛІЗ ВИЗНАЧЕНЬ ТЕРМІНА "РЕЗИЛЬЄНТНІСТЬ" ТА ЙОГО ІНТЕРПРЕТАЦІЙ У МІЖНАРОДНИХ СТАНДАРТАХ.....	145
Ю.О. Гарбуз РЕЗИЛЬЄНТНІСТЬ ЕНЕРГЕТИЧНОЇ СИСТЕМИ УКРАЇНИ: ОСНОВНІ ПРИНЦИПИ ТА ПОНЯТТЯ.....	150
С.В. Дубровський МОДЕЛІ ТА КОМП'ЮТЕРНІ ЗАСОБИ МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ ПРОЦЕСІВ ФУНКЦІОНУВАННЯ ВЕРСТАТІВ З ЧПК.....	152
А.В. Полухін ПОБУДОВА МАТЕМАТИЧНОЇ МОДЕЛІ ВИЗНАЧЕННЯ ПОГОДИННОГО СПОЖИВАННЯ СПОЖИВАЧІВ З РОЗБИВКОЮ ПО АДМІНІСТРАТИВНИМ ОБЛАСТЯМ УКРАЇНИ.....	154

Т.В. Пучко

ПРОБЛЕМА ПІДТРИМАННЯ СУМІСНОСТІ МІЖ НАДАВАЧАМИ ТА КЛІЄНТАМИ ВЕБІНТЕРФЕЙСІВ ПРИКЛАДНОГО ПРОГРАМУВАННЯ..... 158

І.В. Пучко

ПРОБЛЕМА ПАРТИЦІОНУВАННЯ КЛАСТЕРУ ТА АКТУАЛЬНІСТЬ ЇЇ ВИРІШЕННЯ НА ПРИКЛАДІ АККА-CLUSTER FRAMEWORK 161

Є.С. Чернозьомов

ТИПИ ТА ВЛАСТИВОСТІ СИСТЕМ ПЕРЕДАЧІ ПРОМЕНЕВОЇ ЕНЕРГІЇ 164

О.В. Сіроткін

ПАРАЛЕЛЬНЕ МОДЕЛЮВАННЯ З ВИКОРИСТАННЯМ РЕАКТИВНИХ ПОТОКІВ . 167

С.М. Осінов, І.В. Єрмоєнко

ПРО ВІДПОВІДНІСТЬ ПРОЦЕСІВ У БІОЛОГІЧНИХ ТКАНИНАХ ТА НИЗЬКОТЕМПЕРАТУРНІЙ НАПІВПРОВІДНИКОВІЙ ПЛАЗМІ 175

І.В. Блінов, Є.В. Парус, Є.О. Зайцев

СЦЕНАРІЇ ВИКОРИСТАННЯ МАЛИХ МОДУЛЬНИХ РЕАКТОРІВ З НАКОПИЧУВАЧАМИ ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ В ЗАГАЛЬНОМУ БАЛАНСІ ОЕС УКРАЇНИ 178

Є.О. Зайцев, І.В. Блінов

СКЛАДОВІ СИСТЕМИ МОНІТОРИНГУ АВАРІЙНИХ СТАНІВ КАБЕЛЬНИХ РОЗПОДІЛЬНИХ ЕЛЕКТРИЧНИХ МЕРЕЖ..... 181

Д.О. Олефір

ЩОДО ДОБОВОЇ ОПТИМІЗАЦІЇ РОЗПОДІЛУ ГІДРОРЕСУРСІВ ТА ВИРОБНИЧИХ ПОТУЖНОСТЕЙ ГЕС НА РИНКУ «НА ДОБУ НАПЕРЕД»..... 185

М.С. Кондратенко

ВИЗНАЧЕННЯ КІЛЬКОСТІ БЛОКІВ ПІДТВЕРДЖЕННЯ У БЛОКЧЕЙНІ, В ЯКОМУ РОЗМІЩЕНО РЕЄСТР ДРУГОГО РІВНЯ У ВИПАДКУ, КОЛИ В ОБОХ БЛОКЧЕЙНАХ ВИКОРИСТОВУЄТЬСЯ ПРОТОКОЛ КОНСЕНСУСУ POS..... 188

M. Chaikin

PROBLEMS AND PROSPECTS OF IMPLEMENTING ASSESSMENT OF THE LEVEL OF MATURITY OF CYBER SECURITY PROCESSES OF CRITICAL INFRASTRUCTURE OBJECTS OF THE ENERGY SECTOR OF UKRAINE IN ACCORDANCE WITH THE NIST CYBERSECURITY FRAMEWORK

The relevance of cybersecurity of energy sector facilities has been especially evident since the beginning of the open aggression of the Russian Federation against Ukraine starting from February 24, 2022.

From the beginning of the military aggression, the occupiers showed a special interest in the capture and destruction of energy facilities. On February 24, 2022 the Kakhovskaya hydroelectric power station was captured. On 25 February, Russian troops blew up a gas pipeline near Kharkiv, Ukraine's second-largest city. On 2 March, 2022, Russia claimed to have taken control of the area surrounding the 5.7GW nuclear power plant in Zaporizhzhia, Europe's largest. In addition, during the period of autumn 2022 - spring 2023, the occupiers repeatedly launched rocket-bomb strikes specifically at energy facilities. At the same time, according to the analysis of the specialists of the ESET corporation, which works in close contact with the State Service for Special Communications and Information Protection of Ukraine, energy facilities were one of the priority targets of cyberattacks by the aggressor state [1].

Such activity of the enemy caused the accelerated modernization of requirements for the protection of critical infrastructure, including in cyberspace. At the beginning of last year, the state of regulatory regulation of cyber security issues was not fully determined. It is worth noting that the requirements for cyber security for critical infrastructure objects are described in the following legal documents:

- Law of Ukraine On the Basic Principles of Cybersecurity in Ukraine [2];
- Law of Ukraine On information protection in information and communication systems [3];
- Resolution of the Cabinet of Ministers of Ukraine On Approval of General Requirements for Cyber Protection of Critical Infrastructure Objects [4];
- Law of Ukraine On Critical Infrastructure [5]

Law of Ukraine "About Critical Infrastructure" was entered into force on June 15, 2022 and finally defined a special body that will have to develop requirements for the protection of critical infrastructure and create a register of critical infrastructure objects – this body is State Service of Special Communications and Information Protection of Ukraine. Also, according to the text of the Law, a list of types of organizations is included, which, according to their type of activity, belong to critical infrastructure. Energy is included in this list. In addition, an

important innovation of this law is the introduction of a risk-based approach and the requirement for insurance of security risks.

In 2021, the Administration of the State Service for Special Communications and Information Protection of Ukraine published Order No. 601 dated October 6, 2021, containing "Methodical recommendations on increasing the level of cyber protection of critical information infrastructure"[6]. Changes to this order, which were approved by the orders of the State Special Communications Administration dated 12.10.2021 No. 616 and dated 10.07, were published later. 2022 No. 343. These recommendations are developed taking into account the Framework for Improving Critical Infrastructure Cybersecurity issued in 2014 and updated in 2018 by the National Institute of Standards and Technology of the United States of America (NIST Cybersecurity Framework - NIST CSF) [7].

As a next step, on March 24, 2023, the Cabinet of Ministers of Ukraine adopted the Resolution on "Some issues of conducting an independent audit of information security at critical infrastructure facilities", which introduced a mandatory cyber security audit of critical infrastructure facilities every 2 or 3 years (depending on the category criticality)[8].

Since the State Service for Special Communications and Information Protection of Ukraine is responsible for the cyber protection of critical infrastructure objects, it can be stated that at the moment there are 3 different ways to confirm compliance with cyber security requirements, according to the 601st Order:

- Construction of a comprehensive information protection system with confirmed compliance (KSZI);
- Building an information security management system (ISMS);
- Audit for compliance with NIST CSF requirements and re-audit following implementation of recommendations.

In addition, it should be noted that some Ukrainian energy companies fall under the scope of regulation of the European Union in matters of cyber security. For example, the Ukrenergo company, as an operator of the dispatching and trunk transmission system, is part of the European network of electricity transmission system operators, which unites 43 operators in 39 countries of the European continent - ENTSO-E (European Network of Transmission System Operators for Electricity), which has and develops its cybersecurity requirements - Network code on energy cybersecurity.

The recast of the Electricity Regulation (Regulation (EU) 2019/943)[9] gives the Commission a mandate to develop a network code for cybersecurity. The Smart Grids Task Force has been doing preparatory work since 2017, and released its second interim report in July 2018. The report recommends setting up an early warning system for the energy sector in Europe, cross-border and cross-organisation risk management, minimum security requirements for critical infrastructure components, a minimum protection level for energy system operators, a European energy cybersecurity maturity framework and supply chain risk management.

In January 2022, the European Network of Transmission System Operators for Electricity (ENTSO-E) announced the details of its new cybersecurity code. The Network Code on Cybersecurity(NCCS) is the first network code that will be developed according to the new rules established by the European Union on the internal market for electricity and is expected to enter into force by January 2024. The network code aims to set a European standard for the cybersecurity of cross-border electricity flows. It focuses on improving cybersecurity resilience through the enhancement of threat decision and incident reporting and proposes various measures to improve cybersecurity resilience that are essential to preserving the continuity of the services. On January 14, 2022, the preparation of the draft document was completed. [10]

At the same time, the State Service for Special Communications and Information Protection of Ukraine and the Cabinet of Ministers of Ukraine, with the active help of international partners, are working on updating Resolution No. 518 of the Cabinet of Ministers of Ukraine dated June 19, 2019 "On the approval of General requirements for cyber protection of critical infrastructure objects", which will lead to the acquisition of NIST CSF status is necessarily the standard for critical infrastructure facilities, instead of a recommendation status. This is a very important and timely step, as it will allow to synchronize the issue of cyber protection of critical infrastructure with the United States and implement a standard that was created specifically for critical infrastructure, as well as remove the variability of the choice of the approach by which to build cyber security at the objects of critical infrastructure.

At the same time, for some energy companies, this may lead to the need to fulfill various requirements in the field of cyber security, which will require more resources for their implementation. In addition, at the moment there is a very small number of specialists on the Ukrainian market who have the necessary competencies to conduct audits and implement NIST CSF, since this framework was practically not used in Ukraine before.

Thus, it can be concluded that the implementation of NIST is a very useful and timely initiative for the cyber protection of critical infrastructure, including the energy sector, but it raises new challenges, namely:

- the need to train specialists in audit and implementation of NIST;
- determining the priority of the requirements for building a cyber protection system in the energy industry;
- the need for simultaneous harmonization of the regulatory framework with US and EU requirements at the same time.

[1] A year of devastating cyber attacks in Ukraine: how threats attacked users and organizations, URL: <https://www.eset.com/ua/about/newsroom/press-releases/malware/god-razrushitelnykh-kiberatak-v-ukraine-kak-ugrozy-atakovali-polzovateley-i-organizatsii/>.

[2] Law of Ukraine On the Basic Principles of Cybersecurity in Ukraine, URL: <https://zakon.rada.gov.ua/laws/show/2163-19?lang=en#Text> Application date: 15.05.2022.

- [3] Law of Ukraine On information protection in information and communication systems, URL: <https://zakon.rada.gov.ua/laws/show/80/94-бп?lang=en#Text> (link is external) Application date: 15.05.2022.
- [4] Resolution of the Cabinet of Ministers of Ukraine On Approval of General Requirements for Cyber Protection of Critical Infrastructure Objects, URL: <https://zakon.rada.gov.ua/laws/show/518-2019-п?lang=en#Text> Application date: 15.05.2022.
- [5] Law of Ukraine On Critical Infrastructure, URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text>.
- [6] Order No. 601 dated October 6, 2021 of Administration of the State Service for Special Communications and Information Protection of Ukraine "Methodical recommendations on increasing the level of cyber protection of critical information infrastructure", URL: <https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601>.
- [7] NIST Cybersecurity Framework, URL: <https://www.nist.gov/cyberframework>.
- [8] Resolution of the Cabinet of Ministers of Ukraine "Some issues of conducting an independent audit of information security at critical infrastructure facilities", URL: <https://www.kmu.gov.ua/npas/deiaki-pyannia-provedennia-nezaleznoho-audytu-informatsi-inoi-bezpeky-na-s257-240323>.
- [9] Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity (recast), URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0943&from=EN>.
- [10] Network Code on Cybersecurity Drafting Status, URL: https://www.entsoe.eu/network_codes/nccs/.

IMPROVEMENT OF THE CONTROLLING SYSTEM TO ENSURE ENERGY MANAGEMENT OF TECHNICAL SYSTEMS

To improve the quality of technological processes, it is necessary to improve the existing systems for forecasting and controlling energy management of technological processes. Controlling of energy management should be based on correct boundary value problems with differential equations that describe the state of the modeled system. The question of the correctness of boundary value problems arises most significantly when it is necessary to ensure energy management control for technological processes over multilayer, heterogeneous, microscopic objects. In this case, to substantiate the conditions for the correctness of boundary value problems with differential equations, the author proposes to use the method of parametrization in the space of generalized, upper-bounded power functions. This means that it is necessary to find conditions on the functions of solutions to boundary value problems under which the Fourier symbol of the underlying differential equation can be written as a sum of infinitely differentiable functions bounded together with their derivatives on a segment of the real axis. Among the scientific publications related to the subject matter studied by the author of this work, it is necessary to distinguish scientific publications [1, 2], which present mathematical models and methods for improving the quality of functioning of complex systems containing concentrated sources of physical field loading.

To control energy costs, the author proposes to implement an applied optimization mathematical model for minimizing the deviation of the obtained value of the physical field from its assumed value, obtained on the basis of an expert assessment of the technical parameters of the hardware used to support the technological process. It should be noted that in order to control energy management, it is necessary to solve boundary value problems many times over. Thus, it was possible to increase the accuracy of controlling the energy management of technological processes by solving boundary value problems and implementing the specified applied optimization mathematical model.

- [1] Romanova T.E. Proportional Packing of Circles in a Circular Container. / Romanova T.E., Stetsyuk P.I., Fischer A., & Yaskov G.M. // *Cybernetics and Systems Analysis*. – 2023. – No. 59. – Pp. 82–89. <https://doi.org/10.1007/s10559-023-00544-8>
- [2] Levkin D. Upravlinnia yakistiu tekhnichnykh rishen v biotekhnologichnykh protsesakh. / Levkin D., Zhernovnykova O., Shtonda O. // *Vcheni zapysky Tavriiskogo Natsionalnogo Universytetu imeni V.I. Vernadskogo. Serii: «Tekhnichni nauky»*. – Kyiv, 2023. – Vol. 34(73). No. 1. – S. 108–112. <https://doi.org/10.32782/2663-5941/2023.1/16>

I. Furtat, Yu. Furtat

METHODS FOR EXPERIMENTAL STUDIES OF HEAT AND MASS TRANSFER PROCESSES DURING DYEING OF TEXTILE MATERIALS

Carrying out the dyeing process under intensified high-temperature conditions imposes its own specific requirements on the methods of experimental studies of these processes. All methods for measuring the diffusion coefficients of a dye in a fiber can be divided into two main groups - differential and integral. In integral methods, the change in average concentrations in the substrate over time is determined, and in differential methods, the spatio-temporal change in concentrations is determined.

Integral methods include: the method of diffusion through membranes, the method of determining the delay time, the method of kinetic curves of fixation, when dyeing from baths of constant and variable composition; method for determining the dependence of the diffusion coefficient on concentration. In the case of intensive dyeing processes occurring under non-stationary temperature and concentration conditions, with variable properties of the solvent and substrate, integral methods for determining the diffusion coefficients seem generally inapplicable. Differential methods include methods for studying the concentration profiles of dye distribution in the substrate. In one case, the substrate is modeled as plastic of infinite thickness with a constant dye diffusion coefficient in the polymer. Solutions of the equations are obtained for two limiting cases: a very large excess of the dye in the external solution (suspension) and a very small amount outside the fiber. If it depends on the concentration of the dye, the Matano-Boltzmann method or the Hull method, which is a modification of the Matano-Boltzmann method, is used. It should be noted that in the case when the process occurs under variable concentration boundary conditions, the Matano-Boltzmann method is not applicable. In regard of the procedure for determining the distribution of dyes in the substrate, the following most widely used methods can be noted: 1) Method of multilayer membranes; 2) Method of diffusion from the end of the lamina; 3) Microsection method; 4) Radioactive labeling method.

As for the first two methods, they can give a very approximate idea of the diffusion coefficients. First, in the case of a study of the diffusion process in a fiber, the latter is modeled by a lamina. The interrelation of polymer molecules in a fiber and a lamina is different, just as relaxation stresses, swelling, etc. are also different. Therefore, the modeling of such capillary-porous colloidal bodies is a very conditional technique. Secondly, even in the case of determining the diffusion coefficients in laminas, these methods are quite approximate, and under intensified modes are simply incorrect, since in the first case the effect of the lamina-liquid interfaces between the lamina layers is practically not taken into account, and in the second case, the identity of diffusion processes is postulated along and across the lamina, which also seems to be very controversial.

S. Grechko

VERIFYING MODELS WITH COQ

As by now “modeling” plays a crucial role in the whole science and engineering. We can be a bit more specific and replace “modeling” with “mathematical modeling” nearly without loss of generality. A “mathematical model” is an abstract description of some system within some mathematical framework (like analytical geometry, probability theory, computability and algorithms, etc.) and thus it may or may not be inadequate. Obviously, one has to take extra care not to use a wrong model to explain a real world phenomena. Hence, the “mathematical model verification” problem comes.

To “verify a mathematical model” is to somehow gain more confidence that it does represent the system correctly enough. There are two major approaches here: an empirical one, aiming to run a series of experiments and compare predicted output with an observed one and thus get a statistical acknowledgement of how accurate the model is. This type of knowledge is known to be an “inductive” one: the more experiments one runs, the stronger confidence he achieves yet it never reaches 100%. The other way to do it is by “deduction” - to provide a correct mathematical proof that the given model fulfills its formal specification and requirements and can not possibly violate it. This paper is focused on the later one.

Logic and writing proofs is (arguably) not the hardest part; “axiomatization” and “formalization” of the system seems to be much harder. By “axiomatization” an act of defining concrete mathematical axioms is meant; these could be any axioms whatsoever as long as no contradiction could be derived, which would render such a system completely useless. “Formalization” means a rather similar but not identical act: a typical mathematical model is attached to a certain mathematical context and operates on some other mathematical objects (like real numbers, previously proved theorems, fundamental isomorphism and whatnot). Therefore, a typical verification requires this context to be well defined - at least as rigorous, as the set of axioms itself. Once the system has these two, one may derive a purely mechanical, machine-verifiable proof of its adequacy.

This is what Wikipedia says about Coq: “Coq is an interactive theorem prover first released in 1989. It allows for expressing mathematical assertions, mechanically checks proofs of these assertions, helps find formal proofs, and extracts a certified program from the constructive proof of its formal specification. Coq works within the theory of the calculus of inductive constructions, a derivative of the calculus of constructions. Coq is not an automated theorem prover but includes automatic theorem proving tactics (procedures) and various decision procedures”. A few more words also to be told about the “calculus of inductive constructions”, let’s cite Wikipedia again: “the CoC is a higher-order typed lambda calculus, initially developed by Thierry Coquand. It is well known for being at the top of Barendregt’s lambda cube. It is possible within CoC to define functions from terms to terms, as well as terms to types, types to types, and types to terms. The CoC is strongly normalizing, and hence consistent”.

Practically, it implies that in order to verify some model, one needs to define it in terms of higher-order typed lambda calculus, which is known to be powerful enough to capture if not entire than most of the mathematics. Given it's done, one has to pick a mathematical framework to be based upon; there are two options, generally:

- A ZF(C) set theory with an axiom of excluded middle (AEM) implied implicitly.
- A (constructive) type theory in the Brouwer-Heyting-Kolmogorov sense - with the AEM ignored.

By its nature, Coq fulfills the later one, while being agile enough to allow AEM to be defined within it with no sudden contradictions. As such, it pays to dive into details:

“Briefly, Brouwer viewed mathematics as the activity of building constructions in the mind (of an ideal mathematician); mathematics is about such mental constructions, not about objects in some outside reality. For Brouwer, there is no platonistic universe of abstract ideas existing somewhere quite independently of human cognition. In his thesis, Brouwer had not yet realized the effect of his views on logic; but in a paper which appeared a year later, in 1908 (“On the unreliability of the logical principles”) he did see the consequences. He demonstrated that from an intuitionistic point of view, we cannot assume that a mathematical statement is either true or false, independent of human knowledge; we can assert “A or not A” only in case we either have a proof of A or an argument showing that any attempt at constructing a proof of A must fail.

This was made explicit, first by Heyting (1898-1966) in 1930, and more fully in 1934, and independently by Kolmogorov (1903-1987) in 1932. Actually, Heyting and Kolmogorov regarded their respective formulations as distinct. To convey the idea, let us consider the explanations of disjunction, implication, and negation in Heyting’s formulation:

- A proof of “A or B” is given by exhibiting either a proof of A or a proof of B.
- A proof of “A implies B” is a construction transforming any proof of A into a proof of B.
- A proof of “not A” is a construction which transforms any possible proof of A into a contradiction, e.g. $0 = 1$ [1].

That is how Coq forces to construct a proof of a proposition in mind and such a construction is a mathematical object in its own right: it can be thought of as a programming object. Moreover, Coq itself is nothing but a programming language and thus can be copied and shared freely as any other text file, which makes it perfect for collaboration using well-known programming techniques and methodologies (for example, Git).

[1] A.S. Troelstra, From constructivism to computer science, Theoretical Computer Science, Volume 211, Issues 1–2, 1999, Pages 233-252, ISSN 0304-3975, [https://doi.org/10.1016/S0304-3975\(97\)00172-2](https://doi.org/10.1016/S0304-3975(97)00172-2).

DEVELOPMENT OF RENEWABLE ENERGY SOURCES IN UKRAINE

One of the most promising trends in the development of world energy at present is the use of renewable energy sources (RES), which removes a number of problems associated with the use of traditional fuels. According to the definition of the International Energy Agency, renewable energy is energy obtained from the sun, wind, biomass, geothermal, hydropower and ocean resources, biogas, liquid biofuels.

Before the war, a number of regulatory documents and national strategies were adopted in Ukraine, which determine the future direction of the development of renewable energy sources in Ukraine during this and future decades. Thus, in the adopted Energy Strategy of Ukraine until 2035, renewable energy is recognized as one of the main priorities of the energy reform. Renewable energy guarantees environmental safety and energy independence to the entities that implement it. The strategy envisages the possibility of achieving a 25% share of RES in the total primary energy supply by 2035 [1, 2].

The operation of wind (WPP) and solar (SPP) power plants is characterized by the instability of the current capacity. During the day, frequent changes in the amount of generated active power are possible in a significant range, which may affect the work of other power plants of the power system and consumers. In order to respond to these changes in advance, the electric power system must develop taking into account the growth of the share of RES in the country's energy balance. To ensure balance, the electric power system must have a certain amount of generating capacity that can change its operating power in accordance with the load change (increase or decrease).

Variability of the volumes of electricity production of WPP and SPP has a special impact on the operation of the electric power system. The dynamics of the volumes of electricity production by WPP and SPP do not coincide with the dynamics of the volumes of electricity consumption. Therefore, the use of WPP and SPP capacities to cover the current demand has a special effect on the loading modes of HPP, HAPP and TPP power units, which have the ability to maneuver capacity.

In 2021, the share of electricity generated from RES reached 8.1% or 12.8 TW•h, of which 56% — due to solar radiation, 33% — wind energy, almost 8% — due to the burning of biomass and biogas, and 3% accounted for small hydropower plants.

Thus, in 2021, all RES power plants produced 12,804 million kW•h of clean electricity, which was 1,941.9 million kW•h or 17.8% higher than in 2020:

- WPP of Ukraine produced 3,866 million kW•h or 614.4 million kW•h more than in 2020, which is 2.97% of total electricity production;

- SPP produced 7,670 million kW•h or 4.8%, which is 1,065.4 million kW•h more than the amount of electricity produced in the same period of 2020;
- the generation of small hydropower plants increased by 56.1 million kW•h, reaching 276 million kW•h or 0.17% of the total balance;
- Ukrainian bioenergy generated 992 million kW•h or 0.6%, which is 206 million kW•h more than the production level of the previous year.

At the same time, it should be noted that 2021 has become a defining year for the national RES sector, because on May 11, 2021, the daily production of electricity from RES for the first time in the history of Ukraine exceeded the level of generation by thermal power plants — 79 million kW•h versus 77 million kW•h.

In 2021, 731 MW of RES capacity was installed in Ukraine, which received a "green" tariff (Feed-in tariff), while in 2020 this indicator was almost twice as high — 1,337 MW, according to the calculations of the National Commission, which carries out state regulation in the spheres of energy and communal services. [3]. According to the regulator, the total installed capacity of renewable energy facilities in Ukraine as of the end of 2021 reached 8,451 MW.

The large-scale war launched by russia on the territory of Ukraine in February 2022 left the RES sector in a state of waiting and uncertainty, which deepened not only due to active hostilities, damage and occupation of energy facilities, but also due to the artificial creation by individual state structures of additional problems and challenges in the market.

Despite this, the political will of Europe, aimed at maximally reducing its dependence on russian fossil fuels at the expense of increasing the pace of RES development, gives hope for a bright future for the Ukrainian RES market, which is not only a direct part of the European energy system, but also has sufficient capacities to replace a significant part of russian energy resources with its own renewable generation [4].

- [1] On the approval of the Energy Strategy of Ukraine for the period until 2035 "Security, energy efficiency, competitiveness".— Decree of the Cabinet of Ministers of Ukraine dated August 18, 2017, No. 605, Kyiv.
- [2] On amendments to Article 9-1 of the Law of Ukraine "On Alternative Energy Sources" regarding the settlement of the issue of electricity generation by private households. — Law of Ukraine. Information of the Verkhovna Rada, 2019, No. 32, Article 126. — <https://zakon.rada.gov.ua/laws/show/2755-19#Text>
- [3] National Commission, which carries out State Regulation in the Spheres of Energy and Communal Services.— <http://www.nerc.gov.ua/data/filearch/elektro/energo>
- [4] The renewable energy sector of Ukraine before, during and after the war [V. Omelchenko].— Kyiv, 2022.—<https://razumkov.org.ua/statti/sector-vidnovlyuvanoyi-energetyky-ukrayiny-do-pid-chas-ta-pislya-viyny>

АНАЛІЗ ЗМІН В КЛАСИФІКАЦІЇ ГЛИБОКИХ ГЕОТЕРМАЛЬНИХ СИСТЕМ ЧЕРЕЗ ПОЯВУ НОВИХ РІШЕНЬ В СФЕРІ БУРІННЯ

В останні роки спостерігається значне зростання інноваційних пропозицій в сфері геотермальних систем, зокрема завдяки використанню технологій зі сфери видобутку нафти та газу [6]. Аналіз змін в класифікації саме глибоких геотермальних систем обрано тому, що хоч запропоновані в цій сфері інноваційні рішення і знаходяться ще на стадії дослідження, проте в перспективі здатні зробити застосування геотермальної енергії значно доступнішим. Одночасно, ці рішення потребують своєчасної систематизації з тим, аби краще уявляти стан справ в розглянутій галузі, зокрема й через те, що для опису схожих рішень пропонуються відмінні терміни [2].

Слід відзначити, що власне сам термін «глибокі геотермальні системи» має різні визначення. Так за поділу геотермальних систем на поверхневі (*або* субгеотермальні) та глибокі, то в [2] межа між ними становила 400 м, а в [1] – 500 м. Є й альтернативні класифікації [2], де є поділ на поверхневі (до 400 м), середні (від 400 до 1000 м) та глибокі (глибше 1000 м). В розглянутих інноваційних рішеннях глибина більша за 1000 м, тому можливо однозначно використовувати термін «глибокі геотермальні системи».

Раніше глибокі геотермальні системи переважно класифікували залежно від типу їх ресурсу на дві категорії: **гідротермальні**, в яких використовуються тепло та глибокі підземні термальні води у вигляді геотермального теплоносія; та **петротермальні**, в яких використовується тепло перегрітих сухих гірських порід [1, 2]. В першому випадку вже є придатний для використання резервуар, а в другому випадку необхідно створювати окремий теплообмінник та організувати циркуляцію теплоносія через нього [1].

Такі системи можна характеризувати як традиційні (рис. 1а), що не використовують додаткового стимулювання теплообміну та є переважно розташованими в регіонах на межі тектонічних плит, геотермальні ресурси яких характеризувались значним надходженням теплоти, наявністю води в гірських породах та високою ступінь проникності гірських порід [5].

Наступним типом є «вдосконалена (або штучна) геотермальна система» (*англ.* enhanced (or engineered) geothermal system, EGS), яка покращувала проникність геотермального родовища за допомогою гідравлічної, хімічної та теплової стимуляції. Терміном EGS можуть позначати системи як гідро-, так й петротермальні, і хоча певні джерела його оминають [2], загалом термін отримав широке застосування [4–6]. Переважно EGS демонструють як дві вертикальні свердловини з розривом пласту (рис. 1, b), але сьогодні є й більш оновлені концепції [5], які використовують горизонтальне буріння та багатостадійну технологію гідророзриву пласта (рис 1, c).

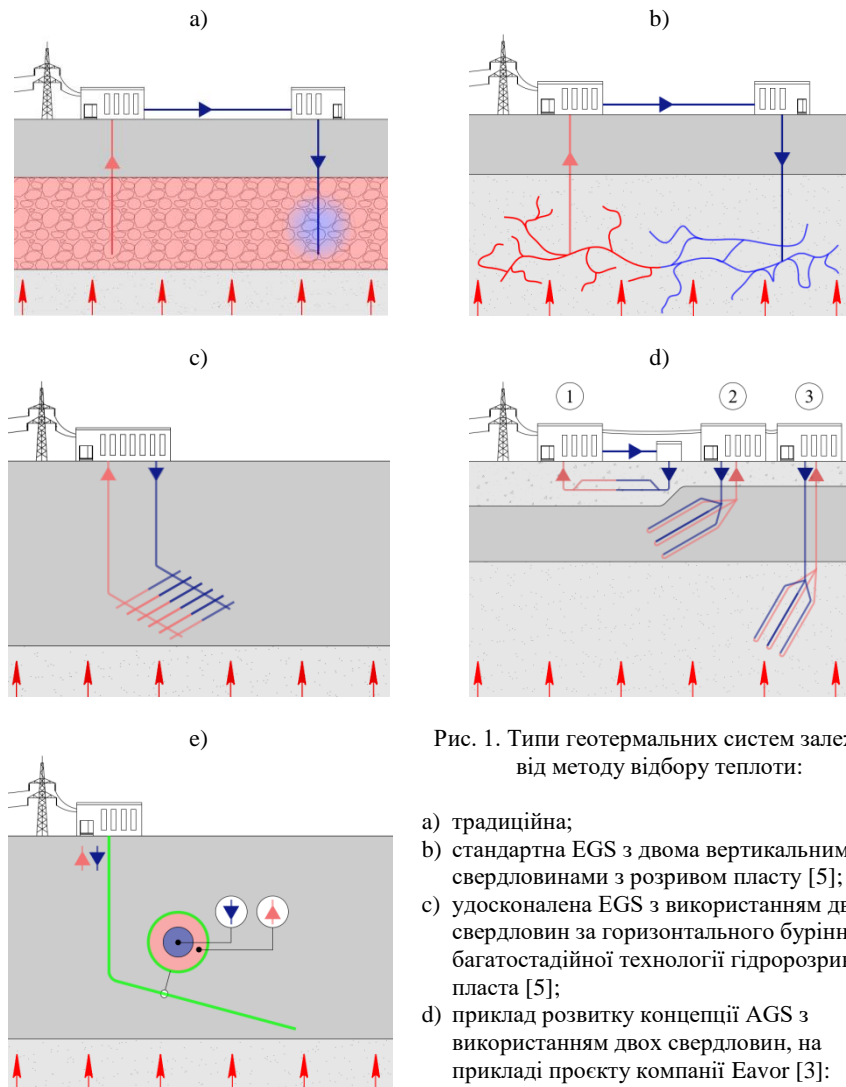


Рис. 1. Типи геотермальних систем залежно від методу відбору теплоти:

- a) традиційна;
- b) стандартна EGS з двома вертикальними свердловинами з розривом пласту [5];
- c) удосконалена EGS з використанням двох свердловин за горизонтального буріння та багатостадійної технології гідророзриву пласта [5];
- d) приклад розвитку концепції AGS з використанням двох свердловин, на прикладі проекту компанії Eavor [3]:

- (1) перша фаза впровадження проекту, з горизонтальним теплообмінником;
- (2) друга фаза впровадження проекту, з масштабуванням продуктивності до мінімального рентабельного значення, з нижчим та похилим розміщенням теплообмінника;

- (3) третя фаза проекту, впровадження якої й буде фактичним проривом в розвитку технології, а продуктивність має бути значною;

- e) AGS з використанням теплообмінника типу «труба в трубі» [5].

Подальші інноваційні рішення в геотермальних системах переважно характеризують за допомогою трьох термінів. **Першим** є вдосконалена геотермальна система (*англ.* advanced geothermal system, AGS), що позначає глибокі, великі, штучні замкнуті контури, в яких циркулює теплоносії, що нагрівається гірськими породами високої температури, тобто теплообмін здійснюється за рахунок теплопровідності [4]. AGS не потребує водоносного пласта і може бути застосована практично в будь-якому місці. Однак через потребу в довгих свердловинах, вартість таких систем є вищою (рис. 1, d-e). AGS можна характеризувати як петротермальну, проте за своєю конструкцією та технологією створення вона значно відрізняється від петротермальних систем, що використовувались раніше. **Другим** є надкритична геотермальна система (*англ.* supercritical geothermal system, SGS), яка використовує природний резервуар, що містить рідину в надкритичному стані [4]. Ця система має бути продуктивнішою за традиційні, але потребуватиме вдосконалення технології буріння та спеціальних матеріалів. В [5] SGS розглядали в розділі про AGS, а в [4, 6] – як окрему систему. **Третім** є «гібридна геотермальна система» (*англ.* hybrid geothermal system, HGS), яка є або геотермальною системою поєднаною з/зі: іншим джерелом енергії, зберіганням CO₂, акумуляцією теплоти, видобутком ресурсів (зокрема, літію), забезпеченням опріснення води, виробництвом водню; або яка поєднує різні типи геотермальних систем [4–6].

Отже, проведені дослідження показали, як останні інновації в сфері геотермальної енергетики призвели до розширення та ускладнення класифікацій геотермальних систем, зокрема й те, що нові системи вже не мають бути прив'язані до природних джерел з високою температурою теплоносія, а можуть бути створені й в будь-яких інших регіонах.

- [1] Відновлювані джерела енергії / За заг. ред. С.О. Кудрі. – Київ: Інститут відновлюваної енергетики НАНУ, 2020. – 392 с.
- [2] Breede K., Dzebisashvili K., Falcone G. (2015) Overcoming challenges in the classification of deep geothermal potential // *Geothermal Energy Science*. 2015. № 1 (3). P. 19–39. <https://doi.org/10.5194/gtes-3-19-2015>
- [3] Eavor. Technology. (2023). URL: <https://www.eavor.com/technology/> (accessed: 29.04.2023).
- [4] International Renewable Energy Agency - IRENA. (2023). Global geothermal market and technology assessment. Abu Dhabi, UAE. URL: <https://www.irena.org/Publications/2023/Feb/Global-geothermal-market-and-technology-assessment> (accessed: 29.04.2023).
- [5] Livescu S. et al. The University of Texas at Austin (2023). Chapter 1: Geothermal and Electricity Production: Scalable Geothermal Concepts in The Future of Geothermal in Beard J.C. & Jones B.A. (eds) Texas: Contemporary Prospects and Perspectives. Austin: The University Of Texas At Austin, 2023. P. 25-46 <https://doi.org/10.26153/TSW/44083>
- [6] Patel S. (2023) Startups Are Shaking Up Geothermal Power's Prospects // *POWER*. URL: <https://www.powermag.com/startups-are-shaking-up-geothermal-powers-prospects/> (accessed: 29.04.2023).

ДОСЛІДЖЕННЯ МЕТОДУ ВЕРИФІКАЦІЇ TLC ПРИ ВИРШЕННІ ЗАДАЧ ЕНЕРГЕТИКИ

Обчислювальні і просторові витрати, супутні прикладному застосуванню формальних методів, зокрема методів перевірки на моделі, істотним чином залежить від архітектурної складової (структури і зав'язків) артефактів, що залучаються у якості вихідних конструкцій, на основі яких синтезуються відповідні формалізовані подання [3]. Названа складова обумовлюється, у тому числі, сценарієм предметної області, який подається на етапі проектування процесу розроблення у формі відповідного артефакту – блок-схеми алгоритму, UML-діаграми (Unified Modeling Language) дій тощо – сутності, що характеризується архітектурою і змістом [2]. Показовими є, наприклад, сценарії, що мають місце у сфері авіоніки [4]. У якості граничних випадків раніше було охоплено також синтетичні сценарії [5, 6].

Для доповнення / узагальнення попередньо зроблених висновків стосовно обчислювальних і просторових витрат, супутніх прикладному застосуванню поширеного формального методу перевірки на моделі TLC (TLA Checker), дослідження останнього було проведено також і по відношенню до артефакту, яким оперують у галузі енергетики, – артефакту-подання (у формі відповідної рольової моделі – UML-діаграми дій) процесу оновлення реєстру міжнародних ідентифікаційних кодів [7], що має місце за гармонізованої моделі європейського ринку електроенергії [1]. Названий метод при цьому застосовано по відношенню до формалізованого подання зазначеного артефакту.

Досліджено дві альтернативні реалізації методу – на основі обходу простору станів системи переходів у ширину (BFS, Breadth-first Search) і у глибину (DFS, Depth-first Search). Отримані результати показали, зокрема, істотно вищі просторові витрати, супутні DFS-реалізації методу, у порівнянні із витратами, супутніми альтернативній BFS-реалізації. Проведено також оцінювання характеру зростання названих витрат із збільшенням числа програмних обчислювальних потоків [7].

- [1] Blinov I., Tankevych S. The harmonized role model of electricity market in Ukraine. 2016 2nd International Conference on Intelligent Energy and Power Systems, IEPS (Kyiv, Ukraine, June 07–11, 2016). doi: <https://doi.org/10.1109/IEPS.2016.7521861>
- [2] Broy M. A logical approach to systems engineering artifacts and traceability: from requirements to functional and architectural views. Engineering dependable software systems: NATO Science for Peace and Security Series - D: Information and Communication Security / eds. M. Broy, D. Peled, G. Kalus. Amsterdam: IOS Press, 2013. Vol. 34. P. 1-48. DOI: <https://doi.org/10.3233/978-1-61499-207-3-1>
- [3] Shkarupylo V., Blinov I., Chemeris A., Dusheba V., Alsayaydeh J., Oliinyk A. Iterative Approach to TLC Model Checker Application. Proc. 2021 IEEE KhPI

- Week on Advanced Technology (Kharkiv, Ukraine, September 13 – 17, 2021). P. 283–287. DOI: <https://doi.org/10.1109/KhPIWeek53812.2021.9570055>
- [4] Shkarupylo V., Alsayaydeh J.A.J, Tomičić I., Chemeris A., Dusheba V. A technique for checking the adequacy of formal model. ARPN Journal of Engineering and Applied Sciences. August 2021. Vol. 16, No. 16. P. 1707-1719. URL: http://www.arpnjournals.org/jeas/research_papers/rp_2021/jeas_0821_8670.pdf (дата звернення: 28.04.2023).
- [5] Shkarupylo V. V., Tomičić I., Kasian K. M. The investigation of TLC model checker properties. Journal of Information and Organizational Sciences. 2016. Vol. 40, No. 1. P. 145-152. DOI: <https://doi.org/10.31341/JIOS.40.1.7>
- [6] Shkarupylo V. V., Tomičić I., Kasian K. M., Alsayaydeh J. A. J. An Approach to increase the Effectiveness of TLC Verification with Respect to the Concurrent Structure of TLA+ Specification. International Journal of Software Engineering and Computer Systems. 2018. Vol. 4, No. 1. P. 48-60. DOI: <https://doi.org/10.15282/ijsecs.4.1.2018.4.0037>
- [7] Shkarupylo V., Blinov I., Dusheba V., Alsayaydeh J. A. J. Case Driven TLC Model Checker Analysis in Energy Scenario. Proc. of the Sixth International Workshop on Computer Modeling and Intelligent Systems, CMIS-2023 (Zaporizhzhia, Ukraine, May 3, 2023). P. (прийнято до друку). URL: <https://www.youtube.com/watch?v=MErmrlRdLg0> (дата звернення: 28.04.2023).

Д.П. Сінько

ПАРАМЕТРИ МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ ПАРТИЦІОНУВАННЯ КІБЕРНЕТИЧНОЇ СКЛАДОВОЇ В ІНДУСТРІАЛЬНИХ КІБЕРФІЗИЧНИХ СИСТЕМАХ ЕЛЕКТРОЕНЕРГЕТИЧНИХ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ

Кіберфізичні системи електроенергетичних інтелектуальних систем (SmartGrid) мають надзвичайно складну структуру як фізичної, так і кібернетичної складової. Основним чинником, який пояснює таку складність, є географічна розгалуженість фізичних компонентів (генерація, підстанції різних рівнів, споживання), що в свою чергу обумовлює розподілену у просторі структуру кібернетичної складової (далі - КС) [1], що, в свою чергу, призводить до рознесення у просторі інформаційної складової.

Сучасні тенденції в архітектурі розподілених інформаційних систем свідчать про 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. Ноди кластеру можуть знаходитися в одному або декількох дата-центрах, які, в свою чергу, можуть перебувати в одній або декількох географічних локаціях.

Будемо вважати, що всі ноди кластеру є необхідними для гарантовано якісного обслуговування користувачів застосунку. Втрата зв'язку між нодами кластеру може приводити до зменшення продуктивності кластеру або до його повної загибелі, де під “загибеллю кластеру” розуміється перехід кластеру в такий стан, коли застосунок не здатен виконувати обслуговування бізнес транзакцій і кластер самостійно не може відновитися, тобто самотужки повернутися до стану, коли виконання таких транзакцій стає можливим. У відкритих джерелах ця проблема відома як партиціонування кластеру або split brain problem [3] і, за нашим переконанням, її слід віднести до проблем резильєнтності SmartGrid. Зазначена проблема досі не має ефективного вирішення. Саме через це побудова математичної моделі є вкрай важливою науковою та практичною задачею з метою попередження станів кластеру, близьких до партиціонування або «смерті кластеру».

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 $c_{i,i} = 1$ визначає реплікацію.

7. Функція доступності може бути визначена як бінарна функція $A: ((i, j, k), (l, m, n)) \rightarrow \{0,1\}$, 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 дозволяють 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 $n_{i,j,k} \cdot n_{l,m,n} \cdot A((i, j, k), (l, m, n)) \rightarrow \{0,1\}$.

Таким чином 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.

МОДЕЛЮВАННЯ ЗБІРНОГО УЛЬТРАЗВУКОВОГО СОНОТРОДУ З ВІБРУЮЧОЮ ЄМНІСТЮ

Одним із видів технології для обробки деталей з метою зміцнення поверхневого шару є спосіб пластичного деформування поверхні під дією металевих кульок в замкненій ємності. Якщо ця ємність вібрує з ультразвуковою частотою, то кожна частина її внутрішньої поверхні передає кінетичний імпульс металевій кульці. Таким чином формується стохастичне поле переміщення металевих кульок всередині ємності, які, в свою чергу, передають кінетичну енергію до поверхні деталі що обробляється [1]. Ефективність цієї технологічної операції безпосередньо залежить від ефективної роботи даної ємності, тобто важливо контролювати значення амплітуд переміщення та вид їх розподілу на поверхні ємності.

Пропонується розглянути збірний сонотрод, який складається з двох частин: циліндричної оболонки та сонотрода-конвертора, який будемо називати сонотродом типу «грибок» [2,3]. В якості вібруючої ємності використовується циліндрична оболонка. Обидві частини збірного сонотроду мають однакову власну резонансну частоту, в даному випадку, це 20 кГц. На рис.1 показано вигляд та епюри резонансної моди коливань циліндричної оболонки та складного сонотрода-конвертора типу «грибок». На поверхні оболонки та сонотрода-конвертора позначимо характерні точки в яких будемо контролювати переміщення. В розрахунках було враховано втрати в матеріалі частин збірного сонотроду та збуджувальне навантаження гармонійного типу (напряг навантаження показано червоними стрілками).

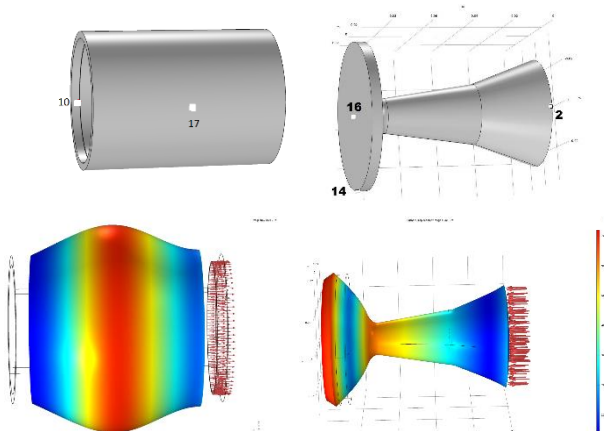


Рис. 1. Форми сонотродів та епюри переміщень на поверхнях двох частин збірного сонотроду

На рис.2 показано залежність модуля переміщення в позначених характерних точках на поверхні оболонки та сонотроду типу «грибок» від частоти збуджувальної сили.

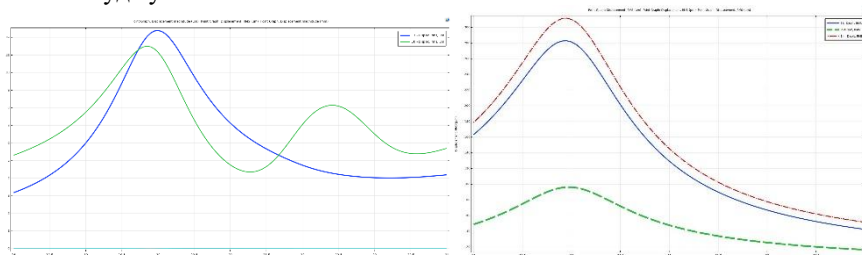


Рис. 2. Графіки модуля переміщення характерних точок на поверхні оболонки та сонотроду від частоти збуджувальної сили

Збірний сонотрод будується шляхом з'єднання внутрішньої циліндричної поверхні ділянки біля торця оболонки з циліндричною поверхнею малого конусу складного сонотроду типу «грибок», як показано на рис.3 [4]. Червоними стрілками показано навантаження збірного сонотроду. При розрахунках були враховані механічні втрати в матеріалах. Характерна точка 5, в якій ведеться спостереження за переміщенням, розташована в центрі на поверхні диску сонотроду.

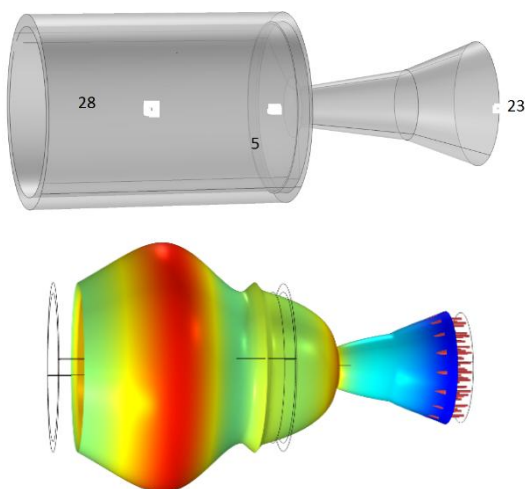


Рис. 3. Зовнішній вигляд збірного сонотроду та епіюра модуля переміщень на його поверхні.

Графіком на рис. 4 показано залежність значення модуля переміщення в характерних точках на поверхні збірного сонотроду від частоти збуджувальної сили.

Можна бачити, що коливання циліндричної оболонки в складі збірного сонотроду має резонансний характер. Амплітуда коливань на середині

циліндричної поверхні та на донній частині ємності приблизно однакові. Посилення амплітуди переміщення на циліндричній поверхні оболонки в складі збірному сонотроду приблизно в 5 разів більше порівняно з значенням при власних коливаннях окремої оболонки.

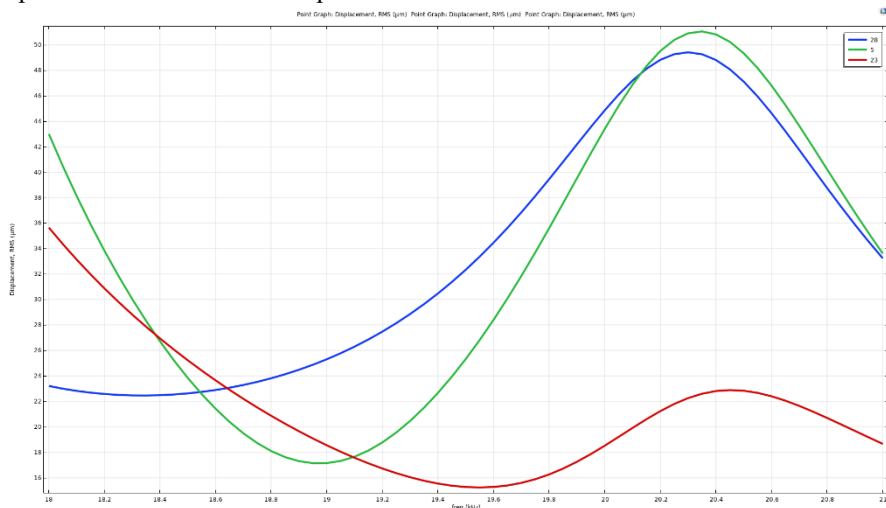


Рис. 4. Модуль амплітуди переміщення точок контролю збірному сонотроду залежно від частоти збуджувальної сили

Наведені результати по моделюванню даного збірному сонотроду показують можливість використання такого типу сонотродів в технології обробки деталей методом бомбардування металевими кульками.

Коло вимог, які ставить технологія обробки поверхні до моделювання ультразвукових сонотродів, вивчено ще недостатньо. Робота над цією задачею визначить напрям робіт на найближчу перспективу.

- [1] Технологическое обеспечение эксплуатационных характеристик деталей ГТД. Лопатки компрессора и вентилятора. Часть 1. Монография. Запорожье, из-во ОАО «Мотор Сич» 2003г. -396с.
- [2] И.К. Сенченков Модальная классификация и проектирование сонотродов для ультразвуковой обработки материалов.//Акустичний вісник. 1998.Т.1 №4 С.55-64
- [3] Сенченков И.К., Козлов В.И., Червинко О.П., Василенко О.Н. К проектированию волноводов с осесимметричной продольно-изгибной модой колебаний//Прикл.мех.-1992.-28, №8.-С.24-29.
- [4] Дяченко С.М. Задача моделювання модальних характеристик збірному сонотроду для ультразвукового зварювання полімерів. Кібербезпека енергетики, науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України : матеріали, 27 травня 2022 р. Київ : ІПМЕ ім. Г.Є.Пухова НАН України, 2022. 129 с.

М.В. Антонішин, В.В. Цуркан

ФОРМУВАННЯ СЦЕНАРІЇВ ТЕСТУВАННЯ УРАЗЛИВОСТЕЙ МОБІЛЬНИХ ПРОГРАМНИХ ЗАСТОСУНКІВ МЕТОДОМ ТОПОЛОГІЧНОГО СОРТУВАННЯ

Нині спостерігається тенденція до орієнтованості типових підходів тестування уразливостей мобільних програмних застосунків на [1], по-перше, окремі аспекти їхнього функціонування. По-друге, суб'єктивне обирання фахівцями кейсів для формування сценаріїв тестування. Подолання даних обмежень досягається використанням графу залежностей [2]. З цим пов'язане встановлення відношень між кейсами і їхнє упорядкування. Тому формування сценаріїв тестування уразливостей мобільних програмних застосунків методом топологічного сортування є актуальним завданням.

Сценарії тестування уразливостей мобільних програмних застосунків формуються упорядкуванням кейсів як вершин графу залежностей. Таке впорядкування застосуванням методу топологічного сортування зводиться до отримання у кінцевому випадку потрібної послідовності дій [3]. Характерною її особливістю є залежність наступного кейсу від виконання попереднього в сценарії тестування уразливостей мобільних програмних застосунків. Наприклад [1], при виявленні уразливостей SSL pinning запускання проксі (BurpSuite, ZAP) передє імплементуванню його сертифікату.

Топологічне сортування кейсів тестування уразливостей мобільних програмних застосунків реалізується різними способами. З огляду на популярність серед них рекомендується використання пошуку в глибину. Такий вибір до того ж обумовлюється його наглядністю і простотою реалізування на практиці. Тож зберігання списку кейсів тестування уразливостей мобільних програмних застосунків організовується за допомогою стеку.

Отже, використання методу топологічного сортування дозволяє формувати сценарії тестування уразливостей мобільних програмних застосунків шляхом упорядкування відповідних кейсів. Це може бути реалізовано різними способами, однак серед них одним з найбільш популярних є пошуку в глибину. Незважаючи на це поза увагою залишається урахування динаміки появи додаткових кейсів при тестуванні уразливостей мобільних програмних застосунків і, як наслідок, нових вершин графу залежностей.

- [1] Antonishyn M. Mobile applications vulnerabilities testing model. Information Technology and Security. 2020. Vol. 8, Iss. 1 (14). P. 49–57. DOI: <https://doi.org/10.20535/2411-1031.2020.8.1.218003>.
- [2] Antonishyn M. The usage of dependency graphs to test the security of mobile software applications. Computer and information systems and technologies : Proceedings of Fourth International Scientific and Technical Conference (Charkiv, 22–23 April 2020). Charkiv, 2020. P. 44. DOI: <https://doi.org/10.30837/IVcsitic2020201369>.
- [3] Introduction to Algorithms / Cormen T. H., Leiserson C. E., Rivest R. L., Stein C. Cambridge : MIT Press, 2022. P. 573–575.

ПЕРСПЕКТИВИ УЧАСТІ СИСТЕМ НАКОПИЧЕННЯ ЕНЕРГІЇ В РИНКУ ДОПОМІЖНИХ ПОСЛУГ

Збільшення частки генерації енергії з відновлюваних джерел енергії (ВДЕ) на фоні обмежених обсягів маневрових потужностей створює ризики для балансової надійності енергосистеми через мінливий характер сонячної та вітрової енергії. Системи накопичення енергії (СНЕ) можуть допомогти вирішити пов'язані з цим проблеми, що посилює їх актуальність в сучасних умовах України.

У 2022р. Верховна Рада України ухвалила Закон про накопичення електроенергії та системи накопичення електроенергії (№ 5436-д), який набув чинності 16.06.2022р., визначаючи статус систем накопичення та операторів накопичувачів енергії. Прийнятий закон має сприяти розвитку СНЕ в Україні та стимулювати ринок ВДЕ. Закон також містить положення щодо створення операторів накопичувачів енергії, визначаючи зберігання енергії як діяльність, пов'язану з відбором електроенергії для подальшого використання [1]. У липні 2022 року Національна комісія, що здійснює державне регулювання у сфері енергетики та комунальних послуг (НКРЕКП) запровадила ліцензійні вимоги для накопичувачів потужністю понад 150 кВт, забезпечивши сприятливі умови для проектів будівництва СНЕ, спрямованих на оптимізацію функціонування ринку електроенергії шляхом збалансування графіків споживання та виробництва електроенергії [2].

Ринок допоміжних послуг, що був запроваджений на ринку електроенергії в Україні у липні 2019 року, надає можливість регулювання потужності і частоти в енергосистемі та забезпечення надійного енергопостачання електроенергією високої якості [3].

В рамках регулювання частоти та потужності в ОЕС України цим законом передбачається забезпечення резервів підтримки частоти, резервів відновлення частоти, резервів заміщення, що відповідають первинному, вторинному і третинному регулюванню, у якості яких можуть виступати системи накопичення енергії. Для забезпечення первинного і вторинного регулювання частоти і потужності в енергосистемі необхідно використовувати резерви потужності з високою швидкодією [4], яким найкраще відповідають накопичувачі на базі наступних технологій: індуктивні накопичувачі, маховики, суперконденсатори та електрохімічні батареї (наприклад, літій-іонні). Створення третинного резерву менш чутливе до швидкодії, а більше залежить від загальних обсягів потужності. Для цілей третинного регулювання можна додатково використовувати гідроакумуючі електростанції та станції, що використовують енергію стисненого повітря.

Стосовно забезпечення підтримки параметрів надійності та якості електричної енергії в ОЕС України, на ринку допоміжних послуг

передбачено послуги з регулювання напруги та реактивної потужності, а також послуги із забезпечення відновлення функціонування ОЕС України після системних аварій [3]. Системи накопичення також можуть бути залучені до регулювання напруги та реактивної потужності [5]. Так, наприклад, наявність відповідної функції в силових перетворювачах батарейних накопичувачів дозволяє компенсувати реактивну потужність без витрачання ресурсу батарей, а їх відносна компактність дозволяє встановлювати їх поблизу великих споживачів, що містять великі індуктивні чи ємнісні навантаження. У разі виникнення аварійних ситуацій накопичувачі можуть стати джерелом стартового струму для запуску інших електростанцій та відновлення нормальної роботи енергосистеми [6].

Законом передбачено можливість створення і інших допоміжних послуг. У перспективі можливо введення послуг, які б допомагали знижувати втрати електроенергії в мережах, більш ефективно інтегрувати джерела ВДЕ та розподіленої генерації, тощо.

Таким чином, розширення участі систем накопичення енергії в ринку допоміжних послуг є досить актуальною задачею та, зокрема, сприятиме інтеграції відновлюваних джерел енергії в енергосистему України, підвищенню якості електричної енергії відповідно до встановлених вимог, а також забезпечить сталу і надійну роботу ОЕС України.

- [1] Закон України від 15.02.2022р. №5436д «Про внесення змін до деяких законів України щодо розвитку установок зберігання енергії URL: <https://zakon.rada.gov.ua/laws/show/2046-20#Text>.
- [2] НКРЕКП затвердила Ліцензійні умови провадження господарської діяльності зі зберігання енергії. URL: <https://www.nerc.gov.ua/news/nkrekp-zatverdila-licenzijni-umovi-provazhennya-gospodarskoyi-diyalnosti-zi-zberigannya-energiyi>.
- [3] Закон України від 13.04.2017.№ 2019-VIII «Про ринок електричної енергії» URL: <https://zakon.rada.gov.ua/laws/show/2019-19#Text>.
- [4] Згуровець О.В., Кулик М.М. Можливості формування сучасного резерву підтримки частоти в об'єднаних енергосистемах на базі акумуляторних батарей для автоматичного регулювання частоти та потужності/ Проблеми загальної енергетики, 2022, 1-2(68-69):20-29. doi:10.15407/pge2022.01-02.020.
- [5] Chaudhary, P., and Rizwan, M. (2018). Voltage regulation mitigation techniques in distribution system with high pv penetration: A review. *Renew. Sustain. Energy Rev.* 82, 3279–3287. doi:10.1016/j.rser.2017.10.017.
- [6] YAO, L., YANG, B., CUI, H. et al. Challenges and progresses of energy storage technology and its application in power systems. *J. Mod. Power Syst. Clean Energy* 4, 519–528 (2016). doi:10.1007/s40565-016-0248-x.

МОДЕЛІ ОПТИМІЗАЦІЇ ПОРТФЕЛЮ ТА МЕТОДИ МОДЕЛЮВАННЯ ЗАДАЧ КУПІВЛІ-ПРОДАЖУ ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ КОМПАНІЯМИ-ПОСТАЧАЛЬНИКАМИ

На лібералізованих ринках електричної енергії постачальник – один з найважливіших учасників ринку, оскільки виступає в ролі посередника між споживачами на роздрібному ринку та виробниками на оптовому. Як учасник ринку, постачальник укладає договори постачання електроенергії з кінцевими споживачами, здебільшого за фіксованою ціною на весь обсяг річного споживання, формуючи власний портфель продажу. Для забезпечення постачання споживачам постачальники здійснюють купівлю-продаж електроенергії на різних сегментах оптового ринку: за двосторонніми договорами на форвардному ринку та/або на спотових ринках "на добу наперед" та внутрішньодобовому ринку [1], за доволі волатильними ринковими цінами, що формуються для кожної години розрахункового періоду. Окрім того, розбіжність між загальним обсягом електроенергії, придбаної постачальником на всіх сегментах оптового ринку для кожної години розрахункового періоду, та спожитою всіма споживачами постачальника – це небаланс, що врегульовується оператором системи передачі на балансуєчому ринку, та призводить до суттєвих фінансових втрат постачальника.

Рентабельність постачальника залежить від його можливості ефективно спрогнозувати графік навантаження всієї сукупності своїх споживачів та здійснити закупівлю оптимального портфелю продуктів на оптовому ринку за середньозваженими цінами, нижчими за ціни продажу на роздрібному ринку.

Стратегія прийняття рішень постачальником є складним процесом, що прямо впливає на можливість отримання прибутку. Постачальником мають бути сформовані цінові пропозиції, що враховуватимуть вплив висококонкурентного середовища та суттєвий рівень невизначеності обсягів споживання електроенергії. Після аналізу укладених угод на постачання, має бути визначено загальний погодинний графік споживання електроенергії для портфелю споживачів, з урахуванням особливостей різних споживчих моделей, притаманних різним групам споживачів. В свою чергу, постачальник має обрати оптимальний набір продуктів для покриття сформованого графіку споживання з урахуванням широкого вибору контрагентів та інструментів, представлених на оптовому ринку.

Таким чином весь процес прийняття рішень може бути поділений на три основні етапи: формування цінових пропозицій для роздрібного ринку; прогнозування загального графіку споживання електроенергії за укладеними договорами її постачання; оптимізація портфелю закупівлі електроенергії на оптовому ринку. Вирішення задачі збільшення рентабельності постачальника потребує математичного моделювання задач формування портфелю для

кожного з наведених етапів. Відповідно, метою дослідження є розроблення моделі оптимізації портфелю постачальника та методів моделювання задач формування портфелю, придатних для вирішення задач підтримки прийняття стратегічних рішень.

Постачальник здійснює продаж електроенергії споживачам здебільшого за фіксованою ціною не весь період постачання. В статті [7] запропоновано ігрову модель у вигляді моделі Бертрана, що враховує можливість споживача змінювати постачальника і, у такий спосіб, впливати на стратегію роздрібного ціноутворення, що реалізується постачальником. Доведено, що через високу конкуренцію на роздрібному ринку, постачальник має знижувати ціни продажу для збільшення частки ринку. Для вирішення проблеми оптимізації прибутків від продажу на роздрібному ринку в [6] та [8] застосовується математичні моделі задач продажу у вигляді нейронних мереж. Постачальник є фінансово відповідальним за появу небалансів і має складати погодинні графіки обсягів споживання електроенергії для всієї групи своїх споживачів з метою здійснення адекватної закупівлі. В [4] прогнозування графіка споживання електроенергії споживачем представлено у вигляді задачі нелінійного програмування, для вирішення якої застосовано центроїду кластеризацію історичних даних. В [3], з метою оптимізації закупівлі електроенергії, пропонується використовувати модель сезонної авторегресійної інтегрованої ковзної середньої (SARIMA) для генерації великої кількості сценаріїв навантаження споживачів. Натомість, в [6] пропонується застосовувати глибинне машинне навчання штучних нейронних мереж для прогнозування обсягів споживання електроенергії споживачами з урахуванням їх реакції на цінові показники відповідно до моделі ціноутворення, що враховує реагування попиту.

На оптовому ринку постачальник має невеликий вплив на ціни, тобто, фактично, він приймає запропоновані ціни за моделлю «price-taker». Отже, стратегія роботи постачальника на оптовому ринку має бути спрямована на визначення оптимальних обсягів придбання електроенергії на кожному сегменті та за різними умовами для зменшення витрат на придбання. В [5] та [6] проблему оптимізації закупівлі електричної енергії на оптовому ринку запропоновано вирішувати із застосуванням машинного навчання штучних нейронних мереж методами LSTM, A2C та DQN. В [3] представлена стратегія короткострокових рішень для мінімізації витрат через оптимальні рішення щодо купівлі-продажу електроенергії на спотових ринках, використання власної розподіленої генерації та системи накопичення енергії, що визначена через двоетапну стохастичну оптимізаційну модель із застосуванням CvaR для зменшення ризиків. В [9] автори розглядають проблему закупівлі електроенергії у вигляді стохастичної задачі моделювання з обмеженням ризику, що вирішується методом обмеження ризику збитків. Натомість в [4] розглядається стратегія оптимізації закупівлі шляхом поетапного укладання контрактів на різний набір продуктів для максимально ефективного покриття графіку споживання електроенергії з використанням моделі робастної оптимізації.

Через високу конкуренцію на роздрібному ринку різниця між роздрібною та оптовою ціною зменшується. Таким чином, у довгостроковій перспективі спосіб отримання прибутку від різниці між роздрібною та оптовою ціною не зможе повністю забезпечити ефективну роботу постачальників. З метою вирішення проблеми підвищення рентабельності постачальника було проведено дослідження запропонованих моделей та методів оптимізації рішень постачальника. Різноманітність запропонованих підходів дозволяє стверджувати про відсутність ефективної універсальної стратегії. Для забезпечення подальшого розвитку ринку електроенергії в Україні та підвищення рентабельності компаній-постачальників, існує потреба подальшого аналізу, адаптації та вдосконалення математичних моделей задач формування портфелю, що забезпечить прийняття оптимальних рішень постачальником.

- [1] Закон України №2019-VIII вид 13.04.2017 «Про ринок електричної енергії»: <https://zakon.rada.gov.ua/laws/show/2019-19#Text>
- [2] Feihu Hu, Xuan Feng, Hui Cao, A Short-Term Decision Model for Electricity Retailers: Electricity Procurement and Time-of-Use Pricing, *Energies* 2018, 11, 3258, pp 1-18. <https://www.mdpi.com/1996-1073/11/12/3258>
- [3] Josue Campos Do Prado, Ugonna Chikezie, A Decision Model for an Electricity Retailer With Energy Storage and Virtual Bidding Under Daily and Hourly CVaR Assessment, *ACCESS* vol 9, 2021, pp 106181 – 106191. <https://ieeexplore.ieee.org/document/9500199>
- [4] Leandro J. Cesini Silva , Cindy P. Guzman, Marcos J. Rider, Contracting Strategy for Consumers With Distributed Energy Resources in the Liberalized Electricity Market, *ACCESS* vol 10, 2022, pp 80437 – 80447. <https://ieeexplore.ieee.org/document/9844706>
- [5] Yuankun Liu, Dongxia Zhang, Hoay Beng Gooi, Data-driven Decision-making Strategies for Electricity Retailers: A Deep Reinforcement Learning Approach, *Csee Journal Of Power And Energy Systems*, Vol. 7, No. 2, March 2021, pp 358-367. <https://ieeexplore.ieee.org/document/9215156>
- [6] Hongsheng Xu , Jinyu Wen, Senior Member, CSEE, Qinran Hu, Jiao Shu, Jixiang Lu, Zhihong Yang, Energy Procurement and Retail Pricing for Electricity Retailers via Deep Reinforcement Learning with Long Short-term Memory, *CSEE Journal Of Power And Energy Systems*, vol. 8, no. 5, September 2022, pp. 1338-1351. <https://ieeexplore.ieee.org/document/9713968>
- [7] Chen Zhao, Shaohua Zhang, Xian Wang, Xue Li, Lei Wu, Game Analysis of Electricity Retail Market Considering Customers' Switching Behaviors and Retailers' Contract Trading, *ACCESS* vol 6, 2018, pp 75099 – 75109. <https://ieeexplore.ieee.org/document/8546748>
- [8] Hyun-kyeong Hwang, Ah-yun Yoon, Hyun-koo Kang Seung-il Moon, Retail Electricity Pricing Strategy via an Artificial Neural Network-Based Demand Response Model of an Energy Storage System, *ACCESS* vol 9, 2021, pp 13440 – 13450. <https://ieeexplore.ieee.org/document/9310260>
- [9] Liping Guo, Thanaporn Sriyakul, Sayyad Nojavan, Kittisak Jermsittiparsert, Risk-Based Traded Demand Response Between Consumers' Aggregator and Retailer Using Downside Risk Constraints Technique, *Digital Object Identifier ACCESS* vol 8, 2020, pp 90957 – 90968. <https://ieeexplore.ieee.org/document/9091164>

АНАЛІЗ СУЧАСНИХ БАЗ ДАНИХ ВРАЗЛИВОСТЕЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

З кожним роком кількість нових вразливостей безпеки, як в програмних так і в апаратних засобах, постійно збільшується. Для протидії цьому потрібен постійний моніторинг та відстежування нових вразливостей, своєчасне оновлення та використання актуальних систем захисту. Далі розглянемо найпопулярніші бази даних та каталоги вразливостей.

Стандарт **Common Vulnerabilities and Exposures (CVE)** було запущено в 1999 році американською некомерційною дослідницькою корпорацією MITRE для виявлення та класифікації вразливостей у програмному забезпеченні та прошивках апаратного забезпечення. CVE надає організаціям безкоштовну базу для покращення кібербезпеки. CVE на сьогоднішній день основним стандартом у галузі уніфікованого найменування та реєстрації виявлених вразливостей програмного забезпечення. На 2013 рік база даних нараховує 200 тис. CVE записів.

National Vulnerability Database (NVD) — це урядове репозитарій США стандартизованих даних про вразливості, представлених за допомогою протоколу SCAP. Ці дані дозволяють автоматизувати керування вразливістю, вимірювання безпеки та відповідність до вимог безпеки[1].

VulnDB – це найбільш повна та своєчасна аналітична інформація про вразливості, яка надає корисну інформацію про останні уразливості безпеки через простий у використанні портал SaaS або RESTful API, який забезпечує просту інтеграцію з інструментами GRC та системами тікетів. VulnDB дозволяє організаціям шукати та отримувати повідомлення про останні вразливості як у програмному забезпеченні користувача, так і у сторонніх бібліотеках чи залежностях. VulnDB є платною. На 2023 р. вона нараховує більше 300 тис. вразливостей, 100 тис. з яких відсутні в системі CVE[2].

База даних **Vulnerability Notes Database US-CERT (VND от CERT/CC)** належить підрозділу CERT, який є частиною Software Engineering Institute, що фінансується з федерального бюджету центру досліджень та розробок, який керується Університетом Карнегі-Меллона[3].

Кожен запис у базі VND агрегує інформацію про безліч схожих вразливостей для будь-якого конкретного ПЗ, посилаючись на безліч відповідних CVE ідентифікаторів. Дана агрегація є характерною відмінністю бази VND від баз CVE List і NVD, дозволяючи перевірити безліч вразливостей однакового типу в конкретному вразливому ПЗ або його компонентах.

[1] National Vulnerability Database Main page <https://nvd.nist.gov/general>

[2] About VulnDB <https://vulndb.cyberriskanalytics.com/>

[3] SEI CERT Coordination Center. <https://www.kb.cert.org/vuls/>

ІНТУЇЦІЯ ОБЧИСЛЮВАЛЬНИХ СИСТЕМ

Науковці по всьому світові задаються питанням чи буде наділений сильний штучний інтелект заданістю, схожою на людську інтуїцію [1]. Це питання має неабиякий філософський підтекст [2]. Попри те, що феномен інтуїції досі не до кінця досліджений, вчені сходяться на думці, що суть цього феномену полягає у здатності розуміти або знати щось без необхідності думати про це чи використовувати розум, щоб виявити це, або відчутті, яке демонструє цю здатність.

Сильний штучний інтелект, або СШІ, [1], [2], насамперед, це математична модель, що описана деякою формальною мовою у вигляді, прийнятному для запуску такої моделі засобами обчислювальної техніки. Іншими словами, СШІ – це обчислювальна система. Ми уявляємо собі інтелектуальну складову СШІ як певну програму, що реалізує деякий алгоритм, в якому кожен крок є доцільним. Іншими словами, важко провести паралель між несвідомим та детермінованим, де під несвідомим ми будемо розуміти прояв людської інтуїції, а під детермінований чіткі кроки формалізованого алгоритму, за яким стоять певні математичні перетворення.

Щоб прослідкувати тенденцію ми поглянемо на ChatGPT [3], який є нічим іншим як тюнінг трансформеної архітектури GPT-3.5 (text-davinci-003), що належить до родини моделей InstructGPT. Для навчання моделі з родини InstructGPT використовується підхід навчання з підкріпленням Reinforcement Learning with Human Feedback (RLHF). Попри значні успіхи ChatGPT важливо визнати, що це лише створює ілюзію розуміння [3]. Насправді ChatGPT маніпулює символами та зразками коду, які він вишукав з Інтернету, не розуміючи значення цих символів і зразків: якщо поставити чіткі та прості запитання, ChatGPT запропонує (зазвичай) чіткі та точні відповіді, але якщо поставити каверзні запитання або запитання з хибними чи негативними передумовами, результати будуть набагато менш передбачуваними. За своєю природою ChatGPT є глибокою рекурентною нейронною мережею, параметризованою матрицею вагових коефіцієнтів запитів [4].

Важливо звернути увагу на феномен «ілюзія розуміння» нейронної мережі. В чому ж механіка такого ілюзорного розуміння? Відповідь на це питання криється в суперпозиції вхідних даних перцептронів на мікрорівні та суперпозиції вагових коефіцієнтів запитів на макрорівні. Фактично, вагові коефіцієнти визначають «логіку» нейронної мережі, які змінюються в процесі навчання. Усвідомлення, що навчання відбувається за принципом зворотного розповсюдження помилки, дозволяє говорити, що в основу «логічного виводу» покладено видозмінний коефіцієнт подібності.

Саме ідея подібності між складовими алгебраїчної системи та суб'єктивний досвід у вигляді коефіцієнту з інтервалу $[-1;1]$ покладені в основу новітньої теорії «Когнітивна алгебраїчна система» [5].

Когнітивна алгебраїчна система виступає формальною моделлю когнітивної діяльності, припускаючи не тільки використання теорії моделей або формальних логік, але й всі відомі класи математичних моделей, включаючи моделі машинного навчання. В термінах [5] інтуїція розглядається як пошук найбільш схожої комбінації елементів системи, для яких відома оцінка суб'єктивного досвіду.

В якості висновку зауважимо, що запропонована в роботі [5] когнітивна алгебраїчна система не тільки дає змогу дати формальний опис феномену інтуїції обчислювальних систем, зокрема сильного штучного інтелекту, але й формальними методами дослідити властивості та закони такого явища, що й буде складати суть подальших досліджень.

- [1] Cleveland, L. (2023) Agi: Will AI achieve a level of critical reasoning and intuition that reaches or surpasses humans?, FightSaga. Available at: <https://fightsaga.com/stories/agi-will-ai-achieve-a-level-of-critical-reasoning-and-intuition-that-reaches-or-surpasses-humans/> (режим доступу: 28 квітня 2023).
- [2] Jolly, M. (2014) The concept of Intuition in Artificial Intelligence, Academia.edu. Режим доступу: https://www.academia.edu/6441833/The_Concept_of_Intuition_in_Artificial_Intelligence (дата доступу: 28 квітня 2023).
- [3] Simon, C. (2023) ChatGPT is impressive, but it may slow the emergence of AGI, TechTalks. Режим доступу: <https://bdtechtalks.com/2023/04/13/chatgpt-agi/> (дата доступу: 26 квітня 2023).
- [4] Hutanu, A. (2023) How ChatGPT works and AI, ML & NLP Fundamentals, Pentalog. Режим доступу: <https://www.pentalog.com/blog/tech-trends/chatgpt-fundamentals/> (режим доступу: 25 квітня 2023).
- [5] Кравцов, Г. (2022) Когнітивна алгебраїчна система / Кравцов Г.О., Гречко С.О., Нікітченко В.В., Примушко А.М. // Електронне моделювання, том 44, №3. - С. 14 – 30.

ПРОГНОЗУВАННЯ ТРАЕКТОРІЇ РУХОМИХ ОБ'ЄКТІВ У НЕДЕТЕРМІНОВАНОМУ СЕРЕДОВИЩІ В РЕАЛЬНОМУ ЧАСІ НА ВБУДОВАНИХ СИСТЕМАХ

Передбачення майбутніх подій у відео потоку є серйозною проблемою для комп'ютерного зору. Він вивчався в різних контекстах, включаючи прогнозування траєкторій об'єктів у невідомих середовищах, семантичне прогнозування та прогнозування шляхів. Передбачити рух деяких об'єктів особливо важко через їх динамічний характер і раптові зміни швидкості та напрямку. У роботі основна увага приділяється прогнозуванню траєкторій об'єктів за даними стереоскопічної 3D відеокамери з апаратною синхронізацією.

Існуючі дослідження щодо прогнозування траєкторії об'єкта часто використовують підхід висоти пташиного польоту, використовуючи кадри з камери, встановленої зверху. Зазвичай об'єкти зображуються у вигляді окремих точок у просторі. Хоча цей підхід ефективно моделює поведінку та взаємодію об'єктів, він нехтує такими важливими візуальними характеристиками, як параметри фізичного тіла та його індивідуальні характеристики. Попередні дослідження показали важливість цих функцій у передбаченні траєкторії, особливо в таких сценаріях, як передбачення того, чи перетне об'єкт певний шлях. Крім того, перспективи підходу, який використовує камеру зверху, не завжди доступні в практичних застосуваннях та як наслідок, останні дослідження направлені на прогнозування траєкторії з точки зору об'єктного рівня. Також одним із важливих аспектів є компактність системи відеоспостереження та обробки, що є актуальною проблемою з боку робототехніки.

У робототехніці траєкторія означає послідовність спостережень протягом певного часу. Кожна траєкторія складається з кількох спостережень, і ми прагнемо передбачити майбутні спостереження на основі минулих. Це завдання прогнозування відоме як прогнозування траєкторії. Для цього були розроблені різні методи, включаючи рекурентні нейронні мережі [1], авторегресивні моделі [2] та моделі простору станів. Ці моделі прогнозують майбутні спостереження шляхом моделювання умовного розподілу кожного спостереження з урахуванням попередніх. Однак під час прогнозування далекого майбутнього ці моделі страждають від кумулятивних помилок, оскільки прогнози повертаються в модель як додаткові вхідні дані. Це може призвести до значних помилок прогнозування, особливо в недетермінованих середовищах. Хоча ці моделі зазвичай застосовуються до таких проблем, як трафік, вони можуть не надати точних довгострокових прогнозів, заснованих виключно на минулих спостереженнях. У фізичних системах, де вимірюються всі відповідні змінні, можна очікувати більш точних довгострокових прогнозів. Наприклад, модель на основі фізики перевершує

рекурентну нейронну мережу LSTM у прогнозуванні траєкторії рухомих об'єктів. Ефект сукупної помилки очевидний у передбаченнях LSTM, оскільки вони відхиляються від реальної траєкторії.

У роботі пропонується новий метод прогнозування траєкторії, який поєднує в собі потужність глибокого навчання і умовні генеративні моделі для забезпечення підходу на основі даних для точного прогнозування траєкторії з низькою затримкою, необхідною для програм реального часу на вбудованих системах.

Це досягається за допомогою умовних варіаційних автокодерів [3], використовуючи латентну змінну z для представлення всієї траєкторії, а також мережу кодера та декодера для відображення траєкторій *до* та *від* латентного представлення z . Модель навчена максимізувати умовний логарифм правдоподібності майбутніх спостережень, враховуючи минулі спостереження, використовуючи стохастичний градієнтний спуск і репараметризацію для оптимізації [4] варіаційної цілі. Крім того, представлено стратегії, щоб зробити модель стійкою до відсутніх спостережень і викидів. Оцінка запропонованого підходу виконується в реальній системі на вбудованому мікрокомп'ютері NVIDIA Jetson Nano та стерео камери ZED2, демонструючи вищу точність прогнозування, ніж рекурентна нейронна мережа LSTM [5], при цьому досягаючи продуктивності виконання в реальному часі.

Мета роботи полягає в тому, щоб безпосередньо представити умовний розподіл та модель таким чином, щоб мати змогу фіксувати нелінійні зв'язки між минулими та майбутніми спостереженнями.

Детермінована регресія з використанням масок введення:

Для фіксованого значення t можна моделювати $p(y_{1:t} / y_{1:t-1})$ безпосередньо як задачу регресії, використовуючи складну нелінійну регресійну модель, таку як нейронна мережа. Щоб обробляти номери змінних входів t і виходів $T - t$, потрібно ввести допоміжні вхідні змінні x^t і x^t . Ці змінні представляють вхідні спостереження з доповненням нуля та маску спостереження відповідно. Використовуючи ці допоміжні змінні, можна робити прогнози з будь-якою кількістю вхідних спостережень, навіть якщо деякі спостереження відсутні.

Врахування невизначеності та мінливості:

Кількісна оцінка невизначеності прогнозованих траєкторій є важливою для прийняття рішень. Пропонується ввести латентну змінну z , щоб вловити невизначеність, яку можна відобразити на траєкторії за допомогою складної нелінійної функції, подібно до інших підходів глибоких генеративних моделей [6]. Можна припустити, що майбутні спостереження $y_{1:T}^n$ не залежать від z^n і попереднього спостереження $y_{1:t-1}^n$ і розподіляються відповідно до розподілу Гауса.

Під час передбачення обчислюється розподіл латентного простору $p(z / y_{1:t-1})$, пропускаючи задані спостереження через мережу кодера. Вибирається кілька вибірок z , і кожна вибірка разом із попередніми спостереженнями

пропускається через мережу декодера, щоб отримати вибірку майбутньої траєкторії:

$$p(y_{t:T}^n | y_{1:t-1}^n, z) = \prod_{i=t}^{T_n} N(y_i^n | \hat{y}_i^n, \Sigma_y)$$

де \hat{y}^n є оціночною траєкторією, створеною мережею декодера, а Σ_y представляє шум спостереження, отриманий з даних.

Оптимізація та процедура навчання:

Щоб оптимізувати умовну ймовірність, використовується варіаційна нижня межа умовної логарифмічної ймовірності. Цільова функція оптимізована за допомогою стохастичного градієнтного спуску та прийому перепараметризації. Навчання моделі виконується з траєкторіями різної довжини, випадковим чином вибираючи точку зрізу t для кожної траєкторії.

Архітектура мережі:

Представлений підхід можна використовувати з будь-яким методом регресії, який дозволяє обчислювати похідні. В експерименті використовуються нейронні мережі з двошаровою архітектурою та щільними зв'язками. Архітектури згорткових мереж також можуть бути ефективними для додатків прогнозування часових рядів або траєкторій.

Прогнозування за горизонтом T:

Використаний підхід передбачає фіксований горизонт прогнозування T , його можна розширити за допомогою рекурсивних ідей, щоб робити прогнози далі в майбутнє. Один із підходів полягає у використанні моделі авторегресійним способом, де передбачення моделі служать вхідними спостереженнями. Інший підхід полягає у включенні моделі простору станів або рекурентної нейронної мережі над латентною змінною z для представлення блоків спостережень. Загалом підхід забезпечує спосіб прямого представлення умовного розподілу, враховує невизначеність у прогнозах і може бути розширений, щоб робити прогнози за межами фіксованого горизонту T .

На рис. 1 було порівняно запропонований метод "TGMA" з LSTM. У моделюванні було введено білий шум Гаусса зі стандартним відхиленням 1 см, щоб імітувати середню помилку оцінки позиції системи зору. Було згенеровано більше 1000 траєкторій об'єктів для навчання та 200 для тестового набору. Результати показали, що LSTM мав трохи кращі результати для короткострокових прогнозів, але значно вищу похибку для довгострокових прогнозів аніж запропонований метод.

Точні передбачення з відносно невеликою кількістю вхідних спостережень були вирішальними для забезпечення достатнього часу реакції для системи. Запропонована модель досягла конвергенції з приблизно 40 до 50 спостереженнями, тоді як LSTM вимагала приблизно 150 спостережень для подібних рівнів помилок.

Отже, в результаті дослідження було представлено новий підхід до використання нейронних мереж для прогнозування часових рядів. Метод

включає приховану змінну, яка слідує за розподілом Гауса, яка фіксує різні можливості траєкторії. Це дозволяє генерувати зразки траєкторії на основі попередніх спостережень, уможливаючи гнучкі прогнози. Система продемонструвала здатність передбачати траєкторії об'єктів з високою варіабельністю в межах жорсткого обмеження реального часу, досягаючи затримки від 8 мс до 10 мс для визначення майбутніх траєкторій об'єктів з минулих спостережень.

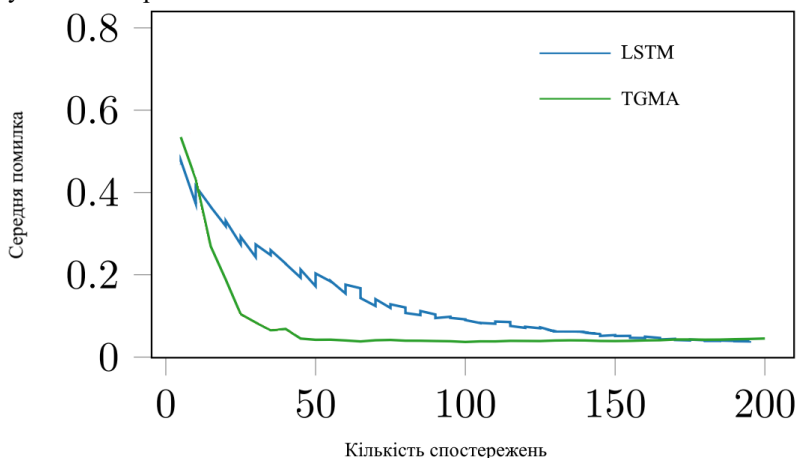


Рис. 1. Результати тестування

Крім того, розглядається суттєвий недолік популярних методів прогнозування часових рядів, таких як LSTM, який полягає в кумулятивній помилці. За допомогою емпіричного аналізу підтверджується, що запропонований підхід перевершує конкуруючі методи в довгострокових прогнозах для таких завдань, як прогнозування траєкторії об'єктів.

- [1] Aaron van den Oord, Nal Kalchbrenner, and Koray Kavukcuoglu. Pixel recurrent neural networks. arXiv preprint arXiv:1601.06759, 2016.
- [2] Anastasia Borovykh, Sander Bohte, and Cornelis W Oosterlee. Conditional time series forecasting with convolutional neural networks. arXiv preprint arXiv:1703.04691, 2017.
- [3] Kihyuk Sohn, Honglak Lee, and Xinchen Yan. Learning structured output representation using deep conditional generative models. In Advances in Neural Information Processing Systems, pages 3483–3491, 2015.
- [4] Xiaopeng Chen, Qiang Huang, Weiwei Wan, Mingliang Zhou, Zhangguo Yu, Weimin Zhang, Awais Yasin, Han Bao, and Fei Meng. A robust vision module for humanoid robotic pingpong game. International Journal of Advanced Robotic Systems, 12(4):35, 2015.
- [5] Sepp Hochreiter and Jurgen Schmidhuber. Long short-term "memory. Neural computation, 9(8):1735–1780, 1997.
- [6] Carl Doersch. Tutorial on variational autoencoders. arXiv preprint arXiv:1606.05908, 2016

В.В. Ткаченко, С.Ф. Гончар

АКТУАЛЬНІСТЬ ОЦІНЮВАННЯ РИЗИКІВ КІБЕРБЕЗПЕКИ ПРИ КАСКАДНИХ АВАРІЯХ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Події останніх років в Україні і у світі показали нагальну необхідність забезпечення кібербезпеки інформаційних систем об'єктів критичної інфраструктури, особливо енергетичного сектору [1, 2].

Як зазначається в [3], при аналізі ризику можуть використовуватися наступні умови чи припущення: втрати від ризику не залежать один від одного; втрати по одному з деякого переліку ризиків не обов'язково збільшують ймовірність втрат по іншим; максимально можливий збиток не повинен перевищувати фінансових можливостей учасників проекту.

Разом з тим, втрати від ризиків можуть залежати один від одного, з каскадним розвитком аварії. При цьому, такі ризики являють собою загрозу і становлять небезпеку для об'єктів критичної інфраструктури. В [4] зазначається, що під каскадним розвитком аварії, або ефектом доміно, мається на увазі процес впливу вражаючих факторів початкової (ініціюючої) події на сусіднє обладнання, що призводить до появи інших руйнівних подій, наслідки яких можуть бути важчими, ніж викликані тільки однією ініціюючою подією. Подібні аварії можуть призвести до серйозних техногенних катастроф на об'єктах критичної інфраструктури, які характеризуються високою енергоємністю і щільністю розміщення технологічного обладнання. У роботах [4 та ін.] приводяться приклади виникнення каскадних аварій на критичної інфраструктури, особливо енергетичного сектору, зокрема, на АЕС "Фукусіма-1", на заводах з виробництва зрідженого природного газу в Монреалі (Канада), в місті Бонтанг (Індонезія), в Алжирі.

Дослідження показують, що каскадні аварії можуть призвести до катастрофічних наслідків на об'єктах критичної інфраструктури, із заподіянням великого збитку, у тому числі екологічного. Даний факт показує може слугувати підставою для обов'язкової жорсткої регламентації заходів, спрямованих на запобігання подібного розвитку подій, а розробка методів оцінювання ризиків виникнення таких аварій являється актуальною задачею.

- [1] Гончар С.Ф. Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури. Монографія. Київ, 2019, 176 с.
- [2] Гончар С.Ф. Дослідження проблем кіберживучості об'єктів критичної інформаційної інфраструктури / Гончар С.Ф., Комаров М.Ю., Дмитрієва Д.О. // Ядерна та радіаційна безпека. – 2021. – №1(89). – С.59-66.
- [3] Дубров А.М. Моделювання ризикових ситуацій в економіці і бізнесі: Навч. посібник/А.М. Дубров, Б.А. Лагоша, Е.Ю. Хрусталеv; Під ред. Б.А. Лагоші.- М.: Фінанси і статистика, 2000.— 176 с.: іл. ISBN 5-279-02068-0.
- [4] Белов П.Г. Управління ризиками, системний аналіз і моделювання: навчальний посібник і практикум. Видавництво Юрайт, 2016. - 272 с.

АНАЛІЗ РОЛІ ЛЮДСЬКОГО ЧИННИКА НА СТАН ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ АСУ ТП

На сьогоднішній день, деякі автори [1] висловлюють думку, що на даний час все більше зростає роль людського чинника на стан забезпечення кібербезпеки автоматизованих систем управління технологічним процесом (далі – АСУ ТП) при недостатній кількості методів і засобів його оцінки та захисту. Засоби і методи, які наразі розробляються дають змогу зменшити рівень помилкової інформації, але не досліджують проблему у цілому, в тому числі не проводять оцінку і захист, як від випадкових, так і від умисних деструктивних дій обслуговуючого персоналу.

При цьому, людський чинник являється одночасно і необхідним елементом людино-машинних систем управління і джерелом загроз кібербезпеці таких систем, рис. 1 [2].



Рис. 1.

В складних людино-машинних системах управління персоналу доводиться приймати ті чи інші рішення. При цьому, на адекватність прийнятих рішень персоналом в таких системах можуть впливати такі фактори [3, 4]: зовнішні та внутрішні дестабілізуючі впливи, нестійкість рішення при великій кількості альтернатив, тривалість часового інтервалу для прийняття рішення.

Враховуючи викладене, можна зазначити, що важливою задачею являється прийняття адекватних рішень обслуговуючим персоналом в різних інформаційних середовищах і відносинах. Для цього актуальною задачею є розроблення моделі імовірних деструктивних дій персоналу АСУ ТП в умовах наявності дестабілізуючих впливів в аспекті кібербезпеки.

- [1] Ємелін В.І. Методи і моделі оцінки та забезпечення інформаційної безпеки автоматизованих систем управління критичними системами: дис. доктора техн. наук : 05.13.19 / Ємелін Вадим Іванович. – 2012. – 238 с.
- [2] Гончар С.Ф. Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури. Монографія. Київ: «Альфа реклама», 2019, 176 с.
- [3] Henshel D., Cains M.G., Hofmann B., Kelley T. Trust as a human factor in holistic cyber security risk assessment. *Procedia Manufacturing*. 2015. № 3. 2015. P.1117-1124.
- [4] Takayuki H., Tetsou S. Extended FRAM model based on cellular automaton to clarify complexity of socio-technical systems and improve their safety. *Safety Science*. 2020. № 123. P.2-16.

ПЕРСПЕКТИВИ РОЗВИТКУ АТОМНОЇ ЕНЕРГЕТИКИ РІЗНИХ КРАЇН СВІТУ

Нині у світі працює 440 атомних реакторів у 32 країнах. Ще 50 знаходяться на стадії будівництва, переважно в Азії. Однак МАГАТЕ не дає однозначних прогнозів щодо майбутньої ролі атомних станцій у виробництві електроенергії у світі. Вона залежить значною мірою від того, чи вдасться побудувати нові потужності на заміну станціям, які будуть виводити з експлуатації. Більш ніж половина активних реакторів у світі працює вже понад 30 років. Сьогодні на атомну енергетику припадає 10% світового виробництва електроенергії. За низьким прогнозом МАГАТЕ до 2050 року ця частка скоротиться до 6%, водночас за високим прогнозом частка атомної електроенергії зросте до 12% [3].

В ядерної енергетики є дві переваги перед іншими джерелами. По-перше вона може забезпечувати теплом виробничі процеси та проводити дешево і надійну електроенергію без виділення парникових газів. По-друге ядерна енергетика на сьогодні дозволяє уникнути викиду 200 мільйонів тон CO₂ на рік, що рівносильно видалення 400 мільйонів автомобілів з усіх доріг світу [4]. Наразі атомна енергетика знову в тренді, розглянемо як змінилися погляди різних країн світу на атомну енергетику. Матеріали для аналізу взято з відкритих джерел інформації: наукові публікації, сайти міжнародних організацій, аналітичні та звітні матеріали та ін. результати проведеного аналізу було згруповано за континентами та країнами.

Європа.

ЄС поки не може остаточно визначитися із статусом ядерної енергетики. Триває дискусія щодо включення атомної енергетики до «зеленої» таксономії. Таксономія – це список екологічно чистих видів діяльності. Він потрібен Євросоюзу, щоб показати «корисні» компанії та стимулювати інвесторів фінансувати саме їх. Компанії з таким маркером залучатимуть більше кредитів та підтримуватимуться владою ЄС. У 2020 р. вчені з Єврокомісії визнали АЕС безпечним низьковуглецевим джерелом енергії, проте у 2021 р. комісія відмовилася включати АЕС до «зеленої» таксономії через проблему з утилізацією ядерних відходів. Однак енергетична криза, яка сталася у ЄС, загострила цю дискусію. Водночас 12 країн союзу закликали Єврокомісію визнати атомну енергію «зеленою» [5].

Енергетика **Польщі** більше ніж на половину залежить від вугілля, тому там також шукають стабільну альтернативу для зменшення кількості викидів вуглецю.

Німеччина після аварії на Фукусімі прийняла рішення вивести з експлуатації свої АЕС. Наразі в роботі ще залишаються сім реакторів, які забезпечують 12% електроенергії Німеччини. Поряд з цим відновлювана енергетика в країні успішно розвивається [3].

Іспанія поступово зменшує частку атомної енергетики. працюючих залишається сім реакторів, які постачають близько 20% електроенергії. За державною вказівкою всі реактори повинні бути відключені між 2025 та 2035 роком. Заплановано замінити станціями з відновлювальними джерелами енергії, однак це може вплинути на терміни реалізації запланованих відключень [3].

Франція є неформальним лідером ядерної енергетики світу. Уряд країни найбільше зацікавлений в утвердженні ядерної енергетики, оскільки є лідером у її виробництві. У Франції працює 56 ядерних реакторів, які забезпечують понад 70% її потреб в електроенергії. Також країна є найбільшим у світі експортером ядерної енергетики. Вона також допомагає будувати ядерні реактори в усьому світі. Водночас, 12 реакторів, строк експлуатації яких завершується, планують вимкнути. Поряд з цим відбувається будівництво нового енергоблоку на АЕС «Фламанвіль». Це буде перший в країні EPR – водно-водяний ядерний реактор третього покоління на 1650 МВт. Затримка будівництва склала вже десять років, очікується, що Фламанвіль-3 буде запущено у 2023 р. [3], [4].

Словаччина є країною, яка буде нові атомні потужності в Європі. Наразі чотири реактори забезпечують половину електроенергії в країні, і ще два знаходяться на стадії будівництва. Ситуація з двома новими реакторами на АЕС в Моховце демонструє загальну проблему спорудження АЕС. Відкриття 2019 р. було відкладено через тиск сусідньої Австрії та перестороги стосовно безпеки енергоблоків, які початково будувалися за радянським дизайном та були модифіковані з використанням «західних» елементів [3].

Великобританія посідає десяте місце у світі по виробництву ядерної енергії. Electricite de France SA (EDF) почала будівництво заводу Hinkley Point C в Сомерсеті у 2016 році та, як очікується, запустить його в середині цього десятиліття. Очікується, що Hinkley Point C буде поставляти близько 7% електроенергії Великобританії, коли вона буде підключена до мережі. Наразі здійснюється планування електростанції MW Sizewell C потужністю 3200 МВт в східній Англії, яку EDF також планує побудувати в партнерстві з China General Nuclear Power Group [4].

Північна Америка.

У **США** активно функціонує 95 реактори, які забезпечують 30% світової атомної електроенергії та залишається її найбільшим виробником. Для потреб країни АЕС генерують близько 20% електроенергії. За період з 1978 р. по 2013 р. жодної нової АЕС не було закладено. Лише у 2012-му, вперше за 30 років, були видані дозволи на будівництво двох нових реакторів на АЕС Vogtle у Джорджії. Нові проекти почали з'являтися з 2016 р., коли відбулося відкриття другого енергоблоку АЕС Watts Bar в Теннесі. Значні затримки та зростання вартості будівництва зумовили закриття у 2017 р. двох реакторів станції V.C. Summer в Південній Кароліні [3]. Наразі розвиток АЕС для США – це частина боротьби з кліматичними змінами. Уряд на підтримку галузі ядерної енергетики у 2022 р. передав 1,85 млрд дол., що на 23% більше, ніж у

2021 р. Ще 6 млрд дол. підуть на продовження терміну служби АЕС і 2,5 млрд дол. – на будівництво експериментальних реакторів [5]. Президент Байден висловився за підтримку ядерної енергетики та наголосив на розширенні робочих місць та можливостях, які будуть створені за через розвиток інновацій та інвестицій в новітні малі модульні реактори [4].

Азія та Близький Схід.

Китай планує значне зростання частки атомної генерації в енергосистемі з 3% до 7,7% у 2035 р. У країні працює 49 реакторів і ще 16 перебувають на стадії будівництва. Перевагу атомній енергетиці в країні надають через надмірне забруднення повітря вугільними електростанціями. Крім збільшення кількості станцій та їхньої потужності, Китай розробляє та планує впроваджувати нові типи реакторів. До прикладу, перший SMR може почати роботу на острові Хайнань вже у 2025 р. [3]. Китай готовий побудувати велику кількість АЕС на власній території, а також 30 реакторів за кордоном, склавши конкуренцію на цьому ринку Франції та США [5]. Президент Китаю у 2021 року безпосередньо був присутній на церемонії закладки фундаменту чотирьох нових атомних енергоблоків у КНР. Енергоблоки 7 і 8 Тяньванської АЕС, а також 3 і 4 енергоблоки станції Худару будуть побудовані з використанням вітчизняного обладнання [4].

Південна Корея оголосила про плани виходу з ядерної енергетики до 2040 р., термін експлуатації АЕС не буде продовжений, і нові об'єкти не будуть побудовані [4].

Японія розглядає ядерну енергетику як ключ до досягнення цілей декарбонізації та скорочення викидів парникових газів. Японія також розглядає можливість використання існуючої ядерної енергетики, запроваджуючи в експлуатацію невеликі модульні реактори, це окреслено у Стратегії зеленого зростання країни [4].

Уряд **Індії** планує за три роки планують запустити дев'ять реакторів. Будівництво ще 12 затвердили у 2020 р. У країні вперше будують АЕС з таким розмахом [5]. Заплановано збільшувати кількість АЕС в Індії у межах масштабних програм з розвитку інфраструктури. Зараз в країні працює 23 реактори. До 2031 р. може бути закладено 21 новий реактор, загальною потужністю у 15 ГВт [4].

Об'єднані Арабські Емірати у 2020 р. запустили першу АЕС «Барака». Планується, що всі чотири енергоблоки станції, загальною потужністю в 5,6 ГВт, будуть працювати вже у 2023 р. та забезпечать до 25% потреб країни в електроенергії [4].

Туреччина буде свою першу АЕС «Аккую». Одна з причин – бажання зменшити енергетичну залежність, адже країна імпортує близько 75% електроенергії. Станція матиме чотири енергоблоки, загальною потужністю в 4,8 ГВт. Її перший реактор планують запустити у 2023 р. [4].

Отже, із проаналізованого вище констатуємо, що Китай та Індія стали лідерами з розвитку галузі атомної енергетики. На підставі аналізу наукової літератури [1], [2], [3], [4] окреслено основні проблеми розвитку ядерної енергетики у світі, а саме:

– зменшення конкурентоздатності атомної енергетики і дострокова зупинка енергоблоків;

– перевищення строків та вартості будівництва нових АЕС;

– старіння діючих енергоблоків і необхідність виведення з експлуатації;

– негативне ставлення суспільства на фоні Фукусімської та інших ядерних аварій;

– відмінність у ліцензування проєктів ядерних реакторів;

– необхідність вирішення проблеми з відпрацьованим ядерним паливом та радіоактивними відходами;

– недієздатність енергоринків для залучення довгострокових інвестицій.

Погоджуємося з вказаним, у публікації [3], про те, що питання безпеки сьогодні залишається чи не найбільш вагомим причиною відмови від будівництва нових АЕС. Воно поставало щоразу жорсткіше після аварій на станції у Чорнобилі та Фукусімі. У 2011 р. активізувалися антиядерні протести особливо у Європі, де станції часто розташовуються поблизу кордонів із сусідніми країнами. Наступною проблемою є складний процес спорудження АЕС, що часто затягується та зупиняється, спричиняючи зростання вартості енергоблоків. Також, актуальним залишається питання поводження з ядерними відходами. Водночас окремі країни вбачають в атомній енергетиці можливість диверсифікувати джерела енергії, зменшення залежності від інших енергоносіїв та заміну вугільним електростанціям [3].

Отже, підсумовуючи вищесказане, до світових трендів розвитку ядерної енергетики можна віднести:

– продовження термінів експлуатації атомних енергоблоків;

– розвиток ядерної енергетики у контексті Паризької угоди;

– розвиток атомно-водневої енергетики;

– синергетична взаємодія відновлювальних джерел енергії та АЕС;

– впровадження нових реакторних технологій.

[1] Zhou, X.: Improvement of the methodology for calculating a once-through steam generator for low-power NPP. Odessa Polytechnic State University, Odessa (2021)

[2] Kilnytskyi O. Energy trends: which projects should be invested in. The landscape of the Ukrainian electricity market will change much faster than many people think. 2018. <https://mind.ua/publications/20190743-energetichni-trendi-v-yaki-proekti-varto-investuvati-koshti>

[3] Lutska V. To close reactors or to build new ones: trends in the development of atomic energy in the world. While Germany is completely abandoning nuclear power plants, China is building a dozen new reactors. 2021. <https://hmarochos.kiev.ua/2021/02/04/zakryvaty-reaktory-chy-buduvaty-novi-tendentsiyi-rozvytku-atomnoyi-energetyky-u-sviti/>

[4] Didenko S. Nuclear power: world trends and Ukrainian realities in the conditions of climate change. 2021. <https://ua.news.ua/money/atomnaya-energetyka-myrovyetendentsyy-y-ukraynskye-realy-y-v-uslovyah-klymatycheskyh-ymenenyj>

[5] Miroshnychenko B. Between "green" and Fukushima: is there a future in nuclear energy. 2021. <https://www.epravda.com.ua/publications/2021/12/13/680582/>

О.О. Попов, С.І. Скуратівський, А.О. Запорожець, О.В. Фаррахов,
Є.В. Пилипчук, В.О. Куценко, І.Д. Мартинюк, Є.Б. Краснов, О.М. Коваленко

ПРО РОЗВ'ЯЗАННЯ ЗАДАЧІ ВИЗНАЧЕННЯ ЩІЛЬНОСТІ РОЗПОДІЛУ РАДІАЦІЙНОГО ЗАБРУДНЕННЯ ТЕРИТОРІЇ ЗА ДАНИМИ ДИСТАНЦІЙНОГО МОНІТОРИНГУ

Разом із широким використанням радіоактивних матеріалів в енергетичних, військовій, дослідницькій сферах, з розвитком видобувної галузі загострилась і потреба моніторингу радіаційного стану навколишнього середовища, робочих систем та забезпечення потрібного рівня безпеки. Швидким, достатньо інформативним та безпечним способом моніторингу радіаційних γ -полів є дистанційний метод, що ґрунтується на використанні засобів БПЛА. Значна кількість переваг які надає така технологія [1] суттєво розширила межі використання БПЛА у дистанційних дослідженнях радіаційних полів, однак усе ще є необхідність у покращенні якості аналізу інформації, зібраною детекторами БПЛА. Як показують проведені дослідження [1, 2], для розв'язання такої проблеми використовуються математичні методи, зокрема розв'язки оберненої задачі для ідентифікації дублетних та подібних їм структур (близько розташовані траншеї, загублені могильники, випадкові сильно радіоактивні джерела тощо) [2]. Зазначена задача являє собою інтегральне співвідношення для оцінки детектором БПЛА кількості гамма-квантів, які випромінюються з поверхні ґрунту та захоплюються на висоті польоту БПЛА. У дослідженнях використовувались синтезовані за відомим поверхневим розподілом джерел гамма-випромінювання σ дані детектора W , отримані як розв'язки прямої задачі

$$\Lambda \int_{t_{i-1}}^{t_i} dt \int_{\Omega} \sigma(X) \frac{e^{-\mu r}}{4\pi r^3} (h^d - h) d\Omega = W_i,$$

де $X = (x, y) \in R^2$ – точка в області Ω яка містить джерела гамма випромінювання; μ – коефіцієнт затухання гамма-променів у повітрі; Λ – масштабний коефіцієнт, що залежить від геометричних та фізичних властивостей детектора; $r = \sqrt{(h^d - h)^2 + (x^d - x)^2 + (y^d - y)^2}$, $(x^d; y^d; h^d)$ – координати детектора, $h = h(x, y)$ – профіль поверхні ґрунту.

Наступний крок – відновлення поверхневого розподілу за відомим даними детектора є оберненою задачею, розв'язання якої здійснювалось за алгоритмом Ландвебера.

Зазначена процедура являє собою ітераційний процес, що здійснюється за наступною формулою

$$(g_{\alpha})_{v+1} = (g_{\alpha})_v - \eta \cdot \text{grad } J((g_{\alpha})_v), \quad v = 0, 1, \dots$$

де $J = \frac{1}{2} \|K \cdot g - w\|^2$, $\text{grad } J = K^T \cdot (K \cdot g - w)$, параметр η – скаляр, що визначає швидкість збіжності ітераційного процесу.

Варто зазначити, що процедуру Ландвебера можна записати у формі матричного співвідношення виду

$$(g_\alpha)_v = \eta \sum_{j=0}^{v-1} (I - \eta K^T K)^j K^T \cdot w,$$

що спрощує використання алгоритму у прикладних задачах. Зокрема, вказані математичні процедури було реалізовано засобами системи Mathematica, результати роботи яких зображено на Рис.1.

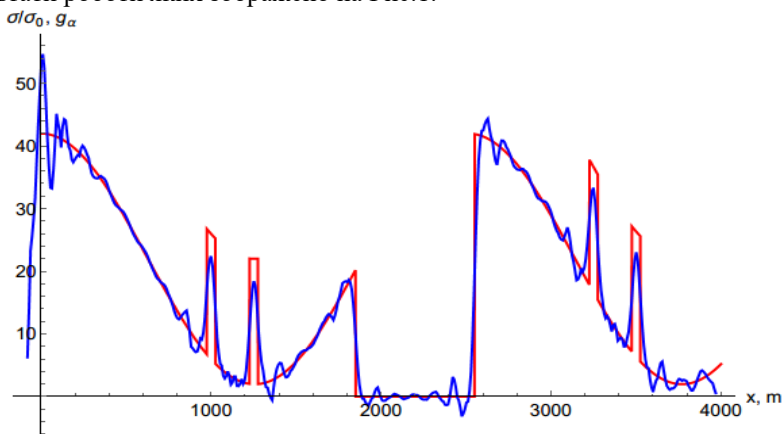


Рис.1. Порівняння теоретичного профілю функції σ (суцільна регулярна крива) та відновленого профілю σ (нерегулярна крива), відновленого за алгоритмом Ландвебера. Параметр $\eta = 0.4$.

З аналізу Рис.1. випливає, що застосування алгоритму Ландвебера в оберненій задачі дозволяє достатньо якісно відтворити складний профіль поверхневого розподілу та впевнено ідентифікувати дублетні структури. Проведені дослідження є перспективними у використанні їх при аналізі реальних показів детектора.

- [1] Popov O. et al. Features of the Modern UAV-Based Complexes Use to Solve Radiation Control Problems. In: Zaporozhets A., Popov O. (eds) Systems, Decision and Control in Energy IV. Studies in Systems, Decision and Control. 2023. Vol. 456. P. 35-57. https://doi.org/10.1007/978-3-031-22500-0_3
- [2] Zabulonov Y et al. Remote Gamma Ray Mapping of Ground Surface: Mathematical Issues. In: Zaporozhets A., Popov O. (eds) Systems, Decision and Control in Energy IV. Studies in Systems, Decision and Control. 2023. Vol. 456. P. 173-184. https://doi.org/10.1007/978-3-031-22500-0_11

АНАЛІЗ ІСНУЮЧОГО ДОСВІДУ ПРИ ЗБЕРІГАННІ ВИСОКОАКТИВНИХ ВІДХОДІВ, ЩО МІСТЯТЬ ЯДЕРНІ МАТЕРІАЛИ

Усі промислові процеси призводять до утворення відходів, які в подальшому потребують безпечного поводження зберігання та захоронення. В результаті експлуатації ядерних реакторів, а також пов'язаних з ними паливних циклів (видобуток урану, збагачення, виготовлення, використання та переробка палива) та іншої діяльності утворюються радіоактивні відходи (РАВ) різної форми, активності, періодом напіврозпаду. Це означає, що всі держави, які займаються будь-яким видом використання ядерної енергії, повинні розглянути питання забезпечення безпечного поводження з радіоактивними відходами, відповідно до національних норм, які часто базуються на стандартах безпеки МАГАТЕ [3], [5] або узгоджуються з ними.

Оскільки вміст радіоактивності в різних типах радіоактивних відходів сильно варіюється, відходи можуть бути віднесені до класів дуже низькоактивних, низькоактивних, середньоактивних та високоактивних відходів [1]. При цьому кожна країна в рамках національних програм має свою класифікацію РАВ і відповідно до їх небезпеки та наявних або запланованих шляхів поводження з ними.

В природі існують такі радіоактивні матеріали, що мають настільки низький вміст радіонуклідів, що радіологічний на навколишнє середовище вплив є незначним, і вони можуть бути звільнені від регулюючого контролю відповідно до державних нормативних документів. На рисунку 1 показаний розподіл всіх РАВ, які зберігаються або захороненні станом на 2016 рік.

Але й існують клас відходів, що не попадає під класифікацію та концепцію захоронення. Ці відходи утворилися внаслідок ядерних аварій на установках з утворенням критичної маси і виникненню невідтворюючої ланцюгової реакції, які отримали назву - відходи, що підлягають збереженню. Тобто, це ядерний матеріал, отриманий в результаті обробки чи технологічної аварії, що вважається на даний момент таким, що не регенерується, але підлягає збереженню. Це формулювання визначає ядерний матеріал, що розглядається як відходи, що підлягають збереженню; зміни інвентарної кількості матеріалу в інвентарних записих і звітах визначаються як «переведений у відходи, що підлягають збереженню».

Тобто, чим вища небезпека, тим більш розробленою та/або глибшою є концепція захоронення відходів. Залежно від національної політики, декілька категорій відходів іноді об'єднуються разом з метою поводження з ними на одному об'єкті. У цьому випадку об'єкт повинен бути спроектований з урахуванням безпеки для найвищого класу відходів, які на ньому розміщуються.

Тому перш ніж вибрати стратегію поводження з високоактивними відходами (ВАВ), важливо знати та розуміти джерело утворення ВАВ. В Україні та світі розрізняють ВАВ по таких групах:

- ВАВ, що утворилися в наслідок експлуатації та зняття з експлуатації АЕС;
- ВАВ, що утворилися в наслідок переробки відпрацьованого ядерного палива;
- ВАВ, що утворилися в наслідок аварії на АЕС.

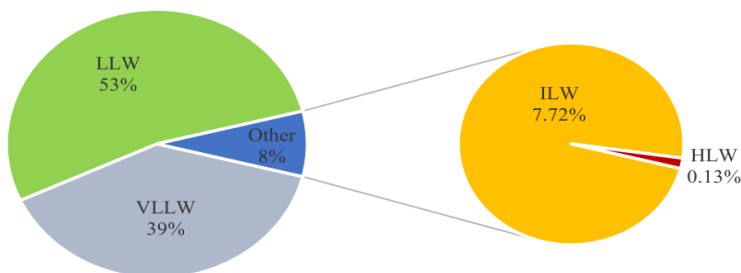


Рисунок 1. Розподіл різних класів РАВ, які зберігаються або захороненні станом на 2016 рік

За обсягом ВАВ утворюють менше 0,5% світового обсягу радіоактивних відходів, але вони складають близько 95% загальної активності радіоактивних відходів.

У країнах Європи, ВАВ, утворені в процесі експлуатації АЕС і зняття АЕС з експлуатації, зберігаються, головним чином, у сховищах, що на майданчиках АЕС або в централізованих сховищах.

При цьому, найкращою стратегією поводження з усіма радіоактивними відходами є їхня локалізація (тобто обмеження радіонуклідів в межах матриці відходів, упаковки та сховища для захоронення) та ізоляція від населення, та навколишнього середовища [2]. В основному, для захоронення відходів використовуються пасивні, інженерні і природні засоби наскільки це необхідно з огляду на пов'язану з ними небезпеку. Розміщення РАВ в ретельно спроектованих спорудах, заглиблених у відповідні геологічні формації, забезпечує довгострокову стабільність, характерну для стабільного геологічного середовища [6], [7].

Розрізняють два способи захоронення відходів: для середньо і низькоактивних РАВ можливе захоронення в приповерхневих сховищах з різним ступенем ізоляції, коли ВАВ з рівнями активності, достатньо високими для того, щоб генерувати значну кількість тепла в процесі радіоактивного розпаду, або відходи з великими кількостями довгоживучих радіонуклідів, як правило, необхідне захоронення в глибоких стабільних

геологічних формаціях. Також такому захороненню підлягає відпрацьоване ядерне паливо (ВЯП) та відскловані ВАВ після переробки ВЯП.

В теперішній час єдине глибоке геологічне сховище, що має ліцензію на захоронення – це сховище WIPP (Waste Isolation Pilot Plant) у Сполучених Штатах Америки (рисунок 2). Метою його будівництва було захоронення відходів військової промисловості.

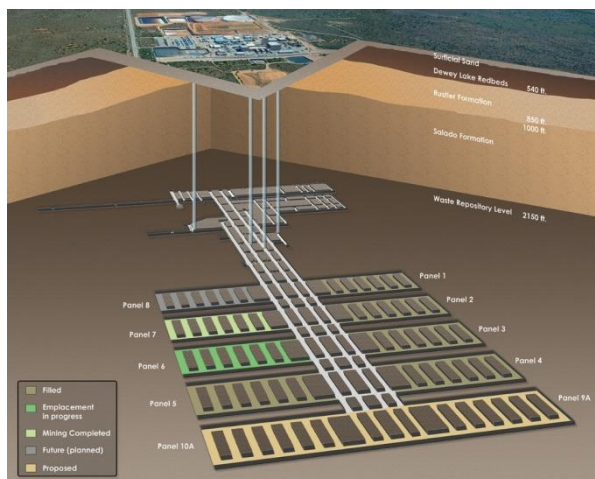


Рисунок 2. Сховище Waste Isolation Pilot Plant (США)

Компанія Posiva Oy у Фінляндії отримала ліцензію на будівництво від свого регуляторного органу у 2015 році, і будівництво триває. Заявка на отримання ліцензії на експлуатацію була подана у 2020 році. Остаточне захоронення планується розпочати у 2020-х роках. Дане сховище знаходиться на глибині близько 660 м і передбачає захоронення 175 тис. м³ відходів [9]. На рисунку 3 наведено приклад контейнерів для відпрацьованого ядерного палива, які будуть використовуватися у Фінляндії (рисунок 4).

Даний метод утилізації складається з наступних етапів (рисунок 5):

- Відходи зберігаються в проміжному сховищі протягом 30 років.
- Відходи капсулюють у чавунні каністри.
- Чавунні каністри інкапсульовані в мідні (сплав CuOFP) капсули.
- Капсули розміщуються в шарі бентонітової глини в круглому отворі глибиною вісім метрів і діаметром два метри, пробуреному в тунелі глибиною 500 метрів у кристалічній породі.

На рисунку 1.4 показана загальна схема сховища, що будується у Фінляндії, проект якого був розроблений компанією SKB.

Сховища таких типів зможе захоронити близько 6000 капсул з ВЯП та ВАВ, а приймати 200 капсул на рік.

У 2011 році SKB подала заявку на будівництво сховища відпрацьованого ядерного палива до регулюючих органів Швеції, а у 2019 році SKB подала документацію, необхідну для прийняття рішення урядом.



Рисунок 3. Приклад контейнерів KBS-3

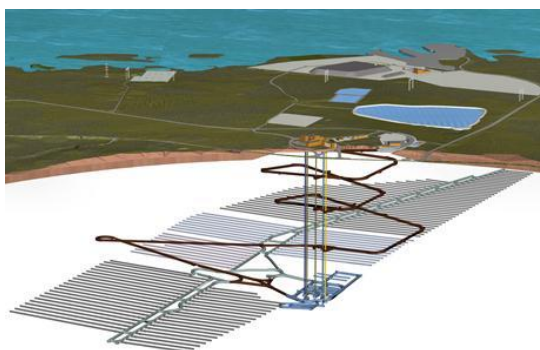


Рисунок 4. Схема глибокого геологічного сховища Olkiluoto (Фінляндія)

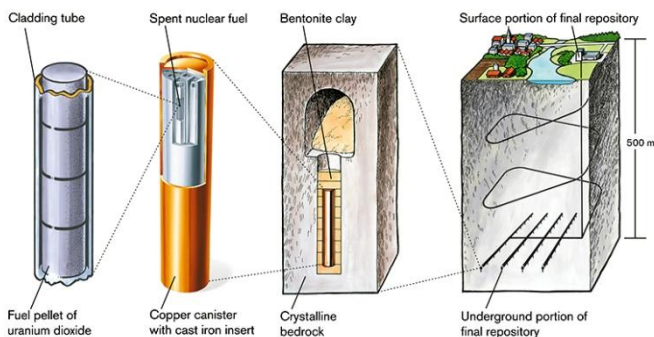


Рисунок 5. Схема захоронення ВАВ та ВЯП методом KBS-3

У Франції триває процес проектування Cigéo (промислового центру геологічного захоронення), а подання заявки на отримання ліцензії до регулюючого органу очікується у 2020 році. У деяких інших країнах, таких як Канада, Німеччина та Великобританія, тривають офіційні процеси вибору майданчиків [8]. У країнах, де захороненню підлягають як відпрацьоване ядерне паливо, так і ВАВ, типовим підходом є єдиний пункт захоронення радіоактивних відходів для обох матеріалів. Більшість інших країн, що мають відпрацьоване ядерне паливо, працюють над національними рішеннями, хоча вони в основному знаходяться на ранній стадії планування. Деякі країни також виявили зацікавленість у створенні багатонаціональних сховищ для захоронення на додаток до власної національної програми.

Важливу роль в поводженні з РАВ є їхнє зберігання. Практично завжди перед остаточним захороненням ВЯП та ВАВ потребує тимчасове зберігання (до 30 років) або довготривале зберігання (до 100 років). Вибір зберігання відходів залежить від стратегії поводження з відходами, природними показниками, соціальними та економічними факторами і інше для кожної країни [4].

Зберігання передбачає розміщення РАВ в придатному місці з можливим наступним вилучення. При цьому захоронення відходів, навпаки, призначення для розміщення відходів без наміру їхнього вилучення в майбутньому.

На тип сховища переважно впливають характеристики відходів, що повинні в ньому зберігатися. Існує два різних етапи зберігання під час поводження з РАВ: буферне зберігання не перероблених відходів і проміжне зберігання кондиціонованих відходів.

Цілі цих фаз зберігання можна сформулювати так [4]:

- експлуатаційне зберігання (наприклад, зберігання відходів в очікуванні кондиціонування або транспортування);
- безпечна витримка протягом періоду радіоактивного розпаду перед наступними етапами поводження з відходами;
- проміжне зберігання кондиціонованих відходів (наприклад, безпечне утримання відходів до створення остаточних сховищ або початку кампанії із захоронення).

Більшість сховищ являють собою інженерні споруди, у виняткових випадках також використовується зберігання на спеціально виділеному майданчику. Зберігання на майданчику характеризується зберіганням упаковок на підготовленому майданчику на відкритому повітрі або, можливо, у простих відкритих або перекритих для захисту від несприятливих придатних умов ангарів.

Інженерне сховище визначає зберігання ВАВ в спеціально побудованих спорудах, таких як приміщення, будівлі та бункери. Дані інженерні сховища можуть створюватися з різним ступенем складності систем вентиляції, відведення тепла, контролю за температурою та активністю залежно від національних нормативних вимог і відповідно до фізичних і хімічних властивостей ВАВ, активності та потужності дози упаковок з відходами. У

сховищі можуть використовуватися пристрої дистанційного управління, такі як мостові крани або обладнання прямого управління, а також обладнання для моніторингу активності, протипожежні системи тощо.

- [1] International Atomic Energy Agency, Classification of Radioactive Waste, IAEA Safety Standards Series No. GSG-1, IAEA, Vienna (2009)
- [2] International Atomic Energy Agency, Disposal of Radioactive Waste, IAEA Safety Standards Series No. SSR-5, IAEA, Vienna (2011)
- [3] International Atomic Energy Agency, Methodology for Safety Assessment Applied to Predisposal Waste Management, IAEA-TECDOC-1777, IAEA, Vienna (2015)
- [4] International Atomic Energy Agency, Nuclear Power Reactors in the World, Reference Data Series No. 2, IAEA, Vienna (2022)
<https://www.iaea.org/publications/15211/nuclear-power-reactors-in-the-world>
- [5] International Atomic Energy Agency, Safety of Radioactive Waste Disposal, Proceedings Series - International Atomic Energy Agency, IAEA, Vienna (2006)
- [6] International Atomic Energy Agency, Scientific and Technical Basis for the Geological Disposal of Radioactive Wastes, IAEA Technical Reports Series No. 413, IAEA, Vienna (2003)
- [7] National Research Council, Disposition of High-Level Waste and Spent Nuclear Fuel: The Continuing Societal and Technical Challenges, The National Academies Press, Washington, DC (2001)
- [8] Oecd Nuclear Energy Agency, Int. Conf. on Geological Repositories 2016. Conf. Synthesis 7–9 December 2016, NEA No. 7345, OECD, Paris (2017)
- [9] Witherspoon P.A., Bodvarsson G.S. (eds.). Geological Challenges in Radioactive Waste Isolation. Fourth Worldwide Review. Report. (LBNL, 2006)

ПРО ПІДХІД ДО СТВОРЕННЯ Gd-ВМІСНИХ НАНОКОМПЗИТИВ НА ОСНОВІ КОНЦЕПЦІЇ «SAFE BY DESIGN» ДЛЯ ЗАХИСТУ ВІД НЕЙТРОННОГО ВИПРОМІНЮВАННЯ РІЗНИХ ДЖЕРЕЛ

Нейтронне випромінювання завдяки великій проникній здатності широко використовується в різних народному господарства. З іншої сторони, воно є одним з найнебезпечніших видів опромінення. Його вплив на біологічну тканину призводить до іонізації матеріалу та, як наслідок, суттєвих змін функціональності клітин організму або втрати здатності до відновлення. Також можуть утворюватися інші хімічні елементи, в т.ч. радіонукліди, що породжує в організмі наведену радіоактивність. Ця ж проблема є актуальною і для ядерних установок, оскільки через нейтронне опромінення обладнання стає радіоактивним, тобто непридатним до використання.

Для захисту від нейтронного випромінювання різних джерел використовуються екрануючі конструкції та матеріали на основі хімічних елементів, які мають властивість поглинати потік нейтронів. Такими хімічними елементами є бор, гадоліній, берилій, кадмій, графіт та інші. Серед них гадоліній (Gd) має найвищий переріз захоплення нейтронів серед усіх стабільних нуклідів, і завдяки цьому, матеріали з вмістом Gd є одними з найбільш ефективних при поглинанні нейтронного випромінювання [1].

Однак, сучасні тенденції у боротьбі зі зміною клімату вимагають використання в галузях народного господарства безпечних речовин та екологічно чистих матеріалів, або таких, що здійснюють мінімальний вплив на навколишнє природне середовище. Розроблення Gd-вмісних нанокompозитних матеріалів на основі біополімерів дозволить реалізувати концепцію «safe by design», яка полягає в тому, що на кожній стадії розроблення/вдосконалення матеріалу (продукту) обираються найбільш безпечні для людини та навколишнього середовища речовини (реагенти).

На сьогоднішній день практично відсутні публікації щодо розробок та створення екологічно-безпечних композитних матеріалів на основі природних біополімерів та гадолінію. Тому, актуальною науково-практичною проблемою є створення нових екологічно безпечних Gd-вмісних нанокompозитних матеріалів, які відповідатимуть сучасним вимогам безпеки (біосумісності, низької токсичності), що дозволить використовувати їх не тільки на об'єктах ядерно-промислового комплексу для захисту персоналу та обладнання, а також і у біомедичних цілях (наприклад в якості гнучких прозорих пов'язок, трансдермальних пластирів тощо).

Нейтрон-захисні композитні матеріали діють в складі певних об'єктів як компоненти захисних споруд. Зокрема, нейтрон-захисні композити, для виконання своєї функції можуть виступати компонентами покриттів, ізоляційних, захисних та конструкційних матеріалів тощо. Відповідним чином, під час експлуатації матеріалів, що містять нейтрон-захисні

композити, важливо враховувати вплив на них різноманітних факторів, в тому числі і навколишнього середовища [2]. Серед факторів, що можуть мати безпосередній (негативний) вплив варто виділити:

- погодні умови;
- супутню радіацію (гамма-радіацію, бета-частинки);
- наведену радіацію (спричинену взаємодією нейтронів з речовиною);
- фактор зміни властивостей матеріалів внаслідок старіння та механічного навантаження, тощо;
- інші.

В даному контексті, використання Gd-вмісних композитів у складі захисних матеріалів видається найбільш імовірним у двох сценаріях: в приміщенні та на відкритому повітрі.

Очевидно що використання нейтрон-захисних на відкритому повітрі включає в себе набір параметрів які підходять для приміщення, плюс захисне покриття від погодних умов (вологість, сонячна радіація, температура тощо).

Зокрема, на рис. 1 запропоновано чотирьохкомпонентну схему, яка складається захисного покриття (шар 1), проміжного шару 2, нейтрон-захисного шару 3 та конструкційного або основного шару 4. Приклад розташування захисних шарів наведено на рис. 1 нижче.

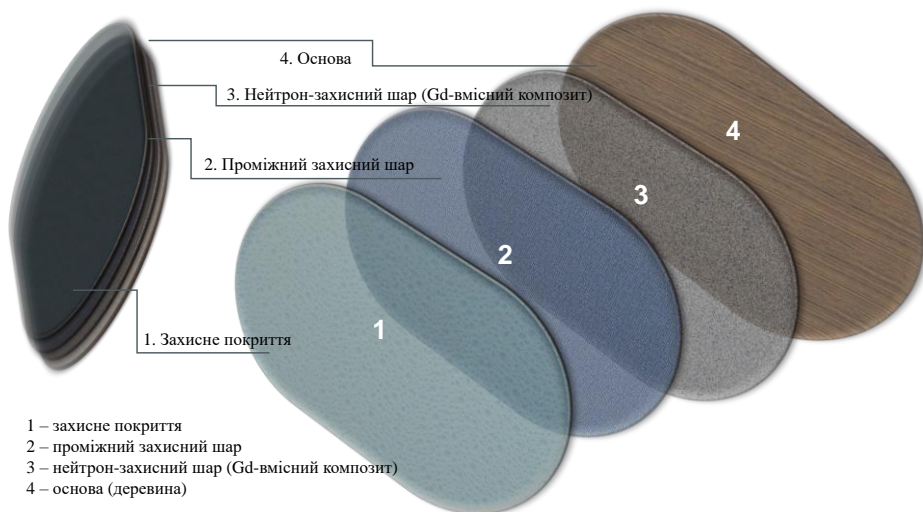


Рис. 1. Приклад схеми розташування захисних шарів та основи для нейтрон-захисного композитного матеріалу

Окрім погодних умов, важливим є вплив супутньої радіації, наявність якої варто очікувати на об'єктах із підвищеною ядерною небезпекою. Важливо, щоб захист від супутньої радіації знаходився на передньому фронті композиту, наприклад в якості захисної фарби, покриття, лаку, тощо.

Радіаційно-стійке покриття наноситься на основу, яка має забезпечувати її надійне закріплення та, відповідно стійкість до погодних умов. Основи таких технологій добре вивчені та відпрацьовані, тому детальне їх висвітлення в даному проекті не має потреби.

Основа може бути будь-яким матеріалом, що відповідає технічних вимогам, наприклад деревина. Деревина має гарні конструкційні властивості та є достатньо ефективним матеріалом для захисту від гамма-випромінювання.

Наступним шаром може бути безпосередньо нейтрон-поглинаючий композитний матеріал. Нейтрон-захисний шар повинен бути розташований найближче до фронту взаємодії з потенційними джерелами опромінення. Товщина шару та кількість нейтрон-захисного композиту в ній може варіюватись в залежності від конкретного призначення. Ресурс роботи має перевищувати максимальне разове навантаження у декілька разів.

Враховуючи супутні фактори, наявні під час експлуатації таких композитів в реальних умовах, важливо також брати до уваги інші компоненти взаємодії нейтронів з речовиною. Варто зазначити що важливо забезпечити нейтрон-поглинаючий композитний матеріал радіаційно стійкою оболонкою товщиною декілька мікрон, виготовленою з матеріалу що запобігає поширенню вторинних електронів та нейтралізує вільні радикали. Варто зазначити, утворення вторинних електронів внаслідок взаємодії нейтронів з бором та гадолієм може спричиняти розрив хімічних зв'язків в мікро метровому масштабі, і саме тому важливо «нейтралізувати» так вторинні електрони. Прикладами таких електрон- та радикал-поглинаючих матеріалів можуть бути зшиті полімерні гідрогелі (наприклад на основі лігніну) та поверхнево-модифіковані неорганічні оксиди (силіка, магнетит, оксид титану та ін.) особливості будови шару 3 та його взаємодії з нейтронним випромінюванням наведено на рисунку 2 нижче.

Бета-частинки (електрони та позитрони) взаємодіють з електронами і ядрами у речовині до повної зупинки. Пробіг бета-частинок залежить від їх енергії. Ефективний пробіг (товщина шару речовини, що зупиняє практично всі частинки) поданий у таблиці 1.

Природа та властивості нейтронного випромінювання накладають специфічні вимоги до створення та експлуатації таких матеріалів. Зокрема, показано, що наявність нейтрон-поглинаючих компонентів є обов'язковою, але недостатньою умовою для їх успішного застосування в умовах навколишнього середовища. Наявність супутньої та наведеної радіації, погодних умов а також особливостей розташування функціональних шарів вимагають ієрархічного підходу до розробки таких нейтрон-поглинаючих матеріалів. В результаті аналізу літературних даних було запропоновано такий підхід. Було показано, що принципова схема створення Gd-вмісних захисних матеріалів полягає у врахуванні усіх факторів їх експлуатації.

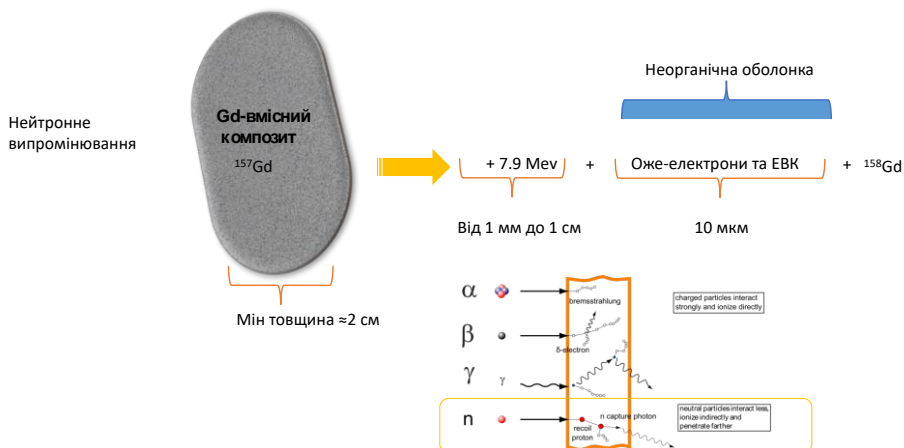


Рис. 2. Фактори, що впливають на оболонку нейтрон-захисного шару

Таблиця 1. Товщина шару речовини, що зупиняє практично всі частинки

Речовина	Енергія електронів			
	0,05 MeB	0,5 MeB	5 MeB	50 MeB
	довжина пробігу, см			
Повітря	4,1	160	2000	17000
Вода	$4,7 \cdot 10^{-3}$	0,19	2,6	19
Алюміній	$2 \cdot 10^{-3}$	0,056	0,95	4,3
Свинець	$5 \cdot 10^{-4}$	0,02	0,3	1,25

- [1] Kovach V., Iatsyshyn Anna, Pylypchuk I., Gurkovskiy V., Romanenko Y. Analysis of Existing Types and Protection Methods Against Neutron Radiation from Different Sources. In: Zaporozhets A., Popov O. (eds) Systems, Decision and Control in Energy IV. Volume II. Nuclear and Environmental Safety. Studies in Systems, Decision and Control. 2023. Vol. 456. P. 77-89. https://doi.org/10.1007/978-3-031-22500-0_5
- [2] Pylypchuk Ie.V., Popov O.O., Kovach V.O., Iatsyshyn Anna V., Kutsenko V.O. Biocompatible Gd-containing micro/nanomaterials from renewable recourses: a new class of environmentally-friendly neutron-shielding materials. Book of Abstracts of the 3rd International Conference on Sustainable Futures: Environmental, Technological, Social and Economic Matters, Ukraine, 24-27 May 2022. Ed. by Anna Iatsyshyn. Kyiv, 2022. p. 84.

О.О. Попов, В.О. Артемчук, Т.М. Яцишин, О.О. Вовк, С.П. Тараненко,
А.М. Лагойко, А.П. Сулима

ПРО ДЕЯКІ ПИТАННЯ ОЦІНКИ РИЗИКУ ХІМІЧНОЇ НЕБЕЗПЕКИ НАСЛІДКІВ АВАРІЙ ПРИ ПЕРЕВЕЗЕННІ НЕБЕЗПЕЧНИХ РЕЧОВИН НА АВТОМОБІЛЬНОМУ ТРАНСПОРТІ

Під час перевезення небезпечних вантажів автомобільним транспортом за різних обставин (ДТП, природні катаклізми, терористичний акт тощо) можуть виникати надзвичайні ситуації (НС), пов'язані із розгерметизацією ємностей (цистерни, контейнери, балони тощо) і потраплянням аварійно-хімічно небезпечних речовин (АХНР) у довкілля та створенням значного ризику для населення прилеглих територій. Небезпека, яку створюють такі НС, дуже велика оскільки досить часто таке транспортування здійснюється в населених районах і поблизу промислових підприємств [1].

В загальному випадку потенційний хімічний ризик на території в районі аварії пересувного хімічно-небезпечного об'єкту і в селітебній зоні поблизу такого об'єкту визначається за формулою:

$$R_x = \sum_i^{m_i} Q^* \times P_i \times R_i, \quad (1)$$

де Q^* - частота реалізації події протягом року;

P_i – ймовірність перебування людини в i -тому середовищі проживання (див. таблиці 1,2);

R_i – умовна ймовірність ураження людини при знаходженні в i -тому середовищі проживання;

На даний момент частоту виникнення небезпечної події Q_j^* розраховують методами теорії ризику, або згідно зі статистичними даними.

Частоту виникнення небезпечної події Q_j^* можна визначити за допомогою теорії експертних оцінок. Експертні оцінки частоти техногенних аварій проводяться з урахуванням їх розподілу на п'ять рівнів:

- часта відмова: $> 1 \text{ рік}^{-1}$;
- ймовірна відмова: $1 \dots 10^{-2} \text{ рік}^{-1}$;
- можлива відмова: $10^{-2} \dots 10^{-4} \text{ рік}^{-1}$;
- рідкісна відмова: $10^{-4} \dots 10^{-6} \text{ рік}^{-1}$;
- практично неймовірна відмова – очікувана частота виникнення $< 10^{-6} \text{ рік}^{-1}$.

Ймовірність перебування людей в i -му середовищі P_i визначають виходячи з виробничої діяльності персоналу, тому розрахунок умовної ймовірності ураження або математичного очікування збитків від негативного впливу АХНР представляє певні складності. Ці складності пов'язані з токсичним впливом на людину різних за фізико-хімічними властивостями типів АХНР та не однаковим часом експозиції в залежності від перебування у зоні можливого хімічного ураження.

Таблиця 1. Середньодобовий розподіл міського населення за місцем перебування [3]

Час доби, год	Житлові та громадські будівлі	Виробничі будівлі	У транспорті			На вулиці (відкрито)		
			Міста з населенням (млн людей)					
			0,25... 0,5	0,5... 1,0	Більше 1,0	0,25... 0,5	0,5... 1,0	Більше 1,0
1...6	0,94	0,06	-	-	-	-	-	-
6...7	0,74	0,06	0,07	0,09	0,12	0,13	0,11	0,08
7...10	0,22	0,5	0,09	0,11	0,17	0,19	0,17	0,11
10...13	0,28	0,52	0,06	0,07	0,1	0,14	0,13	0,1
13...15	0,45	0,37	0,04	0,04	0,07	0,14	0,14	0,11
15...17	0,27	0,49	0,08	0,09	0,13	0,15	0,15	0,12
17...19	0,45	0,24	0,1	0,12	0,15	0,2	0,18	0,15
19...24	0,77	0,14	0,04	0,04	0,06	0,05	0,05	0,03

Таблиця 2. Середньодобовий розподіл сільського населення за місцем перебування [3]

Час доби	Поле та сільськогосподарське виробництво		Жилі приміщення	
	вдень	вночі	вдень	вночі
1...6	0,25	0,1	0,75	0,9
6...7	0,6	0,4	0,4	0,6
7...10	0,75	0,75	0,25	0,25
10...13	0,8	0,8	0,2	0,2
13...15	0,85	0,75	0,15	0,25
15...17	0,85	0,5	0,15	0,5
17...19	0,8	0,4	0,2	0,6
19...24	0,5	0,2	0,5	0,8

Умовна ймовірність ураження у разі знаходження в зоні хімічного ураження з урахуванням висоти підйому хмари в основному визначається зоною ураження, що утворюється за рахунок поширення ураженої хмари на селітебну частину населеного пункту, як на ділянці гальмування, так і в районі аварійної зупинки транспорту з АХНР і може бути визначено як [2]:

$$R = \frac{S_B + S_F}{S_S}, \quad (2)$$

де S_B – площа порогового хімічного ураження на ділянці гальмування, км²;

S_F – площа порогового хімічного ураження в районі аварійної зупинки транспорту з АХНР, км²;

S_S – площа населеного пункту, км².

Площа порогового хімічного ураження на ділянці гальмування та в районі аварійної зупинки визначається глибиною порогового ураження на цих ділянках.

Площа хімічного ураження на ділянці гальмування з урахуванням підйому ураженої хмари може бути обчислена як [2]:

$$S_B = \sum_{i=1}^n S_{B_i} \times \frac{H_C}{H_B}, \quad (3)$$

де S_{B_i} – площа хімічного ураження на i -тій ділянці гальмування, визначається як:

$$S_{B_i} = \frac{\pi\varphi}{360^\circ} \left[D_B + (D_l - D_B) \times k_m \right]^2 - D_B^2, \quad (4)$$

де D_B – відстань від початку забудови до траси, м;

D_l – глибина порогового ураження на i -й ділянці гальмування, м;

l – відповідає ділянці кінцевої гальмівної дороги до аварійної зупинки, м;

$l=1$ – відповідає області маршруту гальмування, коли досягається $D_l=D_B$, м;

k_m – коефіцієнт зменшення поширення ураженої хмари залежно від забудови та кількості поверхів будівель, визначених у роботі [2].

Площа хімічного ураження в області аварійної зупинки, враховуючи зростання ураженої хмари, може бути обчислена як:

$$S_F = \frac{\pi\varphi}{360^\circ} \left[\left[D_b + (D_{n_f} - D_b) \cdot k_m \right]^2 - D_B^2 \right] \times \frac{H_C}{H_B}, \quad (5)$$

де D_{n_f} – глибина порогового ураження в області аварійної зупинки;

φ – кут поширення можливої хімічного ураження, що визначається відповідно до таблиці 3.

H_C – висота підняття порогового ураження хмари, м;

H_B – висота будівель у населеному пункті, м.

Таблиця 3 – Кутові розміри зон фактичного хімічного ураження

Ступінь вертикальної стійкості	Інверсія	Ізометрія	Конвекція
φ , градус	Стійкий вітер		
	11,5	14,5	48,5
	Нестійкий вітер		
	47	48	69

Таким чином, при обчисленні умовної ймовірності ураження під час виникнення таких подій, одним із важливих аспектів є визначення глибини порогу, смертельного хімічного ураження та висоти підйому їх хмари.

- [1] Popov O., Iatsyshyn A., Pecheny V., Kovach V., Kovalenko V. Approaches to Assessing Consequences of Accidents During Transportation of Hazardous Substances by Road. In: Zaporozhets A., Popov O. (eds) Systems, Decision and Control in Energy IV. Volume II. Nuclear and Environmental Safety. Studies in Systems, Decision and Control. 2023. Vol. 456. P. 327-342. https://doi.org/10.1007/978-3-031-22500-0_22
- [2] Savchuk O.N. Forecasting and elimination of consequences in case of accidents (destruction) of mobile chemically hazardous objects: monograph. St. Petersburg, St. Petersburg State Fire Service EMERCOM of Russia, 2014..
- [3] Aksenov A.A. Assessing the risk of chemical hazards during the transportation of hazardous chemically hazardous substances by road. St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia. St. Petersburg, 2019.

АПАРАТНЕ ПРИСКОРЕННЯ ВИЯВЛЕННЯ АТАК НА ЦИФРОВІ ПІДСТАНЦІЇ

Вступ

Цифровізація систем автоматики та АСУ ТП разом з відомими перевагами, на жаль, привносить в роботу промислових систем проблеми інформаційної безпеки. Якщо автоматизуються об'єкти критичної інфраструктури, зокрема, в енергетичній галузі, наслідки від реалізації кіберзагроз можуть бути більш важкими в порівнянні з традиційними галузями застосування інформаційних технологій [1, 2]. У даній роботі розглянуто проблему захисту від зовнішніх атак систем автоматизації щодо цифрових підстанцій (ЦПС). Досліджені питання застосування апаратного прискорення з використанням програмованих логічних інтегральних схем (ПЛІС).

1. Стандарт МЕК 61850

Електричні підстанції є одними з найчисленніших об'єктів енергетики та відіграють вирішальну роль у всій енергосистемі, виконуючі важливі функції з розподілу та перетворення енергії [3]. Складнощі, що виникають при переводі їх обладнання на цифрову елементну базу, пов'язані в першу чергу зі стандартизацією. Якщо життєвий цикл силового обладнання, такого як трансформатори, комутаційні апаратні роз'єднувачі тощо складає близько 40 років, то керуючі системи оновлюються в середньому кожні 15 років. В результаті змушені спільно взаємодіяти пристрої декількох поколінь, не сумісні між собою.

Для вирішення даної проблеми було створено стандарт МЕК 61850 «Мережі та системи зв'язку на підстанціях» [4]. Головна ідея документа – розробити єдині специфікації, які дозволили б, з одного боку, захистити фінансові вкладення в енергетичне обладнання, з іншого – використовувати передові обчислювальні та мережеві технології. Перша редакція документу (який насправді містить низку стандартів) з'явилася ще в 2003 році.

Відповідно до стандарту МЕК 61850 система автоматизації інформаційного обміну на енергооб'єкті за схемою ЦПС складається з трьох рівнів [3]: станційний (Station Level) – найвищий рівень, рівень приєднання (Bay Level) та рівень процесу (Process Level) або "польовий" (Field Level) – найнижчий рівень. Кожен рівень виконує притаманні йому функції, за які відповідають певні типи пристроїв. Комунікації можливі як всередині рівнів (горизонтальні), так і між рівнями (вертикальні).

На додаток до традиційних протоколів, таких як FTP або HTTP, стандарт МЕК 61850 вводить нові протоколи, а саме: MMS (Manufacturing Message Specification) – для зв'язку інтелектуальних пристроїв (IED) зі станційним рівнем, GOOSE (Generic Object Oriented Substation Events) – для зв'язку IED між собою, SV (Sampled Values) – для зв'язку між IED та MU.

Строго кажучи, MMS є не протоколом, а специфікацією, що описує інформаційну модель пристроїв та даних рівня приєднання. Але, оскільки сервіс, що використовує MMS, застосовує рівень додатків стандартного стеку мережевих протоколів OSI, його також можна умовно вважати протоколом обміну. Принаймні, в технічній літературі з питань використання стандарту MEK 61850 та вирішення проблем захисту інформації в ЦПС на його основі, скорочення MMS в переважній більшості публікацій згадується саме як протокол.

Достатньо змістовний опис згаданих протоколів, включаючи часові діаграми, можна знайти в літературі, наприклад, в [3]. Зауважимо, що в кіберфізичних системах, побудованих на базі стандарту MEK 61850, також можуть використовуватися інші мережеві протоколи, наприклад, поширена польова шина MODBUS, або її проприетарна модифікація MODBUS Plus, протокол часової синхронізації PTP (Precision Time Protocol), протокол виявлення мережевих пристроїв LLDP (Link Layer Discovery Protocol) та ін.

2. Системи виявлення вторгнень для цифрових електричних підстанцій

Особливості ЦПС, зокрема, застосування спеціалізованих протоколів, накладають певну специфіку при створенні систем виявлення вторгнень (СВВ) для цифрових підстанцій на базі стандарту MEK 61850 [5]. Технічно робота таких СВВ зазвичай будується на складанні так званих специфікаційних правил (specification rules) для всіх можливих атак на кожний з протоколів.

Одним з обмежень використання традиційних засобів кіберзахисту, що накладаються специфікою промислового застосування, є брак обчислювальної потужності. Прискорити роботу СВВ дозволяє використання програмованої логіки [6] Але традиційні реконфігуровні обчислювачі на базі ПЛІС [7], які застосовуються для апаратного прискорення в ІТ-сфері, розраховані на використання спільно з традиційними комп'ютерами, що ускладнює їх використання для захисту кіберфізичних систем. Аналіз технічної інформації свідчить, що існує можливість використання програмованої логіки в кіберфізичних системах шляхом застосування вже наявних в них реконфігуровних ресурсів. В даному дослідженні знайдено два джерела технічних засобів, що містять ПЛІС.

3. Можливості апаратного прискорення роботи систем виявлення вторгнень на цифрових електричних підстанціях

По-перше, існують деякі технологічні задачі енергетики, для вирішення яких вже використовуються ресурси програмованої логіки, частину яких можна задіяти для цілей кібербезпеки, зокрема, для створення систем виявлення вторгнень. Прикладами таких застосувань можуть бути системи управління, алгоритми яких засновані на використанні апаратів нейронних мереж і нечіткої логіки, інтелектуальні системи збору даних, частотні перетворювачі для керування потужними електроприводами і т.п.

По-друге, інтелектуальні пристрої IED також мають в своєму складі

ПЛІС або системи на кристали для реалізації, зокрема, сумісних зі стандартом IEEE-1588 протоколів паралельного резервування з'єднань HSR (High-availability Seamless Redundancy) і PRP (Parallel Redundancy Protocol), а також для підтримки розглянутих вище протоколів стандарту МЕК 61850 [8].

Висновки

В роботі досліджені питання створення системи виявлення вторгнень для цифрових електричних підстанцій на основі стандарту МЕК 61850. Наведені відомості щодо побудови таких систем з використанням підходу на базі специфікацій. Досліджено можливості використання для синтезу систем виявлення вторгнень реконфігурованих обчислювальних ресурсів, зокрема тих, що присутні в пристроях промислової автоматики та входять до складу інтелектуального цифрового обладнання.

- [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) [Електронний ресурс]. – Режим доступу: <https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html>. – Загл. з екрану. – (Дата звернення: 30.04.2023)
- [2] Radichel T. Colonial Pipeline Hack / T. Radichel // *2nd Sight Lab* (May 15, 2021) [Електронний ресурс]. – Режим доступу: <https://medium.com/cloud-security/colonial-pipeline-hack-4486d16f2957>. – Загл. з екрану. – (Дата звернення: 30.04.2023)
- [3] *Communication Networks and Systems in Substations. IEC Std. 61850.*
- [4] 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.
- [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.
- [6] 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. – P. 210-213, doi: 10.1109/IPDPSW.2018.00040.
- [7] Hilgurt S.Ya. A Survey on Hardware Solutions for Signature-Based Security Systems // *Information Technologies: Theoretical and Applied Problems (ITTAP-2021): Proceedings of the 1st International Workshop, Ternopil, Ukraine, 16 – 18 Nov. 2021.* – Ternopil: Faculty of Computer Information Systems and Software Engineering, 2021. – P. 6-23. Available online: <https://ceur-ws.org/Vol-3039/paper17.pdf>.
- [8] Гільгурт С.Я. Апаратне рішення задач кібербезпеки в електроенергетичній галузі // *Кібербезпека енергетики: Збірка праць конференції, м. Одеса, 28 травня – 1 червня 2019.* – К.: Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, 2019. – С. 11-14.

А.М. Давиденко, С.Я. Гільгурт, О.С. Потенко, О.Г.Кіслово

ПОВОДЖЕННЯ З ПОРОДЖУВАЛЬНИМИ МАТРИЦЯМИ ЗАВАДОСТІЙКОГО КОДУВАННЯ ІНФОРМАЦІЇ В КІБЕРФІЗИЧНИХ СИСТЕМАХ

Так звані коригуючі коди, які використовуються для боротьби з завадами у каналах зв'язку, зокрема в кіберфізичних системах об'єктів енергетичної інфраструктури, дозволяють не тільки виявляти, але й виправляти помилки [1]. У блокових коригуючих кодах, на відміну від потокових, інформація кодується послідовностями бітів фіксованої довжини, тобто словами.

Метою даного дослідження є підвищення ефективності поводження з такими кодами.

Існують нелінійні та лінійні блокові коди, причому останні є більш простими у використанні, тому вони більш розповсюджені. Лінійний код довжини n і розмірністю k позначається як (n, k) -код і однозначно задається так званою породжувальною матрицею G , множення на яку вхідного слова даних (заданного бітовим вектором \vec{v}) дає результуюче закодоване слово (у вигляді бітового вектора \vec{c}):

$$\vec{c} = \vec{v}G = (v_1, v_2, v_3, \dots, v_k) \begin{bmatrix} g_{1,1} & g_{1,2} & \dots & g_{1,n} \\ g_{2,1} & g_{2,2} & \dots & g_{2,n} \\ \dots & \dots & \dots & \dots \\ g_{k,1} & g_{k,2} & \dots & g_{k,n} \end{bmatrix}.$$

Оскільки для виправлення помилок необхідна надмірність даних, закодоване слово має більшу довжину, ніж вхідне. Тобто ширина n породжувальної матриці за визначенням більша за її висоту k .

У зв'язку з тим, що перестановка будь-яких рядків та стовпців не змінює властивостей коду, будь-який коригуючий лінійний блоковий код можна привести до так званого систематичного коду [2], тобто подати у вигляді квадратної одиничної матриці I , доповненої бітами підрахунку надлишкових кінцівок коду у вигляді прямокутної матриці A :

$$G = [I_{k,k}] [A_{k,n-k}] = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{bmatrix} \begin{bmatrix} a_{1,k+1} & a_{1,k+2} & \dots & a_{1,n} \\ a_{2,k+1} & a_{2,k+2} & \dots & a_{2,n} \\ \dots & \dots & \dots & \dots \\ a_{k,k+1} & a_{k,k+2} & \dots & a_{k,n} \end{bmatrix}.$$

Сутність систематичного коду полягає у тому, що будь яке вхідне слово, закодоване таким кодом, є тим самим словом, доповненим наприкінці надлишковими бітами у кількості $(n - k)$. Найважливішим показником коду є найменша кодова відстань між допустимими кодовими комбінаціями, яка безпосередньо пов'язана з кількістю помилок, що їх може виправляти код. Тому пошук породжувальних матриць з максимально можливим значенням цього параметра є актуальною задачею.

Історично так склалося, що лінійний блоковий код позначають його параметрами n та k . Якщо відобразити результати розрахунків мінімальної кодової відстані у вигляді таблиці, де по горизонталі та вертикалі відкладено ці параметри, картина вийде не дуже наочна (Табл. 1).

Таблиця 1.

$n \setminus k$	4	5	6	7	8	9	10	11	12
7	3	x	x	x	x	x	x	x	x
8	4	2	x	x	x	x	x	x	x
9	4	3	2	x	x	x	x	x	x
10	4	4	3	x	x	x	x	x	x
11	5	4	4	3	x	x	x	x	x
12	6	4	4	4	3	x	x	x	x
13	6	5	4	4	4	3	x	x	x
14	7	6	5	4	4	4	3	x	x
15	8	7	6	5	4	4	4	3	x
16	8	8	6	6	5	4	4	4	2
17	8	8	7	6	6	5	4	4	3
18	8	8	8	7	6	6	4	4	4
19	9	8	8	8	7	6	5	4	4
20	10	9	8	8	8	7	6	5	4
21	10	10	8	8	8	8	7	6	5
22	11	10	9	8	8	8	8	7	6
23	12	11	10	8	8	8	8	8	7
24	12	12	10	9	8	8	8	8	8

Оскільки виправляти помилки можуть лише коди з непарним значенням мінімальної кодової відстані, саме вони мають практичну цінність (відповідні комірки в таблиці відмічені темним кольором).

Погана наочність та зайва витратність такого способу подання результатів обумовлена тим фактом, що параметр n – довжина всього коду – вже містить в своєму складі інший параметр k – кількість корисних бітів.

В даному дослідженні пропонується більш зручний та компактний спосіб подання результатів розрахунків. Тут параметр k відкладено по вертикалі, а по горизонталі – кількість надлишкових бітів $(n - k)$. Зовнішній вигляд такого подання наведено в Табл. 2.

Результати розрахунків мінімальної кодової відстані

$k \setminus n-k$	4	5	6	7	8	9	10	11	12	13
4	4	4	4	5	6	6	7	8	8	8
5	3	4	4	4	5	6	7	8	8	8
6	3	4	4	4	5	6	6	7	8	8
7	3	4	4	4	5	6	6	7	8	8
8	3	4	4	4	5	6	6	7	8	8
9	3	4	4	4	5	6	6	7	8	8
10	3	4	4	4	4	5	6	7	8	8
11	3	4	4	4	4	5	6	7	8	8
12	2	3	4	4	4	5	6	7	8	8
13	2	3	4	4	4	5	6	7	8	8
14	2	3	4	4	4	5	6	7	8	8

Дивлячись на результаті в такому поданні нескладно помітити закономірність, яка полягає у тому, що питомі комірки з непарними значеннями формують стовпчики, які інколи "надломлюються" із зсувом праворуч. Врахування цієї закономірності дозволяє не проводити багато зайвих ресурсноємних розрахунків з пошуку корисних породжувальних матриць з використанням високопродуктивних обчислювальних засобів [3].

Результатом дослідження є більш зручна та наочна форма подання породжувальних матриць лінійних блокових коригуючих кодів для протидії завадам в кіберфізичних системах. Запропонований спосіб поводження з результатами дозволив суттєво скоротити кількість обчислювальних витрат.

- [1] Давиденко А.М. Підхід до забезпечення цілісності інформації в кіберфізичних системах / А.М. Давиденко, С.Я. Гільгурт, О.С. Потенко, О.Г. Кіслов // XL Щорічна науково-технічна конференція молодих вчених і спеціалістів: Тези доп., м. Київ, 11 травня 2022. – К.: Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, 2022. – С. 57-58.
- [2] Винничук С.Д. Нижня оцінка максимального кодового розстояння для лінійних блокових кодів (n, k) над полем $GF(2)$ / С.Д. Винничук, А.Н. Давиденко, С.Я. Гільгурт, А.С. Потенко // Тез. доп. Міжнар. наук.-техн. конф. «Моделювання-2012». – К.: Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, 2012. – С.150-153.
- [3] Evdokimov V. Using GRID for Centralized Synthesis of FPGA-based Information Security Systems / V. Evdokimov, A Davydenko, S. Hilgurt // Pattern Recognition and Information Processing (PRIP'2021) : Proceedings of the 15th International Conference, 21–24 Sept. 2021, Minsk: UIIP NASB, 2021. – pp. 115-118.

А.М. Примушко

КОНКУРЕНТНЕ УКЛАДАННЯ ТА ВИКОНАННЯ УМОВ СМАРТ КОНТРАКТІВ ПРЕДСТАВЛЕНИХ У ВИГЛЯДІ ВИСОКОРІВНЕВИХ ФУНКЦІЙ ПЕРЕХОДУ МІЖ СТАНАМИ КОНТРАКТУ ЗА ДОПОМОГОЮ ДЕНОТАЦІЙНОЇ СЕМАНТИКИ

Смарт-контракт – протокол або комп’ютерна програма-контракт який призначений для автоматичного виконання, контролю або документування істотних умов й дій відповідно до умов контракту при його укладанні [1, 2] .

Смарт контракт має блочну структуру зі змінними, функціями, модифікаторами функцій, допоміжними структурами тощо. Семантично смарт-контракт є послідовністю переходів між станами контракту представлену у вигляді деякої послідовності дій:

$$S_a \Rightarrow a_0 \xrightarrow{f(a_0, a_1)} a_1 \rightarrow \dots \rightarrow a_{n-1} \xrightarrow{f(a_{n-1}, a_n)} a_n \quad (1)$$

де S_a – сукупність всіх істотних умов та відповідних дій, що в обов’язковому порядку мають бути виконані після підписання смарт-контракту (тобто його фактичного укладання), a – деяка умова або дія, що направлена на реалізацію інтересу об’єкту договору щодо суб’єкту договору; $f(a_{i-1}, a_i)$ – функція переходу від поточного стану договору з реалізованою умовою a_{i-1} до стану з умовою a_i , що може бути реалізована, за умови, що a_{i-1} й a_i є узгодженими та верифікованими. Варто зазначити, що будь яка f , результуючий стан якої не може бути узгодженим та верифікованим відкидається як та, що несе загрозу об’єкту договору.

В свою чергу високорівнева функція переходу F якісно характеризує перехід між низькорівневими функціями переходу f , що дозволяє верифікувати та прогнозувати наслідки виконання дій, що мають бути виконані при укладанні смарт-контракту. Високорівнева функція переходу між f_{n-1} та f_n відповідно матиме вигляд:

$$F_{[f_{n-1}, f_n]} = f_{n-1} \rightarrow f_n \quad (2)$$

При цьому a та f можуть бути представлені у вигляді категорій [3], а F у вигляді функтору або денотації, що описує перехід від однієї категорії в іншу, в просторі, що повністю описує контекст деякої задачі, як от укладання смарт-контрактів. Ця особливість дозволяє квантувати структуру договору на самостійні, фактично, математичні утворення. Перехід від $F_{[f_{n-1}, f_n]}$ до $F_{[f_n, f_{n+1}]}$ виражається через денотаційну семантику або ж семантику Скота-Стрейчі [4,5].

Ринок двосторонніх договорів дозволяє купувати електроенергію для певного періоду часу у необмеженій кількості продавців. При цьому істотні умови формуються за домовленістю сторін. Конкурентне укладання смарт-контрактів передбачає зміну умов договору в реальному часі, що є характерним для внутрішньодобового (ВДР), “на добу наперед” (НДР) та балансуючого ринків, та їх обов’язкове виконання. В такому процесі декілька умов смарт-контракту в електронній формі, опосередковано, через автоматизовану систему узгоджуються й приймаються або відкидаються як такі, що несуть потенційні ризики для одного з учасників договору або порушують норми права. При цьому рівняння (1), враховуючи кількість учасників, що можуть одночасно пропонувати істотні умови контракту, зміниться:

$$S_{[a,N]} \xrightarrow{i \in [0,N]} a_{[0,N_i]} \xrightarrow{f(a_{[0,N_i]}, a_{[1,N_i]})} a_{[1,N_i]} \rightarrow \dots \rightarrow a_{[n-1,N_i]} \xrightarrow{f(a_{[n-1,N_i]}, a_{[n,N_i]})} a_{[n,N_i]}$$

де N – кількість учасників, що одночасно беруть участь в укладанні договору; i – унікальний маркер учасника. Тут $S_{[a,N=0]}$ слід розуміти як деякий терм, що виступає в якості початкового стану контракту при ініціації процесу його подальшої зміни.

Відповідно (2) запишемо як: $F_{[f_{[n-1,N_i]}, f_{[n,N_i]}]} = f_{[n-1,N_i]} \rightarrow f_{[n,N_i]}$, що характеризує високорівневі зміни в договорі, як от зміна контексту (зміна правила) або перехід від однієї нормативно-правової бази до іншої (загальна зміна набору правил). Такі зміни можуть бути узгоджені, перевірені та, відповідно, верифіковані. Треба зазначити, що перевірку доцільно робити при укладанні контракту, тоді як верифікацію при його безпосередньому виконанні, а саме на етапі підготовки перед виконанням основного блоку контракту.

При укладанні такого електронного договору між багатьма учасниками в реальному часі виникнуть суперечності та з’являться деякі антропоцентричні фактори кібербезпеки, як от недобросовісні дії зі сторони одного з учасників договору. Такими діями може бути штучне завищення ціни на енергоносії, шахрайська схема збагачення за рахунок транзиту електроенергії через третіх учасників ринку, відмивання коштів тощо. Для того щоби вирішити ці суперечності – узгодити запропоновані умови контракту в реальному часі, доцільно використовувати алгоритми консенсусу [6,7,8,9]. Такі алгоритми можуть бути використані для прийняття й подальшого об’єднання або відхилення умов, запропонованих сторонами електронного договору. Відповідний результат консенсусу може вважатися фінальною домовленістю сторін, що може бути зафіксований в електронній формі придатній для сприйняття людиною й буде відповідати визначенню

електронного договору. Згідно ч.1 ст. 527 ЦК України [10] автоматичне виконання зобов'язань є виконанням належними сторонами. Залишається відкритим питання примусового виконання зобов'язань, що виникають при укладанні смарт-контракту.

Алгоритми консенсусу можуть бути скомбіновані з методами штучного інтелекту [11, 12, 13] задля досягнення більшої гнучкості та виявлення антропоцентричного фактору кібербезпеки, що несуть відповідні ризики для учасників договору й системи в цілому.

Узагальнена схема конкурентного укладання смарт-контрактів, використовуючи алгоритми консенсусу показана на рис. 1.

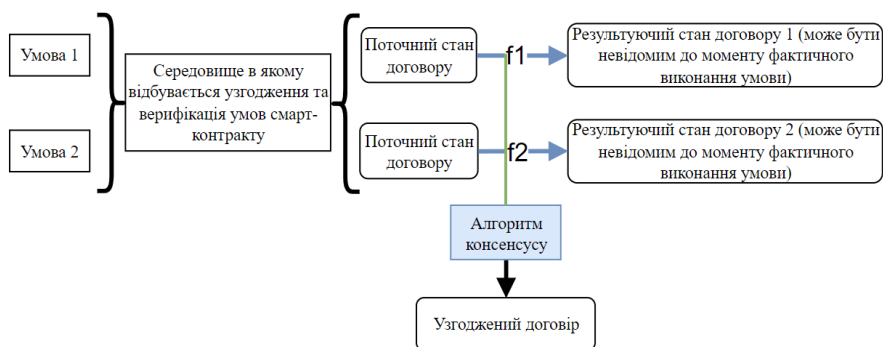


Рис. 1. Узагальнена схема конкурентного укладання смарт-контрактів, використовуючи алгоритми консенсусу.

Розглянутий метод конкурентного укладання та виконання умов смарт-контрактів дозволяє учасникам двостороннього договору узгодити істотні умови, перевірити та верифікувати дії та / або зобов'язання, описані договором, та проаналізувати фактори антропоцентричного ризику кібербезпеки, що робить сам процес створення й реалізації електронного договору надійнішим, гнучкішим, безпечнішим.

Подальші дослідження передбачають визначення й експериментальні дослідження загального методу конкурентного укладання й виконання умов смарт контрактів на основі алгоритмів консенсусу, представлених у вигляді високорівневих функцій переходу між низькорівневими функціями, що характеризують стани контракту, спираючись на денотаційну семантику; визначення алгоритмів консенсусу на основі нормативно-правової бази, що дозволило би в процесі укладання договорів проводити оцінку антропоцентричного фактору кібербезпеки при укладанні смарт-контрактів, прогнозувати та верифікувати їх поведінку на основі методів штучного інтелекту.

- [1] Fries, Martin; P. Paal, Boris, (2019). Smart Contracts (in German). Mohr Siebeck.
- [2] Savelyev, Alexander, (2016). Contract Law 2.0: "Smart" Contracts As the Beginning of the End of Classic Contract Law, Social Science Research Network.
- [3] Milewski, Bartosz, (2019). Category Theory for Programmers, ISBN-10: 0464243874.
- [4] Dana S. Scott, (1970). Outline of a mathematical theory of computation. Technical Monograph PRG-2, Oxford University Computing Laboratory, Oxford, England.
- [5] Joseph E. E. Stoy, (1981), Denotational Semantics: The Scott-Strachey Approach to Programming Language Theory (Computer Science Series), MIT Press.
- [6] Lachtar, Nada., Elkhail, Abdulrahman Abu., Bacha, Anys., Malik, Hafiz, (2020). A Cross-Stack Approach Towards Defending Against Cryptojacking, IEEE Computer Architecture Letters, 19 (2), pp. 126–129.
- [7] Zhao, Wenbing., Yang, Shunkun., Luo, Xiong., Zhou, Jiong, (2021). On PeerCoin Proof of Stake for Blockchain Consensus, ICBCT'21: The 3rd International Conference on Blockchain Technology. ACM. pp. 129–134.
- [8] Daniel Larimer. Delegated Proof-of-Stake (DPOS), електронний ресурс: <http://107.170.30.182/security/delegated-proof-of-stake.php>.
- [9] Kirmann, Hubert. Fault Tolerant Computing in Industrial Automation. Switzerland: ABB Research Center. p. 94.
- [10] ЦИВІЛЬНИЙ КОДЕКС УКРАЇНИ, Документ 435-IV, чинний, поточна редакція — Редакція від 28.04.2023, підстава - 2989-IX, 2970-IX, електронний ресурс: <https://zakon.rada.gov.ua/laws/show/435-15#n2698>.
- [11] Yixiao Lan1., Yuan Liu., Boyang Li., Chunyan Miao. Proof of Learning (PoLe): Empowering Machine Learning with Consensus Building on Blockchains (Demo), The Thirty-Fifth AAAI Conference on Artificial Intelligence (AAAI-21).
- [12] Bo Liu. Consensus-based Distributed Machine Learning: Theory, Algorithms, and Applications, University of Manchester.
- [13] Dariusz Plewczynski. BRAINSTORMING: Consensus Learning in Practice, ICM, Interdisciplinary Centre for Mathematical and Computational Modelling, University of Warsaw.

РОЗПОДІЛЕНИЙ АНАЛІЗ ДАНИХ АВТОНОМНОГО РОЮ

Технологія рою стає все більш актуальною для багатьох галузей, включаючи військову, промислову, аграрну, медичинську і т.п. Поведінка рою, як це можна спостерігати на прикладах рою бджіл або зграї птахів, забезпечує стабільну організацію сенсорних платформ, які є гнучкими та здатними швидко пристосовуватись до змін в навколишньому середовищі. Ці системи забезпечують повільну деградацію функціональності при виході з ладу індивідуального сенсору. Рой дронів являє собою групу безпілотних літальних апаратів.

Наукові дослідження по темі рою дронів активно розвиваються і включають велику кількість напрямків: розробка алгоритмів координації всередині рою, алгоритмів адаптації поведінки до змін зовнішніх умов, що базуються на алгоритмах штучного інтелекту, підвищення автономності рою, тощо.

Мною проаналізовано близько сотні різноманітних матеріалів, включаючи статті, дисертації та монографії, в тому числі роботи [1-7]. Серед великої кількості розглянутих робіт велика увага приділяється моделюванню поведінки рою та алгоритмам взаємодії, проте, як на мій погляд, недостатньо вивченою залишається тема розподілених обчислень всередині рою. Адже обчислювальні можливості одного агента є дуже обмеженими, а необхідність аналізу даних в режимі реального часу постійно зростає. Однією з фундаментальних в області розробки засобів комунікації між агентами в середині рою, на мій погляд, є робота [1]. Яка, незважаючи на дату публікації, й досі залишається актуальною і лягла в основу даного огляду.

За останній час був зроблений значний крок в мініатюризації електронних та електромеханічних систем. Сучасні пристрої обладнані засобами бездротової комунікації, великою кількістю сенсорів та є досить мобільними. Завдяки великій роздільній здатності сучасні сенсори продукують великі обсяги даних (в десятки мегабайтів або навіть гігабайтів), таких як потокове відео, нерухомі зображення та інші.

Традиційно, в умовах обмеженої пропускну здатності мережі, ці дані оброблялись офлайн, і потім результати обробки розповсюджувались через мережу. Це створювало значні затримки між подією та її виявленням і подальшим сповіщенням про неї. Як наслідок - втрата актуальності результатів.

З підвищенням пропускної здатності мереж та ростом обсягу даних з'явилась можливість обробляти інформацію методами машинного навчання з метою отримання високо достовірної інформації.

В роботі [1] використовується поняття спеціалізованої мережі. Спеціалізована мережа - це сукупність нод, об'єднаних бездротовим зв'язком, що динамічно утворюють тимчасову мережу без використання будь-яких існуючих інфраструктур або централізованого адміністрування. В такій мережі кожна мобільна нода не тільки діє як хост, але і як роутер, пересилаючи дані від одних мобільних нод до інших, що можуть знаходитись поза межами діапазону прямої комунікації.

Запропонована методологія моделювання спеціальної мережі комунікації для систем сенсорів на базі рою описує процес оцінки продуктивності протоколів комунікації по відношенню до динаміки рою.

Автором [1] запропоновано математичну модель симуляції рою, що являє собою параметризовану систему, призначену для дослідження характеристик поведінки рою.

Також, було розглянуто три мережевих протоколи комунікації для мережі сенсорів в рою та зроблено порівняння їх продуктивності: Directed Diffusion, Geographical Routing Protocol та Flooding Protocol.

Дослідження показало, що протокол Directed Diffusion є більш продуктивним, ніж Geographical Routing Protocol.

Вочевидь, технології комунікації для бездротових спеціалізованих мереж повинні забезпечувати ефективну передачу великої кількості даних у високо динамічному мережевому середовищі. Велика кількість таких пристроїв (сотні або навіть тисячі одиниць) можуть працювати разом для забезпечення точною інформацією близької до дійсного часу (near real-time basis).

Ефективність в цьому контексті визначається як здатність успішно пересилати дані на необхідну відстань з великою пропускною здатністю та низькою затримкою, при обмеженій пропускній здатності та топології, що динамічно змінюється. Треба враховувати, що комунікація може відбуватися в умовах радіоелектронних завад.

Загалом в роботі [1] було досягнуто три основні цілі:

- розроблено модель рою з розширеною гнучкістю в поведінці для використання в подальшому аналізі комунікаційної мережі
- розроблено класифікаційну методологію аналізу поведінки рою
- розроблено та проаналізовано комунікаційну мережі в контексті поведінки рою

В якості висновку потрібно зауважити, що розглянуту роботу доцільно взяти за основу для подальшого дослідження - розробки методу розподіленого аналізу даних автономного рою.

- [1] Kadrovach, Brian A. “A Communications Modeling System for Swarm-Based Sensors”. Defense Technical Information Center. 2003. URL: <https://apps.dtic.mil/sti/citations/ADA417458>
- [2] DeMedeiros, Kyle D. Wettergren, Thomas A. “Control of Multi-Agent Swarms with Cooperative Particle Swarm Optimization”, Defense Technical Information Center. 2019. URL: <https://apps.dtic.mil/sti/citations/AD1081002>
- [3] Thompson, Richard B. “Confidential and Authenticated Communications in a Large Fixed-Wing UAV Swarm”. 2016. URL: <https://apps.dtic.mil/sti/citations/AD1031535>
- [4] Maj Sean M. Williams. “Swarm Weapons: Demonstrating a Swarm Intelligent Algorithm for Parallel Attack”. 2018. URL: <https://apps.dtic.mil/sti/pdfs/AD1071535.pdf>
- [5] Revall, Michael B. “UAV Swarm Behavior Modeling for Early Exposure of Failure Modes”. 2016. URL: <https://apps.dtic.mil/sti/citations/AD1029909>
- [6] Day, Michael. “Multi-Agent Task Negotiation Among UAVs to Defend Against Swarm Attacks”. 2012. URL: <https://apps.dtic.mil/sti/citations/ADA560588>
- [7] Giles, Kathleen. “Mission-Based Architecture For Swarm Composability”. 2018. URL: <https://apps.dtic.mil/sti/citations/AD1052644>

Я.П. Лукашевич

ДОСЛІДЖЕННЯ РОЗВИТКУ ОБ'ЄКТІВ АЛЬТЕРНАТИВНОЇ ЕНЕРГЕТИКИ В УКРАЇНІ З УРАХУВАННЯМ ЇХ ПРИЄДНАННЯ ДО МЕРЕЖ ПЕРЕДАЧІ ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ

Вступ. Після повномасштабного вторгнення Росії українська енергетика переживає складні часи. Частина об'єктів генерації та енергетичної інфраструктури зазнали пошкоджень, знищені або знаходяться на окупованих територіях, зокрема і об'єкти, що виробляють електричну енергію з відновлюваних джерел. Після закінчення війни електроенергетична галузь потребуватиме суттєвого відновлення і розвитку. Тому важливим є завдання з виявлення підходів та методів підтримки та розвитку виробників з альтернативних джерел (ВАД) у воєнний та післявоєнний періоди.

В різних професійних колах відбувалася жвава дискусія про децентралізацію енергетичної системи в контексті обговорень післявоєнної відбудови. Концепція децентралізації включає заходи, спрямовані на забезпечення надійного постачання електроенергії критичним об'єктам інфраструктури, будинкам тощо у випадку пошкодження важливих об'єктів енергетичної системи. Децентралізована (або розподілена) генерація енергії визначається як система виробництва та передачі енергії, яка включає велику кількість споживачів, які одночасно є виробниками електроенергії та тепла для своїх власних потреб. Вони мають можливість передавати вироблену надлишкову енергію до загальної енергетичної мережі.

Для проведення досліджень з розвитку розподіленої генерації в Україні та впровадження нових підходів та методів підтримки відновлюваної енергії у воєнний та післявоєнний період необхідно мати дані про поточний стан відновлюваної генерації, а також інформацію про потужності відновлюваних джерел енергії (ВДЕ), які підключені до розподільчої мережі.

Тому, **метою роботи** є проаналізувати динаміку розвитку об'єктів альтернативної енергетики у розрізі їх приєднання до мереж передачі електричної енергії.

Основна частина. У роботі над інформаційною системою моніторингу стану та динаміки розвитку електростанцій на ВДЕ [1] вдалося зібрати інформацію про об'єкти ВДЕ, зокрема і дані щодо приєднання кожного об'єкта до розподільчих або магістральної мереж (ці дані були отримані внаслідок аналізу усіх РРА-договорів (Power Purchasing Agreement – довгострокові договори на купівлю електричної енергії з ВДЕ), що заключили виробники альтернативної генерації з Державним підприємством «Гарантований покупець» (ДП «Гарантований покупець») з 2019 по 2022 роки. Проте поки система не містить інформації про об'єкти альтернативної генерації приватних домогосподарств, що підписали договори купівлі-продажу електричної енергії з постачальниками універсальних послуг.

Розрахунки проводились для працюючих станцій (ті, що виробляли електричну енергію).

На рисунку 1 відображена динаміка зміни структури ВАД у розрізі типів мереж приєднання – високовольтні або розподільчі.

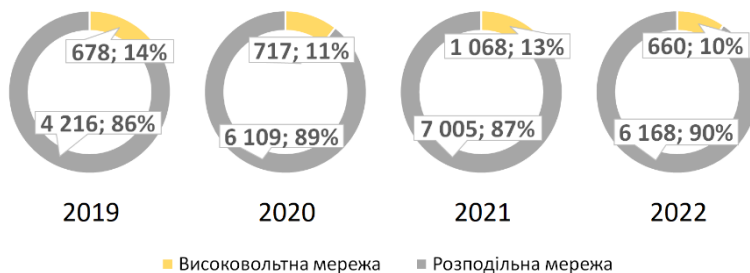


Рис. 1. Розподіл встановлених потужностей працюючих станцій альтернативної генерації у розрізі приєднання до мереж електропостачання за 2019-2022 роки, МВт

З рисунка 1 видно, що пікового етапу розвитку альтернативна генерація досягла у 2021 році.

Можемо спостерігати тенденцію до переважання підключення об'єктів альтернативної генерації до розподільчих мереж над високовольтними. Зокрема це пов'язано з невеликими обсягами встановлених потужностей ВАД (як показано на рисунку 2 встановлена потужність 98% від всієї кількості об'єктів ВДЕ менша за 50 МВт, разом з тим 3 з 5 станцій потужністю понад 100 МВт підключені до високовольтної мережі), відносною простотою та дешевизною приєднання до розподільчої мережі у порівнянні з приєднанням до високовольтних мереж.

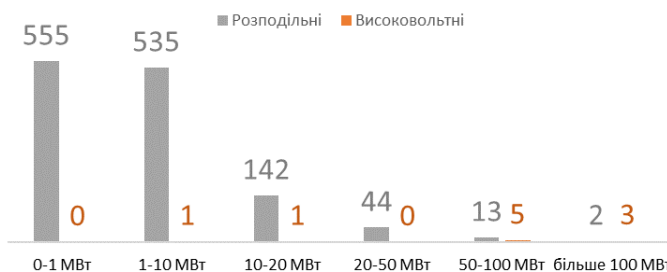


Рис. 2. Розподіл працюючих станцій на ВДЕ за розміром встановлених потужностей у 2021 році, шт

Об'єкти ВДЕ, що приєднані до високовольтних мереж, розташовувалися у Дніпропетровській, Львівській, Миколаївській, Херсонській та Хмельницькій областях. У всіх інших регіонах станції приєднані виключно до розподільних мереж, як показано на рисунку 3.



Рис. 3. Розподіл працюючих станцій на ВДЕ у розрізі приєднання до мереж за регіонами у 2021 році

Приєднання до мереж у розрізі джерел альтернативної генерації зображено на рисунку 4. Так станом на грудень 2021 87% від всіх потужностей були приєднані до розподільних мереж, зокрема 5532 МВт СЕС, 1263 МВт ВЕС, 350 МВт – інші

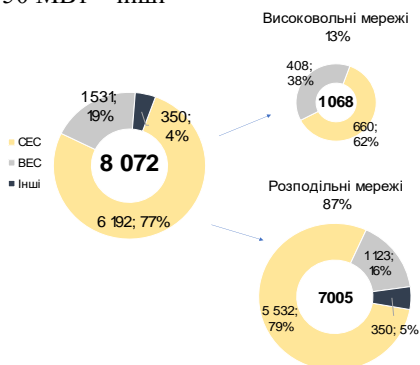


Рис.4. Розподіл встановлених потужностей працюючих станцій альтернативної генерації у розрізі джерел альтернативної енергії та приєднання до мереж електропостачання у 2021 році, МВт

У 2022 році у зв'язку з військовим вторгненням частина об'єктів альтернативної генерації зазнала руйнувань, пошкоджень або опинилася на окупованих територіях. Так переважна більшість встановлених наразі в країні об'єктів відновлюваної енергетики, зосереджені у південних та південно-східних областях України, де вже протягом останнього року ведуться активні

бойові дії. За різними оцінками експертів, станом на серпень 2022 року вже так чи інакше постраждало 30–40% ВДЕ у цих регіонах.

До прикладу, за даними Української вітроенергетичної асоціації, з початку широкомасштабної війни в Україні зупинено понад 3/4 вітроенергетичних потужностей, а 5 вітрових турбін в Херсонській області, що встановлені на Мирненській, Сиваській та Новотроїцькій вітроелектростанціях, сьогодні є знищеними. Через пошкодження 330 кВт лінії електропередачі в Мелітополі не працюють також майже 600 МВт вітроенергетичних потужностей у Запорізькій області. Понад 1 МВт біоенергетичних потужностей в Чернігові зазнали пошкоджень, в той час як біоенергетичні станції сумарною потужністю 2 МВт виявились на окупованих територіях Донецької області, а саме, в Волновасі та Маріуполі. На щастя, потужності малої гідроенергетики, переважно розташовані в західних областях України, не постраждали від бойових дій і продовжують постачати електроенергію. [2]

Як зображено на рисунку 5, станом на липень 2022 року до Об'єднаної енергосистеми України було підключено 6828 МВт працюючих станцій, 88% яких склали СЕС, 7% - ВЕС, 5% - станції, що виробляють електричну енергію з інших джерел. Структура станцій, приєднаних до розподільчих мереж, наступна: 5358 МВт – СЕС, 476 МВт – ВЕС, 334 МВт – інші.

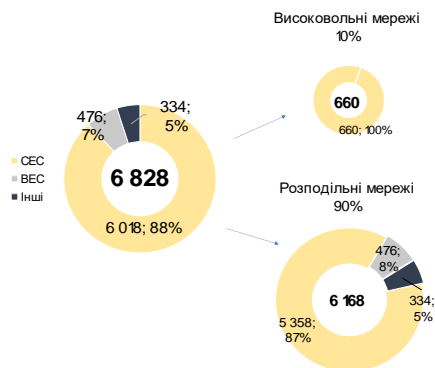


Рис.5. Розподіл встановлених потужностей працюючих станцій альтернативної генерації у розрізі джерел альтернативної енергії та приєднання до мереж електропостачання 2022 року, МВт

Як показано на рисунку 6 потужність уже 99% від всієї кількості об'єктів ВДЕ менша за 50 МВт. Внаслідок активних бойових дій були зруйновані великі потужності на півдні країни. Також бачимо зменшення станцій, що підключені до високовольтних мереж з потужністю більше 100 МВ.

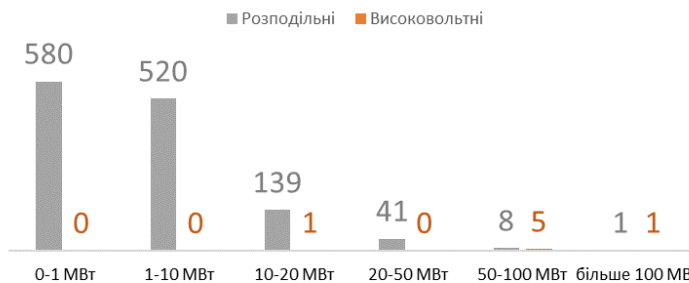


Рис. 6. Розподіл працюючих станцій на ВДЕ за розміром встановлених потужностей у 2022 році, шт

Станом на липень 2022 року структура підключень до мереж по регіонам України зображена на рисунку 7. До високовольтних мереж залишились приєднаними сонячні станції у Дніпропетровській, Львівській, Миколаївській, та Хмельницькій областях.



Рис. 7. Розподіл працюючих станцій на ВДЕ у розрізі приєднання до мереж за регіонами у 2022 році

Як показує дослідження, 90% потужностей ВДЕ підключені до розподільчих мереж. Тому розвиток відновлюваної енергії є однією з важливих складових шляху до децентралізованої енергетичної системи. Також і уряд заявляє про необхідність «створення мініелектростанцій та малих об'єктів генерації, імплементованих у наявну енергосистему» [3].

Ще одним кроком до розвитку розподіленої генерації та розвитку ВДЕ є впровадження віртуальних електростанцій. Віртуальна електростанція - це високотехнологічна система, яка одночасно комбінує електрику від кількох виробників та споживачів. Слід зазначити, що такі об'єкти споживачів та виробників повинні бути гнучкими в виробництві або споживанні

електроенергії. Віртуальна електростанція не втручається безпосередньо в процес виробництва, а регулює обладнання, яке надає підтримку енергосистемі при порушенні балансу між виробництвом та споживанням [4].

Додатково розглядається концепція створення сотової енергетичної мережі (СЕМ) для територіальних об'єднань [5]. СЕМ – це сукупність на певній території центрів генерації, зберігання енергії, з'єднаних між собою і з центрами споживання.

Висновки. Внаслідок збройної агресії Росії електроенергетична галузь України загалом і понад 1000 МВт потужностей ВДЕ потребують відновлення. Проте існуючі методи підтримки виробників ВДЕ є недостатніми.

Разом з тим одним з напрямків еволюції вітчизняної енергетики є розвиток децентралізованої енергетичної системи для забезпечення енергетичної незалежності та безпеки для громадян України. Результати досліджень показують, що близько 90% потужностей ВАД приєднані до розподільних мережами, а лише 10% - до високовольтних мережами. Відповідно, розвиток ВДЕ є важливою складовою розвитку розподільної генерації.

Отже, питання підтримки альтернативної генерації та розвитку розподіленої генерації є взаємопов'язаними, взаємодоповнюючими, актуальними і потребують подальших досліджень.

- [1] Я.П. Лукашевич, В.А. Євдокімов В.А. Євдокімов, *Elektron. model.* 2022, 44(5):90-101
- [2] Сектор відновлюваної енергетики України до, під час та після війни URL: <https://razumkov.org.ua/statti/sektor-vidnovlyuvanoyi-energetyky-ukrayiny-do-pidchas-ta-pislya-viyny> (дата звернення: 28.04.2023)
- [3] Побудова децентралізованої енергосистеми зробить її менш вразливою до ворожих атак, — Прем'єр-міністр, <https://www.kmu.gov.ua/en/news/pobudova-detsentralizovanoi-enerhosystemy-zrobyt-ii-mensh-vrazlyvoiu-do-vorozhykh-atak-premier-ministr>. (дата звернення: 28.04.2023)
- [4] Пантелєєва , І., Шматько , Н., & Шевченко , Є. (2023). ВІРТУАЛЬНІ ЕЛЕКТРОСТАНЦІЇ, ЯК РЕАЛІЗАЦІЯ РОЗПОДІЛЕНОЇ ГЕНЕРАЦІЇ ЕНЕРГІЇ. Collection of Scientific Papers «SCIENTIA», 143–145. URL: <https://previous.scientia.report/index.php/archive/article/view/751> (дата звернення: 28.04.2023)
- [5] V. Unighovsky, The concept of creating a cellular energy network for territorial associations, *Energy journal*, No20-21/1264/65 (17-19)

ЗАСТОСУВАННЯ АНСАМБЛІВ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ ДЛЯ ПРОГНОЗУВАННЯ НЕБАЛАНСІВ ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ В ОЕС УКРАЇНИ

Вступ. На часі задача прогнозування небалансів електроенергії є доволі актуальною. Адже, для забезпечення стабільності та надійності роботи енергетичних систем необхідно мати точні прогнози небалансів електричної енергії. Ці прогнози дозволяють планувати роботу ОСП в частині визначення необхідних обсягів резервів для балансування ОЕС України [1-3] на балансуєчому ринку та ринку допоміжних послуг [4], забезпечувати надійність роботи ОЕС України, а також дає змогу підвищити ефективність роботи учасників оптового та роздрібного ринку електричної енергії [4-6].

Результати досліджень щодо прогнозування небалансів в ОЕС України [7, 8] показали перевагу штучних нейронних мереж перед іншими моделями, зокрема і авто регресійними. Це обґрунтовує доцільність удосконалення методів прогнозування на основі нейронних мереж для прогнозування небалансів задля підвищення точності та стабільності результатів.

Метою дослідження є побудова ансамблю нейронних мереж задля підвищення точності прогнозування небалансів електроенергії в ОЕС України.

Матеріали і методи. Задля досягнення поставленої мети застосовано модель штучної нейронної мережі типу LSTM [9] з додатковою оптимізацією гіперпараметрів, а саме: кількості шарів `num_layers` [1; 2]; розмірності внутрішніх станів шарів `hidden_dim` [16; 32]; кроку навчання `lr` [0.01; 0.1].

Виконано випробовування моделей із різними довжинами вікна (4; 12; 24), яке переміщується по вхідним даним і збирає вхідні значення в кожен момент часу для прогнозування наступного значення. На основі можливих комбінацій цих моделей побудовано чотири ансамблі мереж (4+12; 4+24; 12+24; 4+12+24). Результати прогнозування ансамблів мереж визначені як середнє арифметичне результатів відповідних моделей.

Поділ вибірки даних є наступним: 95% – тренувальна вибірка, 5% – валідаційна вибірка, 5% - тестова вибірка (220 точок). На тренувальній вибірці проводиться навчання мережі, вибір моделі з оптимальними гіперпараметрами проводиться за результатами прогнозування на валідаційній вибірці, безпосередньо прогнозування проводиться на тестовій вибірці.

Прогнозування проведене для вибірок позитивних й негативних небалансів електроенергії ОЕС України на період 01.01.2021-02.01.2022 (8800 точок), горизонт прогнозування 220 точок, кількість передісторії – 4172 точки (півроку), тобто 40 дослідів для кожної моделі, що відрізняються значенням довжини вікна (4; 12; 24).

Ретроспективні дані про позитивні й негативні небаланси ОЕС України отримані з офіційного сайту ОСП – НЕК «Укренерго».

Результати. Порівняльний аналіз результатів проведено за допомогою середньоквадратичної похибки RMSE. На рис. 1 наведено гістограми похибок прогнозування позитивних і негативних небалансів за увесь період дослідження.

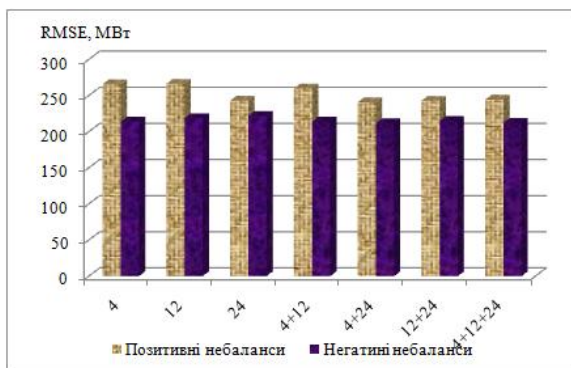


Рис. 1. Гістограми значень похибки RMSE позитивних й негативних небалансів електроенергії кожної моделі

Згідно рисунку 1 найкращі результати для обох розглянутих вибірок небалансів має ансамбль мереж «4+24».

На діаграмах (рис. 2) наведено відсоткову частку мінімальних значень похибки RMSE кожного із 40 дослідів протягом досліджуваного періоду для кожної моделі й ансамблю.

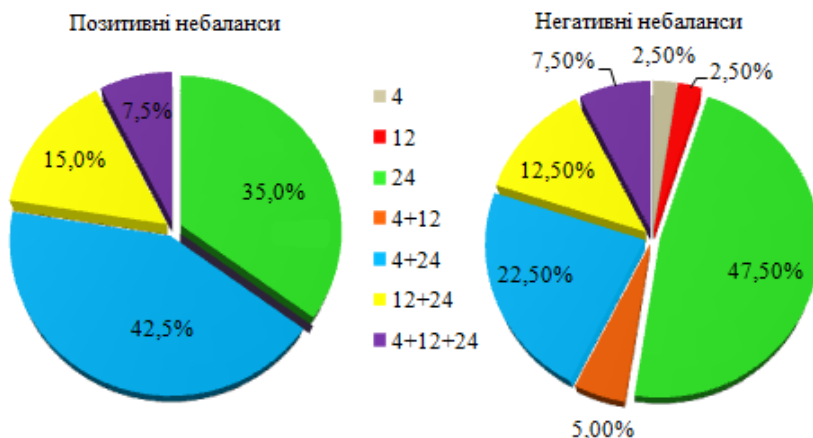


Рис. 2. Діаграми частки мінімальних значень похибки RMSE від загальної кількості дослідів

Зважаючи на результати рис. 2, доцільним було б проводити пошук оптимальної моделі для кожної порції даних серед моделей «24», «4+24» й «12+24». Що дозволить підвищити стабільність результатів.

Висновки. Результати дослідження моделей із різними довжинами вікна та їх ансамблів показали ефективність застосування ансамблів мереж з метою підвищення точності результатів прогнозування небалансів електроенергії. Також, під час аналізу результатів потребу та шляхи у вдосконаленні розробленої моделі за рахунок ускладнення алгоритму вибору застосовуваної моделі, що є основою для майбутніх розробок.

- [1] Кириленко О.В., Павловський В.В., Блінов І.В. Науково-технічне забезпечення організації роботи ОЕС України в синхронному режимі з європейською континентальною енергетичною системою ENTSO-E. Технічна електродинаміка. 2022. № 5, С 59–66. DOI: <https://doi.org/10.15407/techned2022.05.059>
- [2] Блінов І.В., Парус С.В., Мірошник В.О., Шиманюк П.О., Сичова В.В. Модель оцінки доцільності переходу промислових споживачів до погодинного обліку електричної енергії на роздрібному ринку. Енергетика: економіка, технології, екологія. 2021. № 1. С. 88-97. <https://doi.org/10.20535/1813-5420.1.2021.242186>
- [3] Олефір Д.О., Бабіч В.Ю., Блінов І.В. Актуальні проблеми забезпечення ОЕС України ресурсами регулювання частоти та потужності. Енергетика: економіка, технології, екологія, 2021, № 3, С. 39-46. DOI: <https://doi.org/10.20535/1813-5420.3.2021.251196>
- [4] Про затвердження Правил ринку: Постанова НКРЕКП № 307 від 14.03.2018
- [5] Парус С.В., Блінов І.В. Складові імітаційної моделі процесів ціноутворення на ринку електричної енергії України. Праці Інституту електродинаміки НАН України, 2019, Вип. 53. С. 28-34. DOI: <https://doi.org/10.15407/publishing2019.53.028>
- [6] Борукаєв З. Х. Моделі та засоби автоматизації систем організаційного управління енергоринком: монографія / З. Х. Борукаєв, І. В. Блінов, К.Б. Остапченко, О. А. Чемерис, В. В. Шкарупило ; за заг. ред. З. Х. Борукаєва. Вінниця : ГО «Європейська наукова платформа», 2022. 122 с. ISBN 978-617-8037-82-6, DOI: 10.36074/mtzasoye-monograph.2022
- [7] Сичова В. Прогнозування добових графіків сумарних небалансів електричної енергії в ОЕС України. Технічна електродинаміка. 2022. № 4. С 59–63. DOI: <https://doi.org/10.15407/techned2022.04.059>
- [8] Blinov I., Miroshnyk V. and Sychova V. Comparison of models for short-term forecasting of electricity imbalances. 2022 IEEE 8th International Conference on Energy Smart Systems (ESS). IEEE, 2022. DOI: <https://doi.org/10.1109/ESS57819.2022.9969288>
- [9] Sepp Hochreiter, Jürgen Schmidhuber. Long Short-term Memory. Neural computation. 1997. Vol. 9. Pp. 1735–80.

ГРУПОВА СИНХРОНІЗАЦІЯ ДЕРЕВОПОДІБНИХ МАШИН ПАРНОСТІ

Проблематика групової синхронізації деревоподібних машин парності (ДМП) вже підіймалась у попередніх роботах [1]. Використання ДМП (рис. 1) передбачає взаємну синхронізацію нейронних мереж з подальшим створенням ключа шифрування лише для двох кінцевих користувачів, проте в сучасних реаліях часто виникає необхідність створення групового ключа шифрування. Виходом із цієї ситуації є механізм групової синхронізації з використанням машин парності дерева. Механізми групової синхронізації представлені в роботі [4].

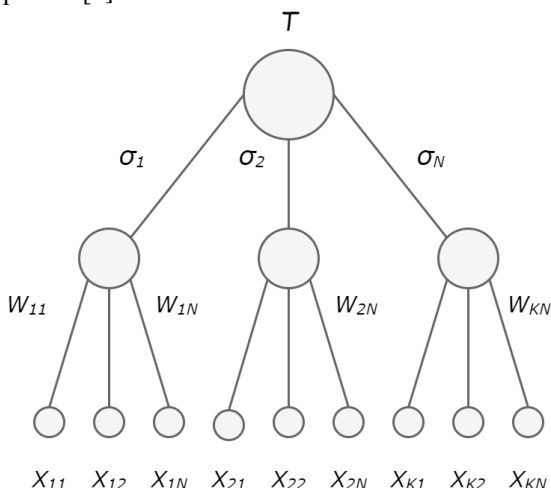


Рис. 1. Структура ДЕРЕВОПОДІБНИХ МАШИН ПАРНОСТІ

Суть алгоритму полягає в тому, що N ДМП повинні бути синхронізовані разом, і вони представлені M кількістю листків повного дерева парності. Існує два підходи до колективної синхронізації ТРМ:

- двійкове дерево з вибором (BTWE);
- двійкове дерево з обміном (BTWS).

Зрештою, обидва дають бажаний результат, але приходять до нього різними шляхами.

За допомогою підходу BTWE N ДМП представлено M листами, на кожній ітерації алгоритму J дерево парності ділиться на 2^J і взаємне навчання застосовується для кожної пари листів, що мають одного батька. На наступному кроці J збільшується, і в кожному піддереві ТРМ вибираються вузли, які також використовують алгоритм взаємного навчання, а потім надсилають біти своїм підгрупам.

Такі ітерації тривають до тих пір, поки алгоритм не досягне кореня,

після чого завершується. Якщо корінь синхронізований, то всі ТРМ також синхронізовані і мають однакові вагові вектори [5].

У підході BTWS (рис. 2) алгоритм взаємного навчання застосовується між кожними двома сторонами, що мають одного і того самого батька в структурі парного дерева. Якщо $mdepth$ є максимально можливою глибиною бінарного дерева, а $cdepth$ є глибиною, на якій алгоритм знаходиться в заданий момент часу. Починаючи з $depth = mdepth - 1$, алгоритм взаємного навчання застосовується між кожною парою листків (ТРМ), які належать одному батьківському елементу. Після досягнення синхронізації виконується перехід на вищий рівень ($cdepth = cdepth - 1$), і між усіма піддеревами цього $cdepth$ між правими листами правої та лівої гілок застосовується механізм перестановки. Як тільки значення $cdepth$ стане рівним нулю, усі листи (ТРМ) будуть синхронізовані [4].

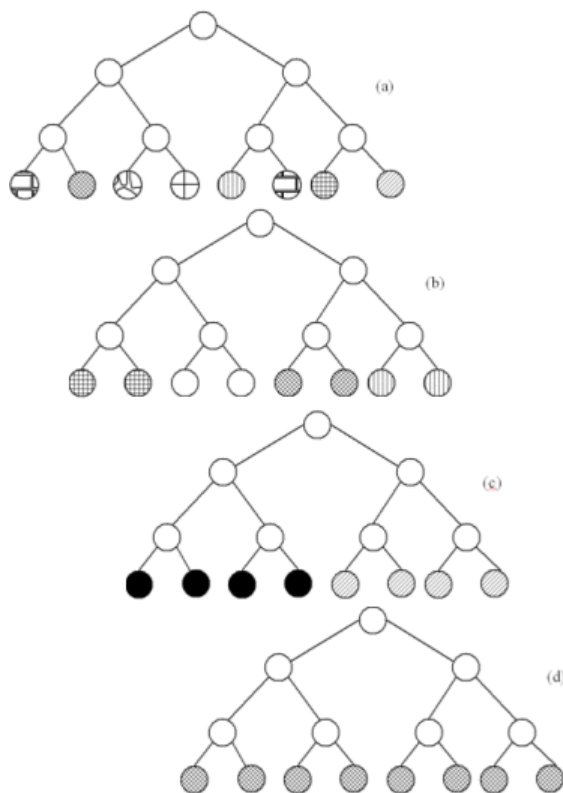


Рис. 2. Послідовність нейронної синхронізації між чотирма ТРМ за допомогою BTWS

Представлені методи використовують прості обчислення і дозволяють

швидко створити секретний ключ групи. Однак ці алгоритми дуже вразливі у випадках, коли зломисник може взяти участь у протоколі та отримати секретний ключ. Виходячи з цього, існує потреба в схемі автентифікації для захисту групи від таких атак.

Для побудови схеми автентифікації передбачається, що група отримує секретний пароль, який можна використовувати для автентифікації протоколу обміну. Цей пароль можна зіставити з деяким публічним параметром нейронної криптографії, який стає секретним і, отже, забезпечує відповідну конфіденційність.

У [6] була запропонована схема автентифікації, яка зберігає шаблони введення в секреті. Таким чином, лише сторони, які знають секрет, можуть синхронізуватися разом. Також у [4] була запропонована схема, у якій пароль використовувався як початкове число для генератора випадкових чисел, який шифрує вихідні біти так само, як [6,7].

В рамках даної роботи було оцінено можливість використання алгоритмів VTWE і VTWS як способу вирішення проблеми групової синхронізації нейронних мереж. Використання цих підходів може вирішити проблему групової синхронізації, але складність алгоритмів логарифмічно пропорційна кількості сторін, які необхідно синхронізувати разом. З чого можна зробити висновок, що зі зростанням розміру групи буде збільшуватися і час синхронізації абонентів групи. Також з'являється ймовірність злому шляхом підключення ДМП зломисника до участі у протоколі, що несе додаткові ризики, а використання схеми автентифікації для групи несе за собою додаткове навантаження на систему. Тож використання алгоритмів VTWE і VTWS для групової синхронізації лише частково доцільно.

- [1] Aleksandrov M., Y. Bashkov, "Factors Affecting Synchronization Time of Tree Parity Machines in Cryptography," 2020 IEEE 2nd International Conference on Advanced Trends in Information
- [2] Aleksandrov M., "Confirmation of Mutual Synchronization of the TPMs Using Hash Functions," 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory (ATIT), 2021, pp. 80-83, doi: 10.1109/ATIT54053.2021.9678779.
- [3] Aleksandrov M. "Approaches to confirming mutual synchronization in tree-like parity machines", Computer science, cybernetics and counting technique, №1 (34), Donetsk National Technical University, 2022, pp. 65-70, ISSN 1996-1588
- [4] Allam A. M. Group key exchange using neural cryptography with binary trees / Ahmed M. Allam, Hazem M. Abbas // IEEE CCECE. – 2011. – P. 783-786.
- [5] Volkmer M. Entity Authentication and Authenticated Key Exchange with Tree Parity Machines / M. Volkmer, S. Wallner // – 2012. – Vol.112. – P. 1–6.
- [6] Allam A. Improved Security of Neural Cryptography Using Don't-Trust-My-Partner and Error Prediction / A.Allam, H.Abbas // International Joint Conference on Neural Networks (IJCNN09) – 2009. – P. 121-127.
- [7] Volkmer M. Entity Authentication and Authenticated Key Exchange with Tree Parity Machines / M. Volkmer, S. Wallner // – 2012. – Vol.112. – P. 1–6

ЄВРОПЕЙСЬКІ ПІДХОДИ БІОКОНВЕРСІЇ ОРГАНІЧНИХ ВІДХОДІВ У ДИГЕСТАТ ТА БІОВОДЕНЬ ІЗ ЗАСТОСУВАННЯМ СУЧАСНИХ БІОТЕХНОЛОГІЙ

У цивілізованому світі, нажаль, одна третина продуктів харчування (приблизно 1,3 мільярди тонн), яка призначена для споживання людиною, втрачається щороку внаслідок тривалого зберігання та втрати ліквідного стану. Фрукти, овочі, а також коренеплоди мають найвищий відсоток втрат через невідповідне зберігання, і як наслідок, розвитку різних хвороб, які спричиняють умовно патогенні мікроорганізми, що становить 40–50% збитків (520–650 млн. тонн) світових кількісних втрат їжі та відходів на рік. В ЄС харчові відходи складають 89 млн. тонн їжі на рік (39% цих харчових відходів утворюються під час виробничих процесів), тоді як загальне виробництво сільськогосподарських відходів (залишки врожаю або частини культурних рослин, які не споживаються в їжу) в ЄС становить 367 млн. тонн на рік. В країнах ЄС було проведено кілька досліджень щодо ефективного використання відходів агропромисловості, як потенційної сировини для виробництва продукції з доданою вартістю. Більшість цих досліджень було проведено в країнах, чия економіка значною мірою залежить від сільського господарства [1]. У країнах ЄС нові директиви наголошують на поняттях «біоекономіка» та «біопереробка», згідно з якими відходи однієї галузі можуть служити сировиною для іншої. Багато відходів агропромислового виробництва є лігноцелюлозними за своєю природою; вони, як правило, містять багато полісахаридів, таких як: целюлоза та геміцелюлоза, а також лігнін, крім того, містять інші поживні речовини, такі як білки, ліпіди, пектин, вітаміни, мікро-макроелементи і поліфеноли (табл.1). Харчові відходи є глобальною проблемою, яка завдає значної шкоди навколишньому середовищу та призводить до значних економічних втрат у всьому світі. Таким чином, використовуючи відходи агропромислового комплексу, можна вирішити одразу дві проблеми – це безпечна утилізація самих відходів та використання їх для виробництва таких важливих продуктів як дигестат та біоводень [2].

Велика кількість відходів агропромислового комплексу підходить для переробки методом твердофазної ферментації, тому що має значні переваги з точки зору стійкості біосистеми та її контролюваності. Такий метод переробки відходів відрізняється від інших екологічністю та низькими собівартістю продукції. Масовий та енергетичний баланс є важливими параметрами цього процесу, пов'язаними з контролем основних технологічних параметрів ферментації (бродиння відходів за участі біоагентів). Складність цього процесу зумовлюється особливостями тепло- та масообміну під час твердофазного бродиння, що і являє собою основну

перешкоду, яка обмежує його застосування для переробки інших типів відходів.

Таблиця 1

Хімічний склад важливих відходів агропромислового комплексу, %

Відходи	Вуглевод	Сира клітковина	Зола	Пек-тин	Жир	Білок	Лігнін
Жом буряку	66,48	-	8,80	0,7	-	2,3	17,79
Рисові висівки	14,1	26,9	3,4 - 8,1	-	30,4	38,2	25,63
Пшеничні висівки	56,8	33,4 - 63,0	3,9 - 8,10		3,5 - 3,9	13,2 - 18,4	5,6
Відход картоплі	55,53	60,46	1,30	0,3	2,29	0,2	23,90
Зерно пивоварне	79,9	3,3	7,9	-	-	2,4	30,48
Яблуневі вичавки	48,0 - 62,0	-	4,7 - 51,1	1,0	-	3,9 - 5,7	23,5
Сирі оливкові вичавки	34,8	-	6,6	-	16,65	0,4	43,2
Бананова шкірка	79,0	9,3	2,7	-	3,0	0,6	6,4 - 9,6
Цитруси	30	-	1,7	14,4	-	7,9	1

Однак, сучасні наукові нароби в технології переробки відходів біотехнологічним методом дозволяють припустити, що фактор, який називається механічним індексом (Imp), може бути використаний, як допоміжний засіб для характеристики фізичного стану та оцінки властивостей середовища, надаючи вищий рівень контролю над процесом бродіння відходів за участі складного консорціуму мікроорганізмів, які реалізують процес бродіння. Індекс (Imp) є продуктом фізичних властивостей твердофазної ферментації, а саме, таких показників процесу як - адгезія та пружність. Під час протікання різних етапів бродіння, індекс (Imp) може корелюватися (позитивно чи негативно) з теплопровідністю, водоутримувальною здатністю, газопроникністю, температуропровідністю та співвідношенням біомаси до твердої фази, враховуючи, що перелічені показники змінюються протягом процесу бродіння. Ці фізичні властивості безпосередньо впливають на тепло- та масообмін, що, у свою чергу, визначає ефективність процесу ферментації. Таким чином, індекс (Imp) може бути успішно використаним для визначення та оцінки фізичних властивостей середовища, а також, для більш жорсткого контролю за якістю дигестату.

В рамках підтримки Європейського курсу щодо переробки відходів з урахуваннях їх виду та рівня небезпеки на державному та законодавчому рівнях, нещодавно прийнятий Закон України «Про управління відходами»

[3], демонструє перш за все ще й економічну складову в рамках циркуляційної економіки, котра передбачає стимулювання поширення зелених біотехнологій відносно переробки органічних біомас в дигестат та біогаз.

Україна разом із багатьма країнами світу приєдналася до виконання договору щодо участі в Енергетичному співтоваристві (підписано протокол від 24.09.2010 р. у Скоп'є – Македонія), який є ратифікований Законом України № 2787-VI від 15.12.2010 р. [4]. Враховуючи вище вказане, дана робота проведена в межах проекту «Clean Energy Technologies and Energy Efficiency: the EU Experience», що реалізується в рамках гранту Європейського Союзу за програмою «Jean Monnet Modules Erasmus+» (Грантова угода Project 101047602 – EnergyC) та присвячена біотехнології переробки овочевих відходів: бурякових, картопляних та морквяних із використанням сучасних ЕМ-технологій. У якості препарату використано український запатентований продукт «Байкал-ЕМ1». Завдяки використанню даного препарату, під час біоконверсії органічних відходів, вдалося отримати якісний дигестат та біоводень за 7 діб ферментації (в термостатних умовах, при температурі культивування 35⁰ С). Експериментами встановлено, що полив, отриманим дигестатом картоплі (під час вирощування), упереджує розвиток патогенних культур, які визивають овочеві хвороби та порчу продукту під час зберігання.

- [1] Ravindran R, Hassan SS, Williams GA, Jaiswal AK. A Review on Bioconversion of Agro-Industrial Wastes to Industrially Important Enzymes. Bioengineering (Basel). 2018 Oct 28;5(4):93. doi: 10.3390/bioengineering5040093. PMID: 30373279; PMCID: PMC6316327.
- [2] Кудря С. О. Відновлювані джерела енергії: монографія. Київ: Інститут відновлювальної енергетики НАНУ, 2020. 392 с.
- [3] Про управління відходами: Закон України № 2207-1-д від 20.06.2022. URL:<https://www.rada.gov.ua/news/razom/224307.html>.
- [4] Про ратифікацію Протоколу про приєднання України до Договору про заснування Енергетичного Співтовариства: Закон України № 2787-VI від 15.12.2010. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/T102787.html.



**Co-funded by
the European Union**

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

ПІДХОДИ ДО МОДЕЛЮВАННЯ ЗАГРОЗ КІБЕРБЕЗПЕЦІ У ЗВ'ЯЗКУ З МАСОВИМИ ВІДКЛЮЧЕННЯМИ ЕЛЕКТРОПОСТАЧАННЯ ТА ПОТЕНЦІЙНІ ЗАХОДИ ПРОТИДІЇ

Актуальність дослідження загроз кібербезпеці у зв'язку з масовими відключеннями електропостачання зумовлена подіями, пов'язаними з російсько-українською війною, а саме її етапом з листопада по лютий 2022-2023 років. Масові цілеспрямовані руйнування енергосистеми призвели до небаченої в новітній історії енергокризи, усі грані впливу якої на всі аспекти функціонування держави потребують детального вивчення. Подібна ситуація може складатись в майбутньому, як під час військових конфліктів, так і під час природних катаклізмів [1].

Досліджувана проблематика є відносно новою і не висвітленою ані в рамках наукових досліджень, ані в рамках інженерних рекомендацій щодо практичних засобів протидії. Якщо роботи щодо дослідження впливу подібних масштабних факторів на економіку та господарство в цілому існують у відкритому доступі, дослідження ефектів другого порядку, зокрема впливу на кібербезпеку поки що потребують додаткової роботи. З наведених вище причин, необхідність висвітлення прихованих ризиків та загроз вважається важливою задачею з точки зору керування ризиками підприємств. На основі проведених досліджень можливе здійснення прийняття рішень щодо контрзаходів.

Основною метою дослідження є ідентифікація загроз кібербезпеці усередненої ІКС в умовах перебоїв електропостачання, врахування даних факторів під час моделювання загроз та в перспективі надання рекомендацій щодо контрзаходів. Дослідження визначеної проблематики відбувається шляхом аналізу прямих шляхів впливу відключень електропостачання на усереднену ІКС, ідентифікації впливу на контролі та процеси забезпечення кібербезпеки зокрема, визначення потенційних шляхів застосування відомих методологій моделювання загроз, та ідентифікації можливих засобів протидії.

За моделлю STRIDE масове відключення електропостачання класифікується лише за категорією Denial Of Service. В свою чергу, похідні загрози, пов'язані з, наприклад, відключенням контролів безпеки або втратою оперативності реагування, можуть класифікуватись як Tampering або Repudiation [2]. Основними ідентифікованими загрозливими ефектами, які мають бути враховані під час моделювання загроз у зв'язку з масовими відключеннями електропостачання визначені:

- Недоступність та простій бізнес-сервісів та застосунків, відключення обладнання та систем;
- Необхідність додаткових витрат ресурсів команд підтримки та безпеки;
- Відключення контролів безпеки;

- Погіршення спостережності внаслідок перерв у постачанні журналів;

Розглядаючи дані проблеми кібербезпеки, дійшли наступних висновків щодо потенційних шляхів протидії загрозам.

Найефективнішим рішенням щодо протидії загрозам відключень електропостачання в ІКС представляється встановлення обладнання для резервного електропостачання — UPS та генераторів. Важливим аспектом в такому випадку вважаємо наявність на обладнанні резервування можливості журналювання свого стану та відправки журнальних даних для аналізу та збереження. Даний функціонал дозволяє проводити кореляцію втрати надходження подій з об'єкту з подією розрядження акумуляторів резервного живлення. Таким чином зменшується навантаження на операційну команду безпеки, вирішується проблема додаткового вичерпання ресурсів сил моніторингу та реагування, зберігається спостережність інформації. Втрата зв'язності з об'єктом ІКС, втрата журналів від такого об'єкту, або зафіксована перерва у його функціонуванні не має розглядатись як інцидент безпеки лише у випадках прописаних в порядку виключення та, зокрема, у разі виявлення повідомлення від відповідного джерела резервного живлення про низький заряд акумуляторів, або, у разі використання генератора з можливістю віддаленого технічного моніторингу, низький рівень палива.

Для забезпечення безперервного зв'язку об'єктів ІКС з центром, де проводиться накопичення та аналіз журналів, а також центром керування ІКС необхідне забезпечення резервного каналу зв'язку, стабільного та достатнього для здійснення, як мінімум, задач моніторингу та керування системою відповідно. В якості такого каналу можуть розглядатись такі технології, як супутниковий зв'язок або ADSL — вибір конкретної технології залежить від можливостей реалізації в поточних умовах, але головним критерієм має залишатись стабільність та гарантованість зв'язку у ситуації відключення електроживлення протягом періоду, як мінімум, гарантованого системами резервування на об'єкті ІКС. Забезпечення такого каналу гарантує, що центр, в якому проводиться накопичення та аналіз журналів зможе отримати необхідні дані для забезпечення спостережності, про що йшлося вище.

Винесення об'єктів ІКС на потужності стабільного та розподіленого хмарного провайдера дозволяє зменшити вимоги до забезпечення резервування електроживлення об'єкту, а також усунути проблему відключення контролів безпеки, у разі перенесення відповідних контролів у "хмару". В загальному випадку не представляється можливим перенесення всіх частин ІКС на потужності хмарного провайдера — певна частина буде фізично локалізуватись там, де знаходиться персонал, що робить дані частини вразливими до відключень електропостачання. Саме тому, можемо дійти двох висновків щодо застосовності "хмарного переходу" для подолання проблеми відключень електропостачання. Перший — перенесення об'єктів ІКС на будь-яку зовнішню платформу не вирішує проблему масових відключень для інфраструктури повністю, хоча і дозволяє нівелювати декілька вище названих

ризиків. Подібні заходи в будь-якому випадку вимагають додаткових вкладень у резервування електропостачання для “не-хмарних” об’єктів. Другий висновок полягає в тому, що чим більше внутрішніх сервісів є винесеними за межі периметру ІКС на потужності хмарного провайдера, тим більше значення отримує канал зв’язку, що забезпечує комунікацію “наземних” сервісів з “хмарними”. Втрата зв’язку, що є одним з основним джерелом загроз в ситуації масових відключень електропостачання, в таких умовах призведе до більш серйозних порушень в роботі системи. Таким чином, резервування каналів зв’язків представляється пріоритетною задачею для забезпечення доступності та нормального режиму функціонування для “гібридних” ІКС, тобто таких, частина компонентів яких дислокується на потужностях хмарних провайдерів.

- [1] КИБЕРАТАКИ, АРТИЛЕРІЯ, ПРОПАГАНДА Загальний аналіз вимірів російської військової агресії [Електронний ресурс]: Державна служба спеціального зв’язку і захисту інформації України. – Режим доступу: <https://cip.gov.ua/services/cm/api/attachment/download?id=50692>
- [2] Habib, S., Khan, I.A., & McClean, S. (2017). STRIDE-based threat modeling for cyber-physical systems. Queen's University Belfast.

ЗАСТОСУВАННЯ МЕТОДІВ ПРОГНОЗУВАННЯ ДЛЯ ВИЗНАЧЕННЯ ОЧІКУВАНИХ ЗНАЧЕНЬ ВТРАТ В РОЗПОДІЛЬНИХ МЕРЕЖАХ

На сьогоднішній день в енергосистемі України втрати електроенергії при передачі можуть досягати 20%, при тому, що в більшості країн даний показник втрат знаходиться в межах 4-6% [1]. Це все зумовлено розвитком різних сегментів ринку, та неточними прогнозами навантажень для цих сегментів. Якщо прогнозування буде неточним, то виникне значна різниця між виробництвом енергії та споживанням, що призведе до необхідності докуповувати енергію на балансуєчому ринку електроенергії. Відповідно це збільшує вартість витрат на електроенергію. Враховуючи, що в електричних мережах втрати електроенергії розраховуються досить грубо, за рахунок коефіцієнтів, що визначаються у дні зимового та літнього піків навантаження.

Ринок «на добу наперед» являється сегментом ринку на якому здійснюється купівля та продаж електричної енергії на наступний день проведення торгів на добу за вільними цінами [2].

Зважаючи на необхідність прогнозування навантаження було запропоновано підхід щодо використання методів прогнозування для визначення очікуваного значення втрат електричної енергії в мережах. В якості методів прогнозування використовувались штучні нейронні мережі.

Для зменшення вартості втрат, запропоновано використання сучасних методів прогнозування на основі штучних нейронних мереж глибинного навчання для розрахунку та прогнозування втрат електричної енергії. Для перевірки ефективності визначення очікуваних значень втрат електричної енергії було розроблено архітектури штучних нейронних мереж глибинного навчання, прогнозні дані яких використовувались для розрахунку втрат електроенергії.

Для прогнозування навантаження вузлів використано дві нейронні мережі. Перша мережа, для прогнозу усіх вузлів описана в [3], є рекурентною нейронною мережею типу LSTM з комбінованою архітектурою, що складається з рекурентного модуля LSTM та багат шарового перцептронну з двома прихованими шарами, де в якості активаційної функції використовується SELU. Друга мережа, розроблена в інституті електродинаміки НАН України, є мережею eResNet [4] і складається з трьох автокодувальних блоків з обхідними з'єднаннями та звичайного багат шарового перцептронну для прогнозу кожного вузла окремо. Особливістю даної архітектури є однакова кількість вхідних та вихідний нейронів.

Обидва методи прогнозування були адаптовані під використання ретроспективних даних. Алгоритм оптимізації ADAM [5] використовується

для навчання обох алгоритмів.

Для визначення очікуваних значень втрат електроенергії були використані ретроспективні дані одного з ОСП України, які охоплювали період з 2017 по 2019 роки з 15ма вузлами навантаження. З яких було використано 14 вузлів навантаження для формування тестової енергосистеми та розрахунку втрат.

В якості основи для побудови тестової електричної мережі було використано схему CIGRE [6] середнього рівня напруги, яка широко використовується для досліджень режимів електричних мереж.

Для аналізу та моделювання електричних мереж було використано мову програмування Python та бібліотеку Pandapower для аналізу даних. Дана бібліотека має велику кількість різних моделей електричних мереж, тестових систем та прикладів енергосистем CIGRE.

Тестова мережа має 14 вузлів, 18 джерел навантаження і складається з двох трансформаторів потужністю 40 МВА з напругою 110/20 кВ., 14 ліній серед яких 12 кабельних ліній та дві повітряні лінії, та перемикач. Усі елементи які використовуються в даній мережі є елементами бібліотеки Pandapower.

Враховуючи що дана схема побудована на основі реальної європейської мережі, вона значно відрізняється за складом навантаження та параметрами мережі України, тому для коректної роботи алгоритму розрахунку втрат було виконано адаптацію розрахункової схеми задля використання наявних ретроспективних даних.

Зважаючи на те що величина середнього рівня напруги в енергосистемах України становить 10-35 кВ для достовірної оцінки визначення втрат електричної енергії. Було виконано адаптацію тестової мережі відповідно під середній рівень напруги енергосистем України. Для цього було замінено трансформатори, та частину повітряних ліній.

В таблиці 1 наведено замінені елементи мережі. Зважаючи що в бібліотеці pandopower лінії з перерізом більше 150 мм для 10кВ відсутні для ефективної роботи було використано лінії для 20 кВ.

Ретроспективні дані вузлового навантаження були розділені на дві частини: навчальну та тестову вибірки. Навчальна вибірка містить усі значення вузлового навантаження, за винятком останніх 744 значень, які були збережені для тестування.

Для оцінки точності представлених підходів використовувався функція похибки MAPE.

Таблиця 1

Елементи мережі

Назва елемента	Тип елемента	Кількість
Трансформатори	40 MVA 110/10 kV	2
Повітряні лінії	243-AL1/39-ST1A 110.0	4
	184-AL1/30-ST1A 20.0	2
	149-AL1/24-ST1A 10.0	9

Результати визначення очікуваних значень втрат з застосуванням прогнозних значень вузлового навантаження та методів прогнозування представлені в таблиці 2.

Таблиця 2

Похибки визначення втрат електричної енергії

Метод визначення втрат	Величина похибки MAPE, %
Розрахунок втрат на основі прогнозу вузлового навантаження	8,70
Розрахунок втрат на основі прогнозу вузлового навантаження кожного вузла окремо	6,56
Прогноз втрат електричної енергії	7,00
Визначення втрат електричної енергії за коефіцієнтами втрат	18,72

За результатами дослідження визначено що методи прогнозування дозволяють зменшити величину очікуваних значень втрат та зменшити похибки втрат ніж при визначенні їх за коефіцієнтами. Також визначення втрат електричної енергії з використанням прогнозних значень вузлового навантаження демонструє меншу похибку ніж при прогнозуванні усіх вузлів разом. Це може бути пояснене різними взаємозв'язками між вузлами навантаження.

Також на величину втрат електричної енергії впливає зміна опору в лініях електропередач, яка в свою чергу залежить від багатьох зовнішніх факторів таких як температура навколишнього середовища, вологість, швидкість вітру, зміна довжини ліній деформацією проводів внаслідок дії вітрових навантажень та ожеледиці.

- [1] Блінов І.В., Мірошник В.О., Шиманюк П.В. Оцінка вартості похибки прогнозу «на добу наперед» технологічних втрат в електричних мережах України. Технічна електродинаміка. 2020. №5 С. 70-73.
- [2] Блінов І.В. Проблеми функціонування та розвитку нової моделі ринку електричної енергії в Україні. Вісник НАН України. 2021. №3. С.20-28.
- [3] Шиманюк П.В., Мірошник В.О., Блінов І.В. Визначення втрат електричної енергії на основі прогнозів вузлового електричного навантаження. Енергетика: економіка, технології, екологія. 2022. №3. С.38-43.
- [4] П.О. Черненко, В.О. Мірошник Короткострокове прогнозування електричного навантаження електропостачальної компанії з використанням штучної нейронної мережі глибинного навчання. Праці Інституту електродинаміки НАН України. 2018р. № 50. С. 5-11.
- [5] D.P. Kingma, J. Ba Adam. A Method for Stochastic Optimization. Proc. of the 3rd International Conference on Learning Representations (ICLR).
- [6] “Benchmark Systems for Network Integration of Renewable and Distributed Energy Resources”, ELECTRA, 2014

О.О. Бакалинський, Д.В. Пахольченко, Д.О. Нагорний

МЕТОДИКА ВИЗНАЧЕННЯ КАТЕГОРІЇ (РІВНЯ) КРИТИЧНОСТІ КІБЕРІНЦИДЕНТУ/КІБЕРАТАКИ

Масштаб, частота та вплив кіберінцидентів зростають та становлять основну загрозу для функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем та інших об'єктів кіберзахисту, особливо з ведення ворогом повномасштабної збройної агресії проти України. Такі інциденти можуть перешкоджати здійсненню господарської діяльності, спричинити значні фінансові втрати, підірвати довіру користувачів та завдати значної шкоди економіці України.

Одним із чинників здатності держави забезпечувати захищеність власних ресурсів та активів в умовах політичної кризи та триваючої війни є спроможність забезпечувати кіберзахист власних інформаційних ресурсів, в тому числі тих, що належать до об'єктів критичної інформаційної інфраструктури.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» суб'єкти забезпечення кібербезпеки у межах своєї компетенції здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків [1].

Нещодавно Кабінетом Міністрів України затверджено Порядок реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі [2], який визначає процедури реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі (далі – кіберінциденти/кібератаки) та категорії (рівні) їх критичності.

Порядок реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі увібрав у себе етапи реагування на кіберінциденти/кібератаки, що були запропоновані авторами у попередніх публікаціях [3].

Відповідно до зазначеного Порядку, суб'єкти забезпечення кібербезпеки для забезпечення пропорційності та співрозмірності подальших заходів з кіберзахисту, здійснюють виявлення кіберінциденту/кібератаки та визначають їх критичність за шістьма категоріями (рівнями): рівень 0 некритичний (білий), рівень 1 низький (зелений), рівень 2 середній (жовтий), рівень 3 високий (помаранчевий), рівень 4 критичний (червоний), рівень 5 надзвичайний (чорний) [2].

Згідно із постановою Кабінету Міністрів України [2] Адміністрації Держспецзв'язку постановлено завдання затвердити методичні рекомендації щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, які у тому числі повинні містити рекомендації щодо визначення суб'єктами забезпечення кібербезпеки категорії (рівня) критичності кіберінциденту/кібератаки.

Відповідно авторами пропонується методика визначення категорії

(рівня) критичності кіберінциденту/кібератаки, яка заснована на поєднанні Посібника з усунення інцидентів комп'ютерної безпеки (NIST SP 800-61 Rev.2: Computer Security Incident Handling Guide) [3] та Національного плану реагування на кіберінциденти, виданого Агентством з кібербезпеки та захисту інфраструктури (CISA) [4], та в подальшому могу бути використана при розробці зазначених вище методичних рекомендацій.

Запропонованою методикою суб'єкти забезпечення кібербезпеки визначають категорію (рівень) критичності кіберінциденту/кібератаки відповідно до трьох критеріїв А, Б та В:

А. Загроза порушення сталого, надійного та штатного режиму функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем:

А1. Загроза відсутня;

А2. Безпосередня загроза для сталого, надійного та штатного режиму функціонування інформаційних, електронної комунікаційних, інформаційно-комунікаційних систем, технологічних систем;

А3. Безпосередня загроза для сталого, надійного та штатного режиму функціонування декількох інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем;

А4. Безпосередня загроза для сталого, надійного та штатного режиму функціонування значної кількості інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем;

А5. Транскордонний вплив загрози порушення сталого, надійного та штатного режиму функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем.

Б. Загроза порушення захищеності (конфіденційності, цілісності і доступності) інформації та даних, що обробляються в інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних системах:

Б1. Загроза відсутня;

Б2. Створені передумови для порушення захищеності (конфіденційності, цілісності і доступності) інформації та даних, що обробляються в інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних системах;

Б3. Порушення захищеності (конфіденційності, цілісності і доступності) інформації та даних, що обробляються в інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних системах.

В. Загрози для національної безпеки і оборони, стану навколишнього природного середовища, соціальної сфери, національної економіки та її окремих галузей, припинення виконання функцій та/або надання послуг критичною інфраструктурою:

В1. Загрози відсутні;

В2. Передумови для припинення виконання функцій та/або надання послуг критичною інфраструктурою;

В3. Потенційні загрози для національної безпеки і оборони, стану навколишнього природного середовища, соціальної сфери, національної економіки та її окремих галузей, припинення виконання функцій та/або надання послуг критичною інфраструктурою;

В4. Реальні загрози для національної безпеки і оборони, стану навколишнього природного середовища, соціальної сфери, національної економіки та її окремих галузей, припинення виконання функцій та/або надання послуг критичною інфраструктурою;

В5. Невідворотна загроза для повноцінного функціонування держави або загроза життю громадян України.

На основі врахування вибраних варіантів в трьох критеріях сформована таблиця 1.

Таблиця 1

Визначення рівня критичності кіберінцидента/кібератаки

Критерії визначення категорії (рівня) критичності													Категорія (рівень) критичності
А					Б			В					
A1	A2	A3	A4	A5	B1	B2	B3	V1	V2	V3	V4	V5	
•					•			•					0 білий
	•				•			•					1 зелений
	•				•				•				1 зелений
		•			•			•					1 зелений
		•				•		•					1 зелений
	•					•		•					2 жовтий
	•					•			•				2 жовтий
		•				•		•					2 жовтий
	•						•	•					3 помаран.
	•						•		•				3 помаран.
	•						•			•			3 помаран.
	•						•				•		4 червоний
		•					•				•		4 червоний
		•					•					•	5 чорний
			•				•					•	5 чорний
				•			•				•		5 чорний
				•			•					•	5 чорний

- [1] Верховна Рада України. 7 сесія. (2017, жовт. 5). Закон № 2163-VIII, Про основні засади забезпечення кібербезпеки України. [Електронний ресурс]. Режим доступу: <http://zakon.rada.gov.ua/laws/show/2163-viii>.
- [2] Кабінет Міністрів України. (2023, квіт. 4). Постанова № 299 «Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі» // [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#Text>.
- [3] Бакалинський О.О. Пахольченко Д.В. Перелік етапів реагування на кіберінциденти та рівні їх критичності. Кібербезпека енергетики: Науково-правкт. конф., м. Київ, 27 трав. 2022 р. С. 84–89. – Режим доступу: <https://ipme.kiev.ua/wp-content/uploads/2022/05/%D0%9C%D0%B0%D1%82%D0%B5%D1%80%D1%96%D0%B0%D0%BB%D0%B8-%D0%9A%D0%91%D0%95-2022.pdf>
- [4] NIST Special Publication (SP) 800-61 Rev. 2: Computer Security Incident Handling Guide. // [Електронний ресурс]. – Режим доступу: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>
- [5] National cyber incident responst plan. December 2016. U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). // [Електронний ресурс]. – Режим доступу: https://www.cisa.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

ДОСЛІДЖЕННЯ МЕЖІ МАКСИМАЛЬНОЇ ЕФЕКТИВНОСТІ РОБОТИ ВІТРОЕЛЕКТРИЧНИХ УСТАНОВОК У ЗАДАНИХ ВІТРОКЛІМАТИЧНИХ УМОВАХ

Оцінка ефективності роботи вітроелектричної установки (ВЕУ) проводиться з метою виявлення таких значень її основних параметрів, які дозволяють виробляти максимально можливу кількість електроенергії із мінімальними капіталовкладеннями в заданих вітрокліматичних умовах. Ефективність роботи ВЕУ (ККД ВЕУ) $\eta_{\text{ВЕУ}}$ визначається співвідношенням потужності генерування ВЕУ $P_{\text{ВЕУ}}$ до відповідної кінетичної потужності вітрового потоку (ВП) $P_{\text{ВП}}$, що діє на площину її вітроколеса (ВК) A [3, 4].

Як відомо, повторюваність швидкості вітру v протягом року підкорюється ймовірнісному закону і добре описується диференціальною функцією розподілу Вейбула – Гніденка (ДРВГ) $f(v)$. Тоді найефективнішою ВЕУ у заданих вітрокліматичних умовах буде ВЕУ з найбільшим показником середньорічного ККД:

$$\eta_{\text{ВЕУ}} = \frac{W}{S}, \quad (1)$$

де W – середньорічна використана потужність (СВП) ВЕУ, S – середньорічна потужність ВП. СВП визначається на основі даних вітрового потенціалу $f(v)$ та кривої потужності (КП) ВЕУ. Нехтуючи зміною густини повітря протягом року, середньорічна потужність ВП S залежить від $f(v)$ та діаметру ВК D .

Попереднім дослідженням [2] було встановлено, що КП ВЕУ добре описуються інтегральним розподілом Вейбула-Гніденка (ІРВГ). Виходячи із існуючої бази даних [1], були визначені параметри ІРВГ b_t та c_t для 115-ти типів ВЕУ з типорозмірами в діапазоні номінальної встановленої потужності P : $0,85 \text{ МВт} \leq P \leq 8,0 \text{ МВт}$ та діаметрів ВК D : $52 \text{ м} \leq D \leq 168 \text{ м}$.

На основі проведеного регресійного аналізу одержана наступна системи рівнянь регресії для параметрів і через основні типорозміри ВЕУ P і D :

$$\begin{cases} b_t = 12,036 + 0,954 \cdot P - 0,0547 \cdot D & (R^2 = 0,917; \delta_{\text{сер}} = 1,3 \%), \\ c_t = c_{\text{cp}} = 4,360 & (\delta_{\text{сер}} = 2,9 \%), \end{cases} \quad (2)$$

де R^2 – коефіцієнт детермінації, $\delta_{\text{сер}}$ – середня відносна похибка регресії.

В роботі [2] доведена визначальна роль значення коефіцієнта використання встановленої потужності ВЕУ (КВВП) визначається головним чином відношенням $k = (b_w/b_t)^{c_t}$ де b_w – параметр масштабу ДРВГ та згідно рівняння:

$$\text{КВВП} = 1 - \int_0^{\infty} e^{-ky^p} e^{-y} dy = 1 - I, \quad (3)$$

де $y = (v/b_w)^{c_w}$; $k = (b_w/b_t)^{c_t}$ та $p = c_t/c_w$, c_w – параметр форми ДРВГ.

Так як згідно (2) $c_t = \text{const}$, скориставшись властивостями логарифму перейдемо від k до змінної $x = b_w/b_t$. Застосовуючи рівняння регресії (3) у випадку слабого ($b_w = 6$ м/с), помірного ($b_w = 8$ м/с) та сильного ($b_w = 10$ м/с) вітрів та двох крайніх значень параметра форми ДРВГ для швидкості вітру $c_w = 2,1$ і $c_w = 2,5$ було отримано 660 значень параметра x та КВВП. За отриманими результатами була побудована логарифмічна регресія вигляду:

$$\text{КВВП} = -0,705 \cdot \ln(x) + 0,461. \quad (4)$$

Так як $W = \text{КВВП} \cdot P$, то з урахуванням (4) та (2), одержимо наступне рівняння регресії для СВП W :

$$W = P \cdot \left[-0,705 \cdot \ln\left(\frac{12,036 + 0,954 \cdot P - 0,0547 \cdot D}{b_w}\right) + 0,461 \right]. \quad (5)$$

Побудовані на основі рівняння (5) криві СВП показані при різних значеннях діаметра ВК D (показані в метрах поблизу кожної кривої) для випадку слабких, помірних та сильних вітрів на рис. 1.

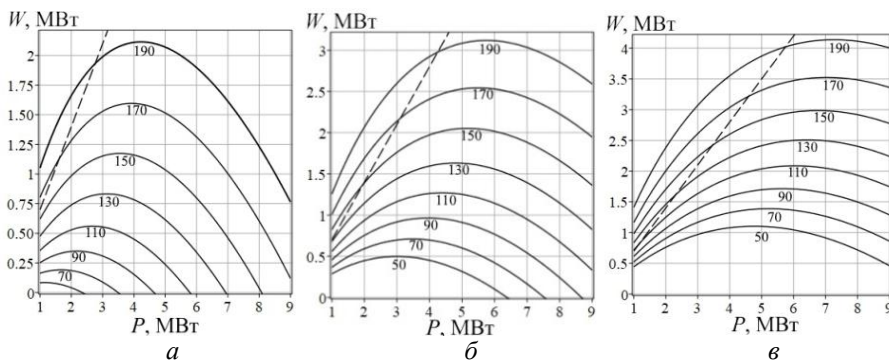


Рис. 1. Залежність СВП від номінальної потужності P та діаметра ВК D при:
а) $b_w = 6$ м/с; б) $b_w = 8$ м/с; в) $b_w = 10$ м/с

Задача оптимізації потребує знаходження локального екстремуму (максимуму) функції двох змінних $W(P, D)$. З першої необхідної умови існування екстремуму витікає рівняння:

$$\frac{\partial W}{\partial P} = -0,705 \cdot \ln \left(\frac{12,036 + 0,954 \cdot P - 0,0547 \cdot D}{b_w} \right) + 0,461 - \frac{0,673 \cdot P}{12,036 + 0,954 \cdot P - 0,0547 \cdot D} = 0. \quad (6)$$

Рівняння (6) дозволяє визначити оптимальне значення одного з трьох параметрів за відомих двох інших, наприклад, за допомогою інструменту «Пошук рішення» програми MS Excel. Обмеживши діапазон D до: $80 \text{ м} \leq D \leq 160 \text{ м}$, який повністю охоплює всі промислові ВЕУ вітропарків України, та знайшовши оптимальні значення P_0 за різних D та b_w , отримуємо наступне рівняння множинної лінійної регресії:

$$P_0 = 0,0204 \cdot D + 0,8324 \cdot b_w - 4,5651 \quad (R^2 = 0,998; \delta_{\text{ср}} = 1,4 \%) \quad (7)$$

На рис. 2 представлені графіки залежності (6) між оптимальною НВП ВЕУ P_0 і діаметром ВК D , а також параметром масштабу b_w (показані над відповідними кривими в одиницях м/с), за яких ВЕУ досягає максимальної технічної ефективності.

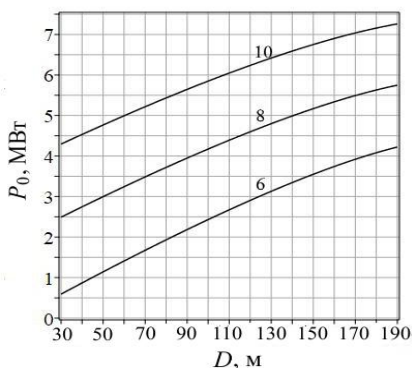


Рис. 2. Зв'язок між оптимальною НВП ВЕУ P_0 і D при різних значеннях b_w

- [1] База даних сайту <https://en.wind-turbine-models.com>.
- [2] Метод оцінювання коефіцієнта використання встановленої потужності вітрової електричної установки / В.С. Подгуренко, О.М. Гетманець, В.С. Терехов // Електронне моделювання. – 2021. – Т. 43. – № 2. – с. 37 – 51.
- [3] Півняк Г., Шкрабець Ф. Основи вітроенергетики: підручник. М-во освіти і науки України, Нац. гірн.ун-т. Д.: НГУ, 2015. 335 с.
- [4] Blackwood M. (2016). Maximum Efficiency of a Wind Turbine. Undergraduate Journal of Mathematical Modeling: One + Two, Vol. 6: Iss. 2, Article 2. Available at: <http://scholarcommons.usf.edu/ujmm/vol6/iss2/2>

НАБОРИ ДАНИХ ДЛЯ СТВОРЕННЯ СИСТЕМ ВИЯВЛЕННЯ МЕРЕЖЕВИХ ВТОРГНЕНЬ З ВИКОРИСТАННЯМ НЕЙРОННИХ МЕРЕЖ

Сьогодні, з розвитком мережеских технологій, питання комп'ютерної безпеки стають все більш актуальними, вимагаючи відповідних рішень. Системи виявлення вторгнень є важливим захисним компонентом екосистеми комп'ютерної безпеки. Система виявлення вторгнень (Intrusion Detection System - IDS) заснована на гіпотезі про те, що поведінка зловмисника відрізняється від поведінки звичайного користувача. Загалом IDS можна розділити на три категорії за принципом встановлення в системі:

- 1) IDS на основі хоста (Host-Based IDS - HIDS);
- 2) IDS на основі мережі (Network-based IDS - NIDS);
- 3) Гібридна IDS.

HIDS розгортається на одному хості. HIDS виявляє атаки з однієї комп'ютерної системи під час аналізу основних файлів операційної системи. Таким чином, ці типи атак зазвичай легко виявити, за винятком вбудованого шкідливого програмного забезпечення, яке дуже важко виявити. NIDS виявляє шкідливу інформацію з різних зв'язків між комп'ютерами. NIDS розгортається на маршрутизаторах або комутаторах у мережі. Гібридну IDS можна розгортати як на хостах, так і в мережах. Основна мета NIDS — виявити зловмисну інформацію, яка реєструється, і повідомити про цю зловмисну інформацію адміністраторів мереж. Системи виявлення вторгнень зазвичай не запобігають атакам на системи. Натомість вони просто генерують сповіщення після виявлення атаки в системі в режимі реального часу або до того, як вона досягне мети. Не менш важливо повідомляти про напад після того, як він стався, оскільки IDS керує профілями атак та оновлює їх в журналах. Операційна система також має підтримувати різноманітні дії, які потребують надмірних ресурсів пам'яті та ЦП (центрального процесора) для аналізу журналу. Керування форматами журналів і порівняння цих форматів із виявленими моделями атак у відповідь на порушення безпеки також є серйозною проблемою для IDS [1].

Ефективність системи виявлення мережеских вторгнень значною мірою залежить від якості та кількості даних, які використовуються для навчання та оцінки системи. З розвитком машинного навчання та нейронних мереж набори даних стали ключовим компонентом при побудові точних та надійних систем виявлення вторгнень. Обраний набір даних використовується не тільки для навчання моделі IDS, але й для оцінки ефективності запропонованої IDS-моделі [2]. Через складність прямого збору даних про атаки в реальному часі дослідники можуть використовувати загальнодоступні стандартні набори даних на основі мережевого трафіку, такі як: DARPA 1998, KDD Cup 99, KYOTO, UNSW-NB15, DEFCON,

CAIDAs, CDX, NSL-KDD, TWENTE, CSC DoS, CICIDS2017, CSE-CIC-IDS2018, ISCX, ADFA2013, CTU-13 [3]. Розглянемо розповсюджені стандартні набори даних більш детально:

1) Набір даних DARPA 1998 базується на даних мережевого трафіку та журналах аудиту, і вперше був доступний у лютому 1998 року. Цей набір даних є класичним набором даних, який використовується для оцінки NIDS і широко застосовується як еталонний набір даних. Він включає дані мережевого трафіку, зібрані в змодельованому мережевому середовищі, з різними типами атак, включаючи DoS, Probe, R2L і U2R. Набір даних надає різноманітний набір функцій, включаючи протоколи транспортного рівня, протоколи прикладного рівня і дані корисного навантаження. Цей набір даних не відображає реальний мережевий трафік.

2) Набір даних KDD Cup 1999 є широко використовуваним еталонним набором даних для оцінки NIDS. Він містить велику колекцію даних мережевого трафіку з позначеними типами атак, які можна використовувати для навчання і тестування NIDS. Набір даних включає різні типи атак, такі як DoS, Probe, R2L і U2R, що робить його цінним ресурсом для оцінки ефективності NIDS проти різних типів атак.

3) Набір даних NSL-KDD є оновленою версією набору даних KDD Cup 1999, в якій усунуто деякі обмеження та упередження, присутні в оригінальному наборі даних. Він містить більшу кількість зразків і більш збалансований розподіл типів атак, що робить його більш придатним для навчання та оцінки NIDS.

4) Набір даних UNSW-NB15 є ще одним популярним набором даних для NIDS, що містить дані мережевого трафіку, зібрані з реального мережевого середовища. Він включає ряд типів атак, таких як DoS, Probe, R2L і U2R, а також дані про звичайний трафік. Набір даних також включає дані на рівні пакетів і потоків, що дає більш детальне уявлення про поведінку мережі.

5) Набір даних CICIDS2017 є нещодавнім доповненням до колекції наборів даних для NIDS. Він включає дані про мережевий трафік, зібрані з різних мережевих топологій і сценаріїв атак, що робить його більш різноманітним і всеосяжним набором даних. Набір даних включає різноманітні типи атак, такі як DoS, Probe, R2L і U2R, і надає детальний огляд характеристик мережевого трафіку, таких як протоколи транспортного рівня, протоколи прикладного рівня і дані про корисне навантаження.

6) Набір даних CSE-CIC-IDS2018 є набором даних, який запропоновано Інститутом безпеки комунікацій (CSE) та Канадським інститутом кібербезпеки (CIC). Набір даних CSE-CIC-IDS2018 включає сім різних сценаріїв атак, зокрема Heartbleed, Brute-force, DoS, DDoS, вебатаки, ботнети та проникнення.

Слід зауважити, що вибір відповідних наборів даних має вирішальне значення для розробки точних і надійних NIDS з використанням нейронних мереж. Набори даних, розглянуті в цій статті, є цінним ресурсом для навчання та оцінки NIDS проти різних типів атак і мережевих середовищ. Використовуючи ці набори даних, дослідники та практики можуть

розробляти більш ефективні NIDS, здатні виявляти та пом'якшувати широкий спектр кіберзагроз.

Враховуючи вищезазначене, в наступних дослідженнях планується:

1) Подальший аналіз літератури, пов'язаної з системами виявлення мережевих вторгнень;

2) Створення та навчання власної нейронної мережі глибокого навчання для системи виявлення мережевих вторгнень з використанням публічних наборів даних;

3) Дослідження використання генетичних алгоритмів для ефективного пошуку оптимальних налаштувань гіперпараметрів нейронної мережі та їх порівняння з іншими алгоритмами оптимізації гіперпараметрів, такими як: алгоритм оптимізації рою частинок, прискорення пошуку за сіткою (grid search) та ін.;

4) Експериментальне визначення можливості використання навченої нейронної мережі для виявлення мережевих вторгнень в реальному часі.

- [1] Kumar S., Gupta S., Arora S. Research Trends in Network-Based Intrusion Detection Systems: A Review. IEEE Access. 2021. Vol. 9. P. 157761–157779. URL: <https://doi.org/10.1109/access.2021.3129775>.
- [2] Sohn I. Deep belief network based intrusion detection techniques: A survey. Expert Systems with Applications. 2020. P. 114170. URL: <https://doi.org/10.1016/j.eswa.2020.114170>.
- [3] Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study / M. A. Ferrag et al. Journal of Information Security and Applications. 2020. Vol. 50. P. 102419. URL: <https://doi.org/10.1016/j.jisa.2019.102419>.

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РОЗРОБКИ ТРЕНАЖЕРНИХ ЗАНЯТЬ ЗА РАХУНОК ЗАСТОСУВАННЯ ФУНКЦІОНАЛЬНО-ВАРТІСНОГО АНАЛІЗУ

Функціонально-вартісний аналіз(ФВА) – це метод дослідження функцій об'єкта (виробу, процесу, структури), що базується на системному підході та спрямований на формування оптимальних співвідношень між корисністю функцій об'єкта, якістю їх реалізації та витратами на всіх етапах життєвого циклу[1]. ФВА заохочує використання альтернативних методів і матеріалів, які є менш дорогими та не знижують функціональність системи, послуги чи продукту. Найчастіше ФВА використовують після завершення процесу проектування, але його найкраще виконувати до того, як проект буде проведено, щоб дозволити експертам включити можливість використання альтернативних матеріалів і методів. В першу чергу мінімізують вартість виконання основних функцій. При цьому якість функціонування виробу прагнуть зберегти на колишньому рівні. Основними принципами ФВА є: застосування системного підходу щодо об'єкта, який є і складовою системи вищого порядку, і самостійної системою, що включає сукупність взаємозалежних, взаємозалежних і об'єднаних загальної функцією елементів; визначення ступеня відповідності між значимістю функцій, витратами та рівнем якості їх реалізації. Витрати, у випадку, пов'язані з спожитими у процесі господарську діяльність ресурсами, ще визнаними витратами, оскільки вони відбиваються у балансі як залишків, незавершеного виробництва, готової продукції наприкінці звітний період. Витрати поширюються попри всі ресурси, спжиті у процесі фінансово-господарську діяльності. У процесі ФВА саме зіставлення значущості функцій, витрат та якості їх реалізації дає можливість виконати економічну оцінку системи управління (як існуючої, так і знову розробленої); застосування колективних форм роботи, активізація творчого потенціалу співробітників з метою покращення якісних характеристик продукту Рішення про застосування ФВА у процесі розробки тренажерних занять, був прийнятий після успішної інтеграції метода у відомих великих компаній у провідних країнах світу. Метод ФВА був розроблений у США та вперше застосований у 1947 році в компанії «General Electric». У цьому ж році в компанії була створена група фахівців під керівництвом інженера Л. Д. Майлса, яка приступила до створення методу зниження витрат, заснованого на пошуку більш економічних способів здійснення тих чи інших функцій виробів, і впровадження його у виробництво. Група Майлса за 4 роки проаналізувала та змінила конструкції 230 виробів, внаслідок чого витрати на їх виготовлення скоротилися в середньому на 25% без зниження якостей Інженер Лоуренс Д. Майлс дійшов висновку, що зниження витрат виробництва треба починати з аналізу споживчих властивостей виробу і технічних функцій його частин. На

сьогоднішній день, в Японії 100 % експортованих промислових виробів піддається ФВА[1].

Першим етапом ФВА є планування та підготовка. На ньому уточнюються об'єкт аналізу та цілі (мінімізація вартості або підвищення якості виконання функції за збереження колишньої вартості). Головним ресурсом який витрачається розробниками під час розробки тренажерних занять(ТРЗ) є час. Тому головною цілю застосування ФВА є зменшення часу розробки ТРЗ. Другий етап ФВА інформаційний включає в собі збір даних щодо умов застосування та виготовлення об'єкту, вимог до його якості, можливих проектних рішень, недоліків. На цьому етапі необхідно порахувати середній час розробки одного ТРЗ. Враховуючи що завдання можуть розроблюватись на основі енергетичних мереж, які містять різну кількість мережевих компонентів(трансформатори, перемикачі і так далі) час розробки тренажерного заняття варто поділити на кількість компонентів у мережі, для більш детальної інформації про метод розробки ТРЗ. Наступним етапом ФВА є аналітичний. В ньому відбувається складання функціональної структури, визначення вартості та цінності окремих функцій, вибір напрямку роботи. Під час цього етапу складають алгоритм, який включає в собі всі процеси які виконуються під час розробки ТРЗ(побудування мережі у графічному редакторі, ввід технічних параметрів для компонентів мережі, визначення цілі тренування, з'єднання компонентів мережі за допомогою гілок чи ліній і так далі), і порахувати час, який витрачається на кожен процес. Чим більше процесів і під процесів буде визначено, тим більше є шанс на підвищення ефективності розробки ТРЗ. Також всі процеси необхідно вказувати в порядку їх виконання. Якщо деякі процеси можуть виконуватись у різному порядку, необхідно вказати всі варіанти того в якому порядку виконуються процеси. Для зручності, процеси розробки ТРЗ можна побудувати за допомогою блок-схем чи бізнес- процесів. Представлення алгоритму розробки ТРЗ такими методами, допоможе візуально показати варіативність виконання процесів. Пошуковий етап ФВА включає в собі покращення рішення на основі залучення евристичних, математичних та експериментальних методів. В цьому етапі відбувається вибір кращих, з запропонованих варіантів. На цьому етапі визначаються процеси які не впливають на якість ТРЗ, і ці процеси більше не виконуються під час розробки ТРЗ. Далі необхідно мінімізувати час процесів, які займають найбільшу кількість часу. Мінімізація може бути досягнута, за допомогою альтернативного шляху виконання процесу. Наприклад, написання програми, яка автоматично виконує процес, і не потребує втручання розробника у цей процес. Також зменшення часу розробки може бути досягнута за допомогою зміни порядку виконання процесів. Останнім етапом ФВА є рекомендаційний, в ньому оформлюють протоколи та рекомендації щодо реалізації пропозицій. У міру того, як керівництво підтверджує просування вперед зі змінами, ФВА переходить від теоретичної практики до процесу реалізації управління змінами. Коли запропоновані зміни приймаються, формуються нові команди та призначаються області нагляду. Розробники

ТРЗ часто залишаються залученими до змін, щоб стежити за тим, що коригується та як очікування узгоджуються з нововведеннями.

Використання ФВА значно зменшить розробку ТРЗ, за рахунок зменшення кількості процесів та пошуку альтернативних методів виконання процесів. Проведенні практичні експерименти розробки ТРЗ для розподільчої мережі, до і після використання ФВА, показали що автоматизація програмним шляхом процесів, які займали найбільшу кількість часу під час розробки, та зміна порядку деяких процесів, зменшує час розробки ТРЗ майже на 10% від середнього часу, яка була до використання автоматизації та зміни порядку процесів. Зменшення часу розробки ТРЗ, призводить до ефективності ТРЗ, за рахунок зменшення часу адаптації персоналу, оскільки вони швидше отримують нові знання чи підтверджують свою компетентність.

- [1] Value Engineering: Analysis And Methodology / [Del Younger]. – Florida, USA, 2003. – 340 p.

В.В. Аскеров, О.С. Засорнов

ВИКОРИСТАННЯ БЛОКЧЕЙН ТЕХНОЛОГІЇ ДЛЯ КЕРУВАННЯ ДАНИМИ СОНЯЧНОЇ ЕЛЕКТРОСТАНЦІЇ ХМЕЛЬНИЦЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ

Хмельницький національний університет (ХНУ)- перший та єдиний ВНЗ в Україні, на даху якого було розміщено сонячні електростанції [1]. На дахах декількох корпусів ХНУ розташовано більше сотні сонячних панелі рис. 1.



Рис. 1. Сонячна електростанція на даху четвертого корпусу ХНУ

У 2018 році потужність сонячної електростанції була збільшена до 650 кіловат [2]. Вартість сонячної електростанції (СЕС) складала близько 1 300 000 гривен. Саме тому використання виробленої енергії повинно бути раціональним. Це може зменшити час окупності обладнання що входить до складу СЕС.

Відомо що влітку університет споживається значно менше енергій, а СЕС виробляє її більше. Це означає, що у літній період можна зайву вироблену електроенергію потрібно продати державі за “зеленим тарифом” (ХНУ отримала ліцензію на виробництво електроенергії 25.10.2019 та здобула “зелений тариф” 15.14 євро центів у гривневому еквіваленті починаючи з 17.02.2021). Далі необхідно здійснити накопичення коштів за які можна купити електроенергію для використання у зимовий період.

Проте на практиці майже не можливо врахувати кількість електроенергії яку зможе виробити СЕ оскільки її кількість залежить від впливу багатьох зовнішніх факторів.

Для раціонального використання необхідно правильно розподіляти електроенергію яку споживають. Чітко знати кількість електроенергії яку виробляє СЕС і віддану у мережу, кількість накопичених коштів та певні інші параметри. Це неможливо виконати без застосування спеціальних методик для визначення цих параметрів, оскільки жодні адміністративні заходи не можуть забезпечити гарантію правильного обліку енергії що виробляють СЕС.

Після отримання потрібних даних їх потрібно обробити та зберігати для подальшого використання. Практично єдиним способом зберігання є база даних. Тому доцільним є використання блокчейн-технології, оскільки її основним призначенням є створення безпечних та надійних баз даних.

У блоках міститься інформація про транзакції або події, що відбуваються у системі [3]. Кожен блок захищений шифруванням і має посилання на попередній блок, що унеможливує зміну або видалення даних. Саме тому можна бути впевненим у збереженні інформації, так як у сучасній сонячній енергетиці величезні зусилля витрачаються на ведення обліку енергії та захист від втрат.

Прозорість, незмінність та відчужуваність транзакцій у блокчейні гарантує більш комфортне середовище для бізнесу, ніж будь-які сучасні технології обліку енергії, які так чи інакше піддаються людському фактору. Технологія блокчейн завдяки своїй сутності позбавляє потреби в послугах третьої сторони, що бере на себе наглядові функції за розподілом енергії.

Основними витоками створення блокчейн проекту для керування даними СЕС Хмельницького національного університету стали два Європейський проекти запропоновані компаніями «Sonnen Group» та «ekWateur». Компанією «Sonnen Group» у Німеччині була створена віртуальна електростанція - VirtualPowerPlant (VPP). Яка може зберігати будь яку надмірну енергію. Її учасники здійснюють оплату у цифровій валюті. VPP це децентралізована сітка розподілених енергоблоків. До яких входять повітряні електростанції, СЕС та системи збереження енергій. VPP «Sonnen Group» використовує блокчейн для збереження надмірної енергії шляхом заряджання батарей з використанням блокчейн додатку, створеного на EW Origin. Для фінансового розрахунку VPP використовують стабільну монету EWDai з сітки Ethereum [4]. Французька енергетична компанія «ekWateur» створила торгову платформу, яка дозволяє відстежувати та сертифікувати продаж енергії. Компанія «ekWateur» дозволяє клієнтам обирати постачальника енергії. Для відстежування та сертифікації транзакцій використовують криптовалюту POWR token [5]

Отже, проведені дослідження та аналіз європейських практик показали,

що використання блокчейн технології для керування даними СЕС Хмельницького національного університету є доцільними. Їх застосування дозволить заощадити кошти університету та зробить експлуатацію СЕС більш ефективною.

- [1] Хмельницький національний університет - перший та єдиний ВНЗ в Україні, на даху якого розмістили сонячні електростанції URL: <https://khamelnytsky.com.ua/ua/fullnews/242785> (доступ 27.04.23).
- [2] Skyba M. Intelligent Solar Tracking System as a Prospect for Developing the Alternative Energetics in Ukraine / M. Skyba, T. Hovorushchenko, V. Martynyuk, O. Zasornov, O. Pavlova // CEUR-WS. 2021. Vol. 2853. Pp. 50-61. URL: <https://ceur-ws.org/Vol-2853/paper2.pdf>.
- [3] Blockchain Technology: Principles and Applications" by M. Narayanan and V. Viranjampuram. Publisher: Academic Press, 2018. P. 312.
- [4] SevenS., YaoG., SoranA., OnenA., MuyeenSM. Peer-to-Peer Energy Trading in Virtual Power Plant Based on Blockchain Smart Contracts // IEEE Access. 2020. Vol.8. pp.175713-175726.
- [5] KimG., ParkJ., RyouJ. A study on utilization of blockchain for electricity trading in microgrid // IEEE International Conference on Big Data and Smart Computing (BigComp). 2018. pp.743-746.

СТВОРЕННЯ 3D-МОДЕЛІ ОБЛИЧЧЯ ЛЮДИНИ ЗА ДОПОМОГОЮ ПІДХОДУ НА ОСНОВІ НЕЙРОМЕРЕЖІ

Дослідники у графічних та візуальних сферах активно займаються моделюванням об'єктів та сцен у тривимірному просторі, оскільки це є важливою задачею. Цифрові моделі є необхідними для навігації, ідентифікації об'єктів, візуалізації та анімації. Застосування таких моделей може бути різним, від віртуального туризму до медицини. Для багатьох застосувань вимоги включають високу точність, фотореалістичність, автоматизацію та мобільність. Вибір технології 3D-моделювання може бути неоднозначним, особливо для складних об'єктів. Реконструкція 3D-моделі з фотографій може здешевити та прискорити процес створення моделі. Важливо знайти ефективний метод та реалізувати систему, яка буде видавати якісний результат без необхідності використання високопотужного обладнання та великих затрат у часі. [1]

Для визначення ефективного шляху вирішення проблеми було зроблено докладний аналіз існуючих методів та підходів. Досліджено помилки оцінки глибини різних методів, час на реконструкцію та середню помилку. Висновок, який можна зробити з аналізу, полягає в тому, що найкращі результати можна отримати за допомогою поєднання підходу 3D Morphable Model та згорткової нейронної мережі. [1-4]

Для удосконалення підходу 3D Morphable Model пропонується модифікувати його за допомогою методу основних компонентів (РСА).

Опис геометрії обличчя в цьому методі надано у [1]. Але для подальшої роботи необхідний аналіз основних компонентів. РСА виконує базисне перетворення в ортогональну систему координат, утворену власними векторами s_i та t_i коваріантних матриць.

$$S_{\text{model}} = \bar{S} + \sum_{i=1}^{m-1} \alpha_i s_i, \quad (1)$$

$$T_{\text{model}} = \bar{T} + \sum_{i=1}^{m-1} \beta_i t_i. \quad (2)$$

Вірогідність для коефіцієнтів α_i визначається $\alpha, \beta \in R^{m-1}$.

$$\rho(\bar{\alpha}) \sim \exp \left[-\frac{1}{2} \sum_{i=1}^m (\alpha_i / \sigma_i)^2 \right] \quad (3)$$

де α_i^2 - власні значення коваріантної матриці C_s форми.

Ймовірнісні коефіцієнти β_i розраховуються аналогічно.

Ідея використання аналізу головних компонентів (РСА) як метод лінійного зменшення розмірності для захоплення характерних розмірів

людських осіб і створення тривимірної моделі обличчя, що змінюється, здатної генерувати правдоподібні особи, є ключовою ідеєю для 3DMM.

Обчислення PCA та перетворення між гранями вимагає повної відповідності по всіх гранях у навчальному наборі.

Буде Створено, проведені аналіз та ~~проведено~~ тестування програмного забезпечення [5]. Програмна система змогла визначити та змоделювати обличчя з оклюзією та без неї (рис. 1-2). Відмічено, що велика кількість ітерацій для оптимізації дає кращі результати, але займає більше часу.

Завдяки використанню графічного інтерфейсу робота з програмою не вимагає спеціальної підготовки та вміння працювати з терміналом. Буде проведено тест для моделювання обличч 100, 500 і 1000 людей. Час, витрачений на кожен етап створення обличчя в секундах, показано в таблиці 1 з використанням 500, 1000 і 1000 ітерацій.

Таблиця 1

Час, витрачений на кожен етап створення обличчя в секундах [5]

Stage	Iterations		
	100	500	1000
Image upload	0.038622	0.035757	0.034777
Face search	0.085725	0.069498	0.074438
Finding Landmarks	0.634996	0.620067	0.618354
Loading a BFM Model	0.103088	0.10012	0.100897
Rigid model fit	3.476556	3.232674	3.56682

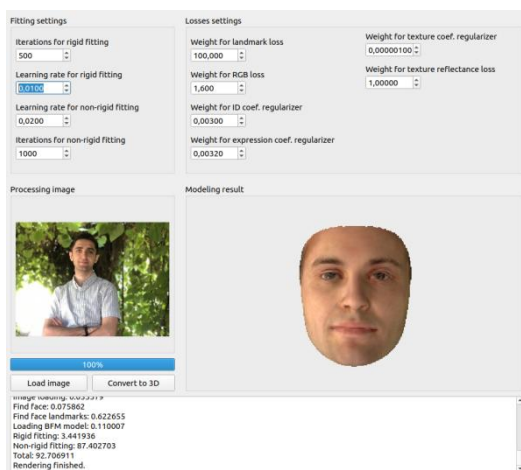


Рис. 1 Завантаження фото обличчя в програму з налаштуваннями 1000 ітерацій для функції оптимізації [5]

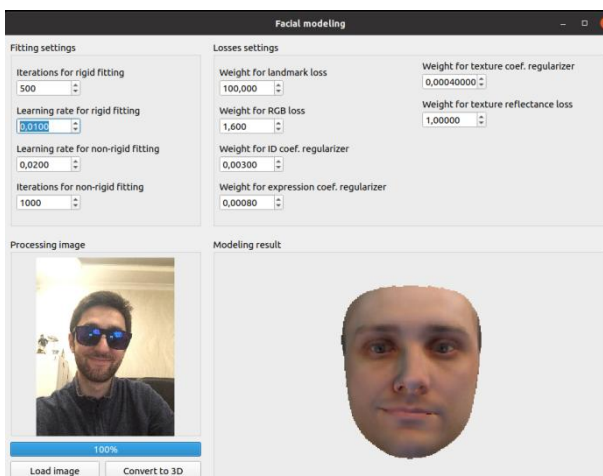


Рис.2 Обробка зображення з оклюзіями на обличчі [5]

У ході дослідження розглянуто методи реконструкції моделі обличчя, проведено їх порівняльний аналіз, була розроблена програма, яка дозволить використовувати систему для моделювання обличчя із завантаженого файлу. Було підібрано найбільш оптимальні методи розпізнавання осіб і орієнтирів обличчя на основі глибинного навчання, а також метод створення моделі за допомогою 3DMM з його модифікацією за допомогою PCA.

- [1] Aleksandrova O., Bashkov Y. (2019) 3D face model reconstructing from its 2D images using neural networks, 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2019, pp. 98-101, doi: 10.1109/ATIT49449.2019.9030503.
- [2] Richardson E., Sela M., Or-El R., Kimmel R. (2017) Learning detailed face reconstruction from a single image. IEEE Conference on Computer Vision and Pattern Recognition, pp. 5553-5562
- [3] Fangmin L., Ke C., Xinhua L. (2017) 3D Face Reconstruction Based on Convolutional Neural Network. 10th International Conference on Intelligent Computation Technology and Automation, pp. 71-74
- [4] Xiangyu Z., Junjie Y., Dong Y., Zhen L., Stan Z.L. Discriminative 3D Morphable Model Fitting, unpublished.
- [5] Aleksandrova O., Bashkov Y., Pohosian A. (2022) Approach for Creating a 3D Model of a Face from its 2D Image, 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2022, pp. 173-176, doi: 10.1109/ATIT58178.2022.10024231

РОЗРОБКА СТРУКТУРИ СИСТЕМИ ВИМІРЮВАННЯ ГЕОМЕТРІЇ ВИГОРОДКИ РЕАКТОРІВ ВВЕР-1000

Протягом багатьох десятирічь атомна енергетика забезпечує значну долю загального виробництва електроенергії України. Продовження термінів експлуатації енергоблоків ВВЕР-1000 має бути засноване на експериментальних та теоретичних дослідженнях технічного стану критичних елементів конструкції енергоблоку – корпусу, шахти та вигородки реактора, які незамінні протягом усього періоду експлуатації реактора.

Мета дослідження полягає у розробленні науково-обґрунтованої методики вимірювань геометричних розмірів вигородки активної зони ядерних реакторів АЕС, а також структури та вимог до спеціальних технічних засобів для їх використання у процесі виконання заходів продовження термінів експлуатації енергоблоків понадпроектний строк. Вигородка призначена для формування поля енерговиділення, дистанціювання периферійних касет і радіаційного захисту. Особливістю експлуатації вигородки є наявність сильного нейтронного випромінювання і високих температур внаслідок радіаційного розігріву, які призводять до розпухання металу. Потенційну загрозу представляють зменшення зазорів між внутрішньою поверхнею вигородки і поверхнею оболонки твелів та між зовнішньою поверхнею вигородки і внутрішньою поверхнею шахти, зміна фізичних властивостей металу вигородки.

Розрахунок формозміни вигородки в процесі експлуатації та аналіз щодо впливу радіаційної повзучості дає суперечливі результати [1]. Всі прогностичні моделі розпухання засновані на результатах модельних експериментів і мають малий часовий відрізок застосування. Інструментальний контроль фактичних розмірів вигородки в процесі експлуатації дозволить скоригувати прогностичні моделі формозмін вигородки з метою оцінки ресурсу конкретних екземплярів реакторів і уникнути надто консервативних оцінок.

Дуже жорсткі умови всередині вигородки – висока радіація та заповнення внутрішнього простору вигородки рідиною, яка вносить спотворення в зондувальні сигнали, суттєво обмежують можливості застосування відомих методів вимірювань геометричних розмірів. При цьому потрібна мікронна точність контролю геометричних розмірів вигородки.

Проведений аналіз відомих систем, а саме: Система СТС-К-ВКУ (ЗАТ "Діаконт", РФ, м. Санкт-Петербург); Спеціальна система вимірювання геометрії вигородки ВКУ (ТОВ "Инжиниринговая компания "АТОММАШЭКСПОРТ", Україна, м. Київ); Система NRI-Rez (Чехія, м. Ржеж); Комплекс ВК-5 технічних засобів вимірювання геометричних розмірів вигородки активної зони ВКП реакторних установок ВВЕР-1000 (ВП «КБ «Атомприлад» ДП «НАЕК «Енергоатом», м. Київ), - дозволяє

сформувати основні положення для розробки перспективної системи вимірювання геометричних розмірів вигородки.

У горизонтальному січенні вигородка має 6 симетричних секторів, які розташовані по периметру вигородки з кроком 60° . Кожна грань вигородки має паралельну грань, яка розташована симетрично відносно осі вигородки. У кожному секторі 15 граней. Всього граней $15 \times 6 = 90$. Вимірювання слід проводити під прямим кутом до паралельних граней вигородки. Так як кожній грані відповідає паралельна грань, можна провести перпендикулярно до граней $90/2 = 45$ хорд. Довжини хорд однозначно визначають внутрішні геометричні розміри вигородки. При практичній реалізації слід визнати допустимим скорочення числа одночасно контрольованих хорд, наприклад, як у системі ВК5.

Перспективну систему пропонується будувати на основі конструкції стабілізованої платформи – доопрацьованого модуля вимірювальної системи ВК5. Це вдалий, продуманий засіб доставки, кутового та лінійного переміщення, точного позиціонування засобів вимірювання всередині вигородки, добре адаптований до штатних засобів, що є на АЕС.

Застосування лазерних триангуляційних перетворювачів (як в системі ВК5) для вимірювання хорд вигородки є малоперспективним. Дистанційні вимірювання неможливі через наявність каламутного рідкого середовища, а поблизу стінки вигородки є висока радіація, яка скорочує "час життя" вимірювальної системи до неприйнятно малої величини. Вибір більш стійких до радіації лазерних вимірювачів та створення захисного бар'єру може виявитися дорогим і малоефективним.

В даний час в Інституті проводиться опрацювання конструкції перспективної вимірювальної лінійки на основі інкрементної магнітної системи для встановлення на стабілізовану платформу системі ВК5. Подібне технічне рішення раніше відпрацьовано при розробці низькочастотної віброкалібрувальної установки [2].

- [1] Чирков О.Ю., Харченко В.В. Вплив радіаційної повзучості на визначення формозміни вигородки активної зони реактора ВВЕР-1000 за умов довгострокової експлуатації. Допов. Нац. акад. наук Укр. 2021. № 3. С. 40—47. <https://doi.org/10.15407/dopovidi2021.03.040>.
- [2] О.А. Владимирський, 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.-с.45-49. <http://doi.org/10.5281/zenodo.3860730>.

газу (до 18 м³/год.), води (8 м³/год.), каналізації, витяжної вентиляції, електромережі.

Реалізуються 3 схеми вимірювань, передбачені стандартом - з прямою циркуляцією та з теплообмінником. Автоматично ідентифікується стан теплової рівноваги, тобто коли температура води на вході і на виході котла стабілізується в межах $\pm 2^{\circ}\text{C}$. Автоматичний розрахунок ККД здійснюється за методиками викладеними в стандарті на підставі показань лічильників газу та води, численних вимірювачів температури, ваг та коректора газу. На практиці деякі складнощі виникають через різноманітність апаратних інтерфейсів, протоколів і форматів даних вимірювальних засобів, що застосовуються в стенді і які необхідно узгодити зі звичайним офісним РС-сумісним ноутбуком, який застосовується як обчислювальна платформа. Робота виконується з використанням науково-технічного доробку, отриманого при розробці Апаратно-програмного комплексу для проведення випробувань іскробезпечних електричних ланцюгів [1, 2] - у частині управління схемами вимірювання та відображення робочих мнемосхем.

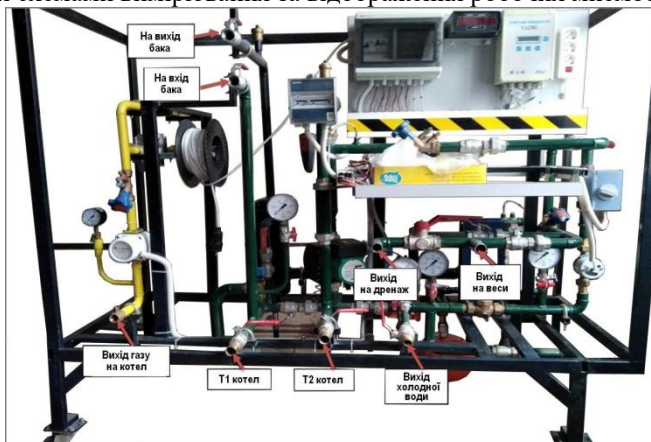


Рис.2. Стенд для визначення ефективності котлів (котел, ваги та бак для води на фотографії не показані).

- [1] О.А. Владимирський, І.П.Криворучко. Апаратно-програмный комплекс для проведения испытаний искробезопасных электрических цепей (АПК “ИСКРА”). Руководство по эксплуатации ИСКРА-1.00.04 РЭ. Свідоцтво про реєстрацію авторського права на службовий твір № 112421 від 16.03.2022р. ІПМЕ ім. Г.Е.Пухова НАН України. Публ. 31.05.2022р, Бюл. №70.
- [2] О.А. Владимирський, І.П. Криворучко. Комп'ютерна програма “Стенд для проведения испытаний искробезопасных электрических цепей Flash 1.03. Версия В.10.20-2022). Свідоцтво про реєстрацію авторського права на службовий твір №112611 від 07.04.2022р. ІПМЕ ім. Г.Е.Пухова НАН України. Публ. 31.05.2022р, Бюл. №70.

РОЗРОБКА ГЕНЕРАТОРА ДЛЯ АКУСТИЧНОГО ЗОНДУВАННЯ ТРУБОПРОВІДІВ

Розробка генератора є продовженням роботи зі створення приладового комплексу низькочастотного акустичного корозійного моніторингу підземних трубопроводів “РАСТР-2” (тема “МОНІТОР-2”). Оскільки експериментальний комплекс “РАСТР-1” [1, 2, 3] пройшов успішні випробування, метою створення наступної моделі є пристосованість до більш інтенсивної польової роботи та покращення параметрів комплексу. Стосовно генератора, основними завданнями були: підвищення потужності генератора та створення приладу без застосування мобільного комп’ютера з мінімально потрібною кількістю регулювань.

На рис.1 представлена функціональна блок-схема розробленого генератора, на рис.2 надано його фото.

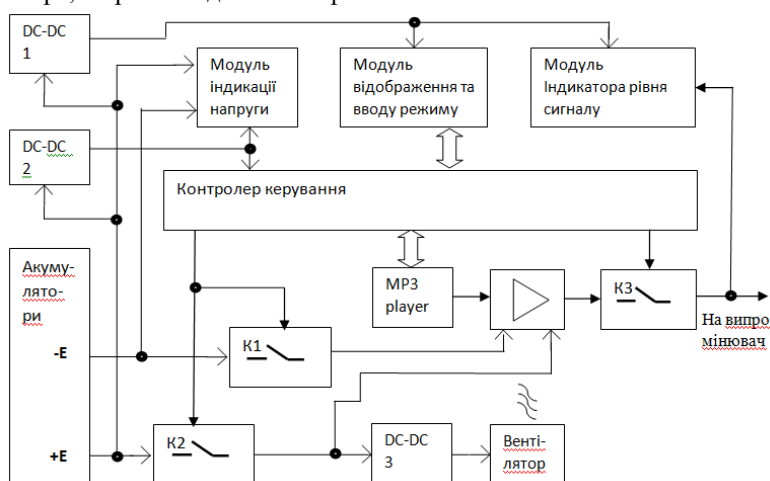


Рис.1. Функціональна блок-схема генератора зондувачі сигналів.

Генератор має два канали потужністю по 50 Вт чи один 100 Вт. Живлення генератора відбувається від двох пар Li-ion акумуляторів. Коли підключена одна пара, інша в резерві. Кожна пара формує напругу +36В і –36В. Безпосередньо від цієї напруги живиться підсилювач потужності класу АВ. Інші модулі живляться крізь знижуючі DC-DC перетворювачі, які формують додаткові напруги: +12 В (на схемі DC-DC 3) для живлення вентилятора підсилювача, +9 В (на схемі DC-DC 2) для живлення контролера керування та модуля індикації поточної напруги акумуляторів, +5В (на схемі DC-DC 1) для живлення модуля відображення та вводу режиму роботи генератора. Треки зондувальних звуків містяться на SD карточці модуля MP3

player. З виходу цього модуля сигнал подається на вхід підсилювача потужності. З виходу підсилювача сигнал проходить крізь ключ К3 на вихід генератора та далі – на вхід акустичного випромінювача. За допомогою ключа К3 контролер керування здійснює затримку підключення випромінювача на 2 сек. відносно моменту вмикання живлення. Затримка запобігає перевантаженню випромінювача від перехідних процесів у підсилювачі. Інші ключі К1 і К2 призначені для автоматичного відключення живлення від підсилювача після закінчення звучання заданого треку. Відключення зроблено для економії енергоспоживання генератора, оскільки підсилювач на холостому ході споживає 0,6 А. Передбачені режими: введення номеру (1.9) тесту (треку), введення одного з 9 рівнів вихідної потужності, тривалості тесту і введення команд пуску зондування та його примусової зупинки.



Рис.2. Генератор зондуючих сигналів.

- [1] А.А. Владимирский, И.А. Владимирский. Создание технических средств для оценки степени коррозионного износа подземных трубопроводов тепловых сетей без их вскрытия. Моделирование та інформаційні технології. Збірник наукових праць. Інститут проблем моделювання в енергетиці НАН України. Вип. 75, Київ, 2015р. -с.42-48.
- [2] А.А. Владимирский, И.А. Владимирский, И.П. Криворучко, Н.П. Савчук. Разработка модернизированной системы низкочастотного диагностирования состояния трубопроводов РАСТР-1М. Моделирование та інформаційні технології. Збірник наукових праць. Інститут проблем моделювання в енергетиці НАН України. Вип. 78, Київ, 2017р.-с.40-45.
- [3] Владимирский, И.А. Владимирский. Система дистанционного диагностирования коррозионного повреждения подземных трубопроводов. Матеріали II Міжнародної науково-технічної конференції "Теоретичні і прикладні аспекти комп'ютерних наук та інформаційних технологій" TACSIT-2017. 12-13 травня 2017р. м. Северодонецьк, Україна. – С.100-103.

О.А. Владимирський, І.А. Владимирський, А.П. Івашенко, І.П. Криворучко

НИЗЬКОЧАСТОТНА ВІБРОКАЛІБРУВАЛЬНА УСТАНОВКА

Група Технічної діагностики ІПМЕ ім. Г.Є. Пухова НАН України спільно з відділом 22 ДП “Укрметртестстандарт” продовжує роботи зі створення низькочастотної віброкалібрувальної установки НАВКУ-3 [1, 2]. В даний час змонтовано горизонтальний низькочастотний вібростенд з ходом каретки 1,5 М (рис.1.), проводяться пусконаладжувальні роботи, відпрацьовуються алгоритми та програмне забезпечення [3].

Функції і основні проектні характеристики низькочастотного стенду:

- Відпрацювання переміщення (вібрації) робочого столу із заданими характеристиками в діапазоні частот 0,1 Гц - 15 Гц.

- Розмах переміщення - до 1,5 м.
- Маса переміщуваного об'єкту - до 3 кг.
- Максимальна швидкість - до 10 м/с.
- Максимальне прискорення - до 2 м/с².

До складу низькочастотного стенду входять:

- Спеціальний постамент - цільнозварювальна силова конструкція.
- Лінійний актуатор компанії ROLLON - привід з зубчастим ременем. Довжина актуатора – 1,8 м.
- Кроковий двигун FL130BYG (живлення 220 VAC, 7 А обертаючий момент 500 кгс*см, кутовий крок, 1.8 град.).
- Силовий розділовий трансформатор 220 VAC, 10 А, який забезпечує гальванічну розв'язку ланцюгів живлення крокового двигуна від мережі 220 В.
- Високовольтний драйвер крокового двигуна типу DM2282 - 2-фазний цифровий кроковий привід (220 VAC, 8,2А).
- Контролер крокового двигуна, який забезпечує формування у реальному часі сигналів керування для драйвера крокового двигуна з метою переміщення каретки стенду за заданим законом – розробка інституту.

Датчики положення каретки:

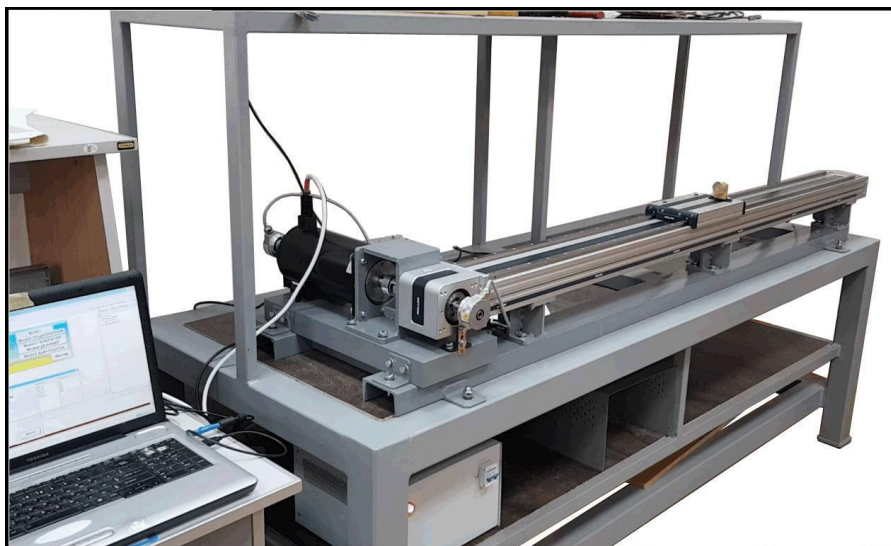
- Оптичний інкрементний датчик кута повороту вала двигуна Kuebler 5825 (6000 дискрет на оберт).
- Оптичний інкрементний датчик кута повороту вала двигуна Kuebler 5825 (36000 дискрет на оберт).
- Магнітний датчик лінійного переміщення каретки Kuebler Limes LI50 / B2 з розподільчою здатністю 5 мкм).
- Контактні датчики крайніх положень каретки стенду, які розривають "Ланцюг безпеки" (знимається електроживлення драйвера крокового двигуна при виході каретки за межі допустимого робочого діапазону переміщень) для реалізації аварійної зупинки.
- Програмно доступні контактні датчики положень каретки стенду на кінцях робочого діапазону, які використовуються для початкового

самокалібрування установки.

Вал двигуна з'єднаний із валом лінійного актуатора за допомогою спеціальної муфти з еластичними елементами. Передбачена можливість установки додаткового планетарного редуктора між двигуном та актуатором.

Компонування та розміщення:

- Низькочастотний стенд монтується на спеціальному постаменті.
- Вимірювальний блок «НАВКУ-3» і PC-сумісний комп'ютер встановлюються на окремому столі в безпосередній близькості від стенду.



- [1] О.А. Владимирський 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.-с.45-49. <http://doi.org/10.5281/zenodo.3860730>.
- [2] О.А. Владимирський. Низькочастотна віброкалібрувальна установка на основі лінійного актуатора з зубчастим ременем і кроковим двигуном. Науково-практична конференція «Безпека енергетики в епоху цифрової трансформації», ППМЕ ім. Г.Е.Пухова НАН України, Київ, 20.12.2019р. – С48-49.
- [3] Криворучко І. П. Кусково-лінійна апроксимація гладких плоских кривих методом січних. Електронне моделювання. 2022. 44 (5). С.51-60.

ДОСВІД РОЗРОБКИ КОНСТРУКЦІЇ СИСТЕМИ КОНТРОЛЮ РОЗМІРІВ ВИГОРОДКИ ЯДЕРНОГО РЕАКТОРА

Генеруючи потужності атомної енергетики нашої держави складають 15 ядерних енергоблоків з яких:

13 енергоблоків типа ВВЕР-1000,

2 енергоблока типа ВВЕР-440.

Більшість потужностей введені в експлуатацію у 80 – роки минулого століття, тобто стає нагальною проблема продовження експлуатації енергетичних ядерних блоків понад проектний термін з дотриманням законодавства України, вимог, норм і правил ядерної безпеки, рекомендацій МАГАТЕ.

Технічне обґрунтування продовження терміну експлуатації енергоблоків базується на експериментальних та теоретичних дослідженнях, направлених на контроль та діагностування технічного стану елементів конструкції енергоблоків. Особлива увага приділяється корпусу, шахті і вигородці реактора, які є одними з найвідповідальніших за відведення теплоти з активної зони і незамінюваних протягом всього періоду експлуатації елементів конструкції реактора (див. рис.1, рис.2).

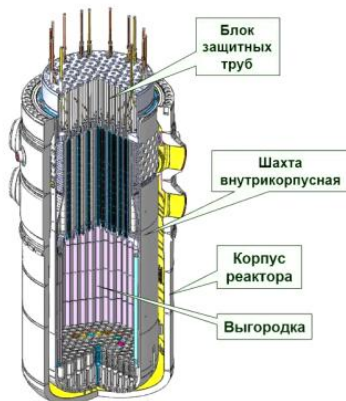


Рис.1. Конструкція реактора ВВЕР.

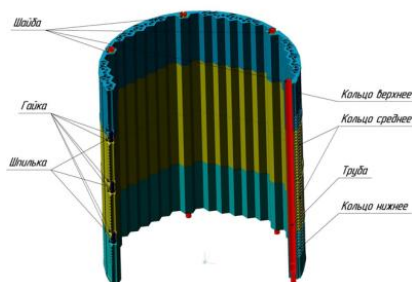


Рис.2. Загальний вид вигородки.

Особливістю експлуатації вигородки є наявність сильного нейтронного випромінювання і високих температур внаслідок радіаційного розігріву, які призводять до розпухання металу.

Вигородка реактору ВВЕР-1000 (див. рис.1) представляє собою захисну оболонку циліндричної форми висотою 4070 мм, зовнішнім діаметром 3470 мм, яка виготовлена із сталі 08X18H10T та має масу 35 тон. Вигородка складається з 4 або 5 кілець, скріплених між собою шпильками і зафіксованих між собою в плані один щодо одного штифтами. Внутрішня

конфігурація кілець вигородки повторює профіль граней периферійних касет активної зони з мінімальним зазором, створюючи таким чином умови для протікання теплоносія і відведення тепла від периферійних тепловиділяючих збірок.

Науково-технічними підрозділами ДП “НАЕК “Енергоатом” виконується комплекс робіт з розробки технічних, програмних засобів та методик для вимірювань геометричних розмірів вигородки ядерної установки. Розроблено та виготовлено пілотний зразок комплексу ВК-5, який застосовано при вимірюваннях на 4 енергоблоці ЗАЕС

До складу основного обладнання комплексу ВК-5 входять: модуль вимірювальний МВ (рис.3); пульт оператора ПО; барабан кабельний БК; комплект електричних кабелів і пневматичних шлангів; щит опорний.

МВ призначений для вимірювання відстаней між гранями вигородки в умовах робочого середовища реактора. На рис.3 наведено загальний вид МВ. За допомогою шарнірного вузла 19 МВ з'єднується з імітатором паливної збірки, який в свою чергу зістиковується з робочою штангою машини перезавантажувальної МП. МП забезпечує транспортування МВ в середину вигородки у заданому кутовому положенні відносно осі реактора на встановлені висотні відмітки для проведення вимірювань відстаней між протилежними гранями вигородки у горизонтальному положенні МВ. Обладнання МВ змонтовано на рамі, утвореній з продовжних 1-3 та поперечних 12-14 балок. До складу обладнання МВ входять засоби вимірювання відстані між протилежними гранями із встановленим на її кінцях перетворювачами відстані, лінійка опорна, датчики температури, інклінометр, чотири візки з роликівими опорами 4,5 з пневматичним приводом (рис.4), відеокамери ВК1-ВК4, блоки управління 9.

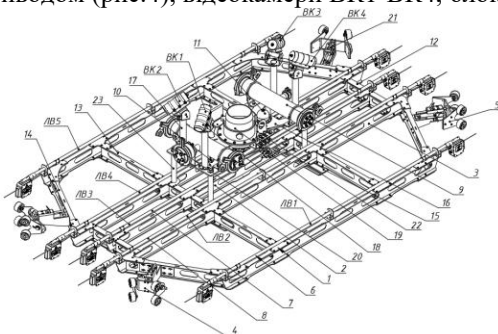


Рис. 3. Модуль вимірювальний.

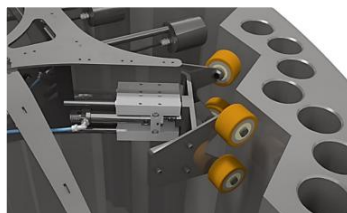


Рис.4. Роликіві опори.

В основу метода вимірювань покладена конструктивна особливість вигородки. Передбачається вимірювання відстаней між паралельними гранями вигородки. При цьому діапазон вимірювань обумовлений в основному відносно малими змінами форми вигородки та точністю позиціонування МВ у вигородці. Тому діапазон вимірювань датчиків ВК-5 на порядок менший (30 мм). Оскільки похибка вимірювань прямо пропорційна

діапазону вимірювань, існує можливість на порядок підвищити точність вимірювань шляхом використання датчиків з меншим діапазоном вимірювань.

Вимірювання здійснюються одночасно між 10 гранями вигородки за допомогою п'яти лінійок вимірювальних. Схема вимірювань передбачає вертикальне сканування вигородки з кроком 100 мм у початковому нульовому кутовому положенні МВ відносно осі реактора (рис.5) з подальшим послідовним поворотом МВ за годинниковою стрілкою на мінус 60° та проти годинникової стрілки на 60° з вертикальним скануванням у кожному кутовому положенні. Таким чином, за три вертикальних сканування здійснюються вимірювання відстаней між 30 гранями,

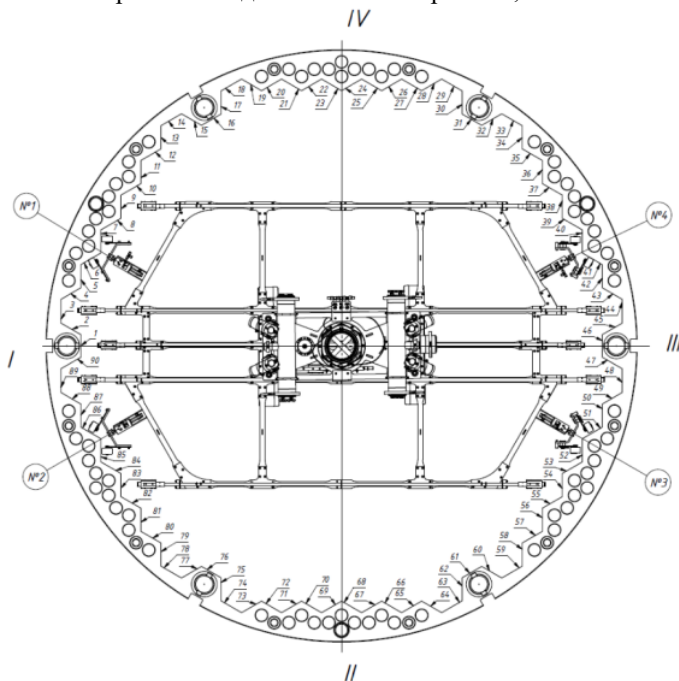


Рис.5. Схема проведення вимірювань.

Д.М. Семенюк

ВИЯВЛЕННЯ ПРИХОВАНИХ МІКРОВИТОКІВ В ТРУБОПРОВОДАХ ВНУТРІШНЬО БУДИНКОВИХ МЕРЕЖАХ ЗА ДОПОМОГОЮ УДОСКОНАЛЕНОГО ТЕРМОАКУСТИЧНОГО ТЕЧЕШУКАЧА А-10ТЗ

Витоки води в трубопроводах водопостачання та опалення - досить поширене явище. Як правило раніше, аварії сталюого трубопроводу викликані сильною корозією ділянки труби, але і при використанні полімерних трубопроводів аварійні витoki достатньо часто явище. Полімерні трубопроводи в новобудовах багатоквартирних та приватних будинках, почали масово використовувати в холодному та гарячому водопостачанні та системах опалення, замурувати в підлозі та стінах. Як показує багаторічний досвід діагностики прихованих трубопроводів, полімерні трубопроводи також мають ефект старіння, особливо під дією температури, час експлуатації систем опалення та гарячого водопостачання без витоків 15-20 років, а потім починається деградація матеріалу трубопровода та виникають мікровитоки.

Визначення місць ушкоджень в трубопроводах відноситься до найважливіших завдань експлуатації систем опалювання і водопостачання, особливо коли трубопроводи приховані. Враховуючи те, що велика частина таких комунікацій знаходиться під підлогою у діючих житлових приміщеннях, для цієї мети потрібне застосування спеціальних технічних засобів. Серед пристроїв, що давно використовуються для пошуку витоків в підземних трубопроводах, працюючих під тиском, широке поширення отримали акустичні і кореляційні течешукачі. Але методи та прилади, були розраховані на застосування в магістральних та розподільчих мережах водопостачання та опалення для трубопроводів із металу при значних витоках не менше 200-300 літрів на годину, не можуть застосовуватися на незначних витоках у внутрішньо будинкових мережах.

Великою перешкодою застосування кореляційного методу при пошуку в полімерних трубопроводах є велике затухання акустичного сигналу, а особливо при мікро витоку води при робочому тиску не виникає значний акустичний шум. Але шум від витоку в пошкодженні трубопроводу можливо збільшити за допомогою додавання стислого повітря. І при таких умовах можна вже застосовувати саме акустичний течешукач.

Акустичний течешукач.

Суть методу пошуку полягає в тому, що витікання води з повітрям або самого повітря через наскрізний дефект під тиском, супроводжується акустичними сигналами, які можна зафіксувати на самому трубопроводі або над ним.

За принципом дії, акустичний течешукач в чомусь схожий на медичний стетоскоп. Так само, як за допомогою стетоскопа лікар прослуховує звуки,

витікаючі від органів пацієнта, за допомогою течошукача фахівець прослуховує звуки, що доносяться від витоку. Спеціальний високочутливий датчик встановлюється на підлогу(стіну) і уловлює шуми, які потім посилюються електронним блоком і передаються в навушники оператора .

Під час пошуку акустичним течошукачем, шуми протікання води реєструються за допомогою датчика вібрації над трубопроводом послідовно уздовж ділянки, що діагностується, з кроком 0,05...0,2 М (рис.1). Координата витоку визначається по максимальному рівню вібросигналу в певній смузі частот рис.1. Оптимальна смуга частот залежить від типу трубопроводу і умов прокладення.

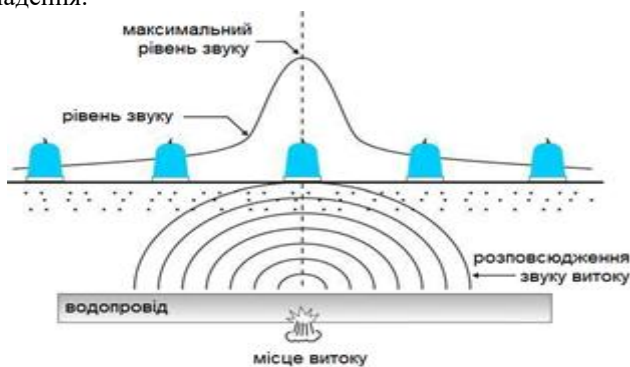


Рис.1. Визначення координати витоку води

Під час багаторічного досвіду, було визначено закономірність, що мікро витоки, при використанні стандартних акустичних течешукачів для підземних трубопроводів (течешукачі серій А-10, А-10Т виробництва ІПМЕ ім. Г.Е.Пухова НАН України [1 - 3]), генерують шум, що не фіксується вимірним блоком, але чути відмінності шуму у навушниках оператора. Було вирішено звернутися до розробника, з пропозицією, провести експериментальні виміри акустичного шуму від мікро витоку на реальних об'єктах в залежності від частоти . При практичних дослідях та застосування різних частотних фільтрів, прийшли до висновків, що акустичний шум від мікро витоку генерується на високих частотах. В новому експериментальному акустичному течешукачі А-10Т3 встановлено високочастотний фільтр з частотою 100-7000 Грц. На рис.2 зображено вимір акустичного шуму від мікрОВИТОКУ однаковим датчиком вібрації та в одній точці, що не фіксується приладом А-10Т (на дисплеї значення 0000), але фіксується приладом А-10Т3 (на дисплеї значення 0091). Після демонтажу кахелю місце витоку підтвердилося рис.3. Практичне застосування експериментального акустичного течешукача А-10Т3 з високочастотним фільтром дало змогу більш ефективно знаходити мікрОВИТОКИ води у внутрішньо будинкових трубопроводах та розширити застосування приладу.



Рис.2. Різниця результатів вимірювання рівня шуму течешукачами А-10 і А10Т3



Рис.3. Демонтаж кахелю та місце витоку.

- [1] А.А. Владимирский, И.А. Владимирский. Разработка термо-акустического течеискателя А-10Т. Моделирование та інформаційні технології. Збірник наукових праць. Інститут проблем моделювання в енергетиці НАН України. Вип. 57, Київ, 2010р.-с.31-34.
- [2] Владимирський О.А., Криворучко І.П. Пристрій для установки вібродатчика з магнітним тримачем на ґрунт при пошуку витоків. Патент на корисну модель № 142320; G01M 3/00, F17D 5/02. Публ. 25.05.2020р., Бюл. №10.
- [3] А.А. Владимирский, И.А. Владимирский, И.П. Криворучко. 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.

ДОЦІЛЬНІСТЬ ВИКОРИСТАННЯ ЗАКОНСЕРВОВАНИХ СВЕРДЛОВИН ДЛЯ ТЕПЛОПОСТАЧАННЯ

Використання геотермальної енергії зі свердловин вже успішно реалізоване в деяких країнах світу. Наприклад, в Ісландії, Новій Зеландії, США та Італії існують великі геотермальні електростанції, які використовують гарячу воду з глибоких свердловин для виробництва електро- та теплоенергії.

Ісландія і Сальвадор на 25 % забезпечують власні потреби в електричній енергії завдяки використанню геотермальної енергії, в Ісландії близько 93 % житлових приміщень опалюються завдяки геотермальній енергії [1].

В Україні налічується декілька сотень чи навіть тисяч законсервованих свердловин на території нафтогазових родовищ. Вироблені нафтові і газові родовища навіть після їх повного закриття з видобування вуглеводнів залишаються важливим енергетичним ресурсом [2-3].

Запаси термальних вод розвідані в Закарпатті, Криму, Прикарпатті, Харківській і Полтавській областях. За деякими даними, для видобутку термальних вод на території Дніпровсько-Донецької западини можуть бути використані 82 законсервовані свердловини [4].

На глибині близько 900 м середня температура вод становить 55°C, із глибиною залягання 5 км – від 80°C до 120°C.

Використовувати води з температурою понад 50°C можливо без теплового насосу [1].

Буріння глибоких свердловин є дорогим, тому використання існуючих законсервованих свердловин може суттєво знизити вартість створення нового теплогенеруючого об'єкта чи системи теплопостачання.

Використання геотермальної енергії свердловин сприятиме підвищенню енергетичної незалежності країни та зменшенню викидів забруднюючих речовин в атмосферне повітря.

Використання законсервованих свердловин може бути економічно вигідним для невеликих населених пунктів чи підприємств, розташованих поруч з такими свердловинами.

Створення та обслуговування нових теплогенеруючих об'єктів сприятиме створенню нових робочих місць та розвитку промислового виробництва в регіонах та країні в цілому.

В дослідженні [5] для визначення економічної ефективності теплонасосної станції на артезіанських водах був використаний показник середньозваженої собівартості теплової енергії за життєвий цикл (середньої вартості теплоенергії за життєвий цикл) LCOH (Levelised cost of heat) та показано, що економічно такі станції не можуть конкурувати з традиційними газовими котельнями, вартість газу для яких менша ніж для бюджетних організації чи промисловості.

Визначення характеристик доцільних для використання в теплопостачанні законсервованих нафтогазових свердловин вимагає подальшого дослідження з використанням методів економічного та енергетичного аналізу.

- [1] Долінський А.А. Геотермальна енергетика: виробництво електричної і теплової енергії / А.А. Долінський, А.А. Халатов // Вісник НАН України. – 2016. – № 11. – С. 76-86. – <http://dspace.nbuv.gov.ua/bitstream/handle/123456789/109877/10-Dolinskiy.pdf?sequence=1>
- [2] Долінський А.А. Перспективні напрямки використання геотермальних ресурсів в Україні / А.А. Долінський, Д.М. Чалаєв О.О., Переяславцева Н.Б. Сильнягіна // Енергетика і автоматика. – 2020. – №5. – С. 42-56. <http://dx.doi.org/10.31548/energiya2020.05.042>
- [3] Петренко А. Інвестиції в газовидобувну галузь: три шляхи для інвестора [Електронний ресурс] / А. Петренко // Юридична газета Online. – 22 квітня 2020 р. – Режим доступу : <https://yur-gazeta.com/publications/practice/energetichne-pravo/investiciyi-v-gazovidobuvnugaluz-tri-shlyahi-dlya-investora.html>
- [4] Шурчкова Ю.О. Економічна ефективність систем геотермального теплопостачання в залежності від тарифів на теплоту та електроенергію / Ю.О. Шурчкова, А.О. Підручна // Проблеми загальної енергетики. – 2020. – Вип. 2(61). – С. 43-50. <https://doi.org/10.15407/pge2020.02.043>
- [5] Станиціна В.В. Визначення середньої вартості теплової енергії за життєвий цикл теплонасосної станції на артезіанських водах. Зб. тез XXXVII науково-технічної конференції молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, м. Київ, 15 травня 2019 р. / ІПМЕ ім. Г.Є. Пухова НАН України. 2019. С. 67-68.

В.В. Станиціна, В.О. Артемчук

ПРОБЛЕМА ДЕКАРБОНІЗАЦІЇ СИСТЕМ ТЕПЛОПОСТАЧАННЯ УКРАЇНИ З ВРАХУВАННЯМ ОСОБЛИВОСТЕЙ НАЦІОНАЛЬНОЇ ЕКОНОМІКИ

У світі все більше уваги приділяється проблемі глобальних змін клімату, на законодавчому рівні в багатьох країнах декларується перехід до низьковуглецевої економіки з метою досягнення вуглецевої нейтральності, в тому числі і в Україні [1-2,4].

Сфера теплопостачання забезпечує життєдіяльність населення, всіх організацій та установ, що обумовлено кліматичними умовами України. До 2022 р опалювальними котельними споживалось більше 4 млрд м³ природного газу, близько 3 млрд м³ - ТЕЦ. Населення для потреб теплопостачання та приготуванні їжі в у 2016-2021 рр. споживало близько 11 млрд м³ природного газу – третину від всього обсягу природного газу, що споживалось в країні. Таким чином, близько половини природного газу в країні споживалось для цілей теплопостачання.

В Україні внаслідок військових дій постраждало чи було зруйновано багато об'єктів систем теплопостачання, тому постає проблема їх відновлення, але при цьому необхідно враховувати те, що Україна взяла на себе зобов'язання виконувати заходи з протидії зміні клімату, зокрема щодо зменшення викидів забруднюючих речовин.

Ракетні обстріли об'єктів енергетики продемонстрували вразливість системи теплопостачання, яка складається з потужних теплогенеруючих об'єктів. З іншої сторони, для великих спалювальних установок розроблені та впроваджуються технології/заходи для зменшення викидів забруднюючих речовин, в першу чергу пилу, оксидів сірки та азоту (зменшення викидів останніх актуальне для газоспалюючих котлів).

Також критичним є залежність економіки країни від імпортних енергоресурсів. Збільшення споживання місцевих та відновлювальних джерел енергії сприятиме підвищенню рівня енергетичної безпеки держави та зменшенню вартості імпортованих товарів.

Однією з великих проблем теплопостачання є стан тепломереж, більше третини з них відносяться до ветхих, що зрештою збільшує питомі витрати паливно-енергетичних ресурсів (ПЕР) на виробництво теплоенергії.

Ще однією з проблем ЖКХ є, в більшості випадків, низька енергоефективність будинків та споруд, що знову ж таки призводить до перевитрат ПЕР для забезпечення комфортних температурних умов в будинках, тому є потреба в проведенні термомодернізації будинків та споруд.

Однією з технологій теплопостачання, що широко впроваджується в світі, є використання різних типів теплових насосів. Проте в Україні відсутнє виробництво потужних теплових насосів, а ті малопотужні теплові насоси,

які випускаються вітчизняною промисловістю, виготовляються з використанням значної мірою імпортних складових та матеріалів, що відображається на їх вартості. Теплові насоси виробництва країн ЄС, Японії та США в разі дорожчі за українські чи китайські, тому без підтримки держави масового їх впровадження не варто очікувати [3].

При впровадженні нового теплогенеруючого обладнання та технологій для заміщення пошкодженого чи зруйнованого потрібно враховувати як їх економічну ефективність, так і енергетичну, а також наявність паливно-енергетичних ресурсів, обмеженість фінансування, задекларовані на законодавчому рівні зменшення викидів забруднюючих речовин, в т.ч. парникових газів.

Впровадження технологій, які сприятимуть переходу до кліматично нейтральної економіки, вимагає великих інвестицій в об'єкти системи тепlopостачання. Тому необхідним є визначення ефективності та доцільності їх впровадження для умов України, прогнозування обсягів зниження викидів ПГ внаслідок їх впровадження, що і визначає актуальність проведення відповідних досліджень.

- [1] Концепція «зеленого» енергетичного переходу України до 2050 року. [Електронний ресурс] // Сайт Міндовкілля <https://mepr.gov.ua/news/34424.html>
- [2] Остап Семерак: Уряд України підтримав Стратегію низьковуглецевого розвитку України до 2050 року. 12.04.2021. URL: <https://www.kmu.gov.ua/news/ostap-semerak-uryad-ukrayini-pidtrimav-strategiyu-nizkovugleceвого-rozvitku-ukrayini-do-2050-roku>
- [3] Станиціна В.В. Визначення середньої вартості теплової енергії за життєвий цикл теплонасосної станції на артезіанських водах. Зб. тез XXXVII науково-технічної конференції молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, м. Київ, 15 травня 2019 р. / ІПМЕ ім. Г.Є. Пухова НАН України. 2019. С. 67-68.
- [4] Що означатиме курс на декарбонізацію для інвестицій у відновлювальну енергетику. 12.04.2021. URL: <https://vkr.ua/publication/shcho-oznachatime-kurs-na-dekarbonizatsiyu-dlya-investitsiy-u-vidnovlyvalnu-energetiku>

І.П. Криворучко

ОСОБЛИВОСТІ ФОРМУВАННЯ СИГНАЛІВ УПРАВЛІННЯ КРОКОВОГО ДВИГУНА У МІКРОКРОКОВОМУ РЕЖИМІ

Кроковий двигун (КД) використовується у електромеханічних системах, де вимагається точне позиціонування робочого органу, механічно зв'язаного з ротором КД. Мінімальне кутове переміщення ротора для повного кроку визначається його конструкцією і може бути від 30 до 0,9 град. При цьому у кожний момент магнітний потік створює лише одна з двох статорних обмоток. На рис. 1 показано схематично роботу КД з величиною повного кроку 30 град.

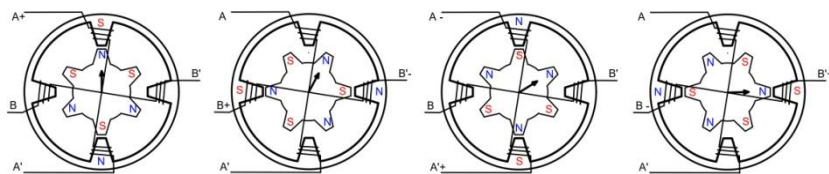


Рис. 1 Схема роботи 2-фазного 4-полюсного КД

Однак для більш точного позиціонування застосовують мікрокроковий режим, при якому дві статорні обмотки заживлюються одночасно, але з розподілом струмів на певну величину. При цьому сумарний вектор магнітного потоку займає додаткові до основних, як для повного кроку, проміжні положення. Для забезпечення обертаючого магнітного поля статорні обмотки заживлюють ступінчасто-змінними синусоїдами U_a та U_b зміщеними між собою на кут $\pi/2$.

Для отримання такого вигляду синусоїди у роботі [1] пропонується використовувати блок Quantizer (MatLab). Аналогічний підхід розглядається у роботі [2]. Для цього, пропонується використовувати формулу:

$$U_a = U \cdot q \cdot \text{round} \left(\frac{\sin \left(\frac{\pi}{2} \cdot f \cdot t \right)}{q} \right) \quad (1)$$

де q – крок квантування, f – частота напруги живлення, функція $\text{round}(x)$ – повертає округлені до цілого елементи масиву x , U – амплітуда. Рівняння для U_b має подібний вигляд, лише замість $\sin()$ використовують $\cos()$. На рис.2 наведені результати моделювання обох напруг живлення U_a та U_b , розрахованих за рівнянням (1) (для $U=1$), модуль результуючого вектору цих напруг та змодельоване кутове переміщення ротора. Але при такому способі формування сигналу управління часові інтервали, які відповідають поточним фіксованим значенням сигналів різних обмоток не рівні між собою. Через це, наприклад, для часового інтервалу 0,054 – 0,105 с значення функції U_a незмінне, а напруга U_b має чотири різних значень. Тому модуль сумарного вектора цих напруг змінюється у часі. Розрахунки проводилися для режиму мікрокроку величини $1/4$. Як видно з малюнку, амплітудне значення

результуючого вектора напруги змінюється у часі. Максимальне відхилення досягає 12%. Вочевидь, нестабільність цього параметру викликає додаткову мінливість магнітного моменту M_E та нестабільність мікрокроку.

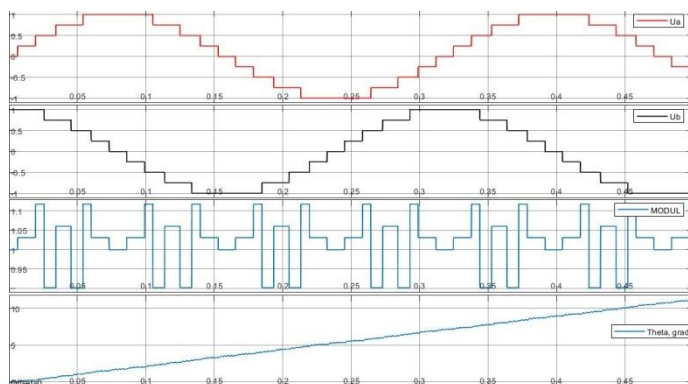


Рис 2. Форма сигналів управління, модуля сумарного вектора та кутове переміщення ротора для випадку розрахунків за формулою (1).

Для усунення цього небажаного ефекту пропонується представлення вхідного сигналу $F(t)$ як фази з подальшим послідовним поділом її на відрізки рівні за величиною $\pi q/2$ і фіксації цих значень в межах кожного відрізка. Чим скоріше змінюється в часі $F(t)$, тим більше відрізків формується за одиницю часу. Потім обраховуються значення тригонометричної функції для кожного із розрахованих значень аргументу $Angle$. Для прикладу вхідну функцію покладаємо рівною $F(t)=kt$, тоді:

$$Angle = \left(\frac{\pi q}{2}\right) \cdot \text{round}(2 \cdot (k \cdot t) / \pi q) \quad (2)$$

де $Angle$ – кут, рад; k – коефіцієнт. Результати моделювання роботи КД для цього випадку наведені на рис.3.

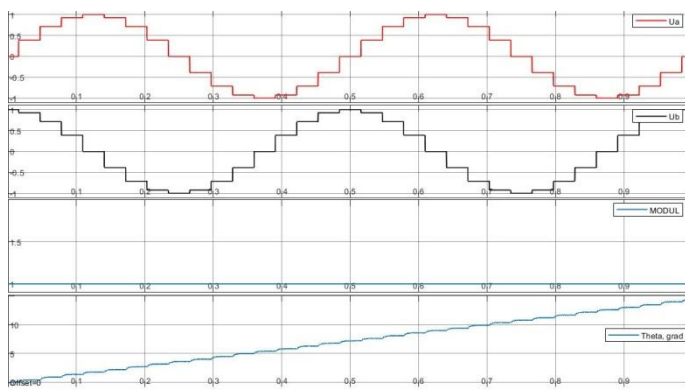


Рис 3. Форми сигналів управління, модуля сумарного вектора та кутове переміщення розрахованих за (2)

На графіку для модуля сумарного вектора напруги живлення часових змін його величини вже не спостерігається. Зображені на рис.2 та рис.3 графіки були отримані з використанням імітаційної моделі з використанням блоків Simulink наведеної на рис.4.

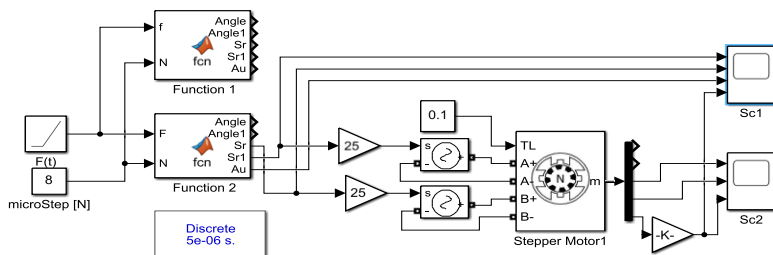


Рис 4. Блок-схема моделі в середовищі MatLab/Simulink для порівняння обох способів формування сигналів управління.

Порівняння графіків кутового переміщення на рис.2 та рис.3 показує більш чітко виражену «кроковість» (періодичність) сигналів. У першому випадку кут зростає ступінчато, але не монотонно. Крім того, з'являються проміжні кутові положення ротора не передбачені алгоритмом управління. У другому випадку величина кута зростає ступінчато, з величиною $\frac{1}{4}$ кроку (0,45°).

Висновки

Запропоновано модифікацію відомого способу формування сигналів управління для мікрокрокового режиму КД. Моделювання роботи КД із застосування цього способу показує стабільність модуля сумарного вектора діючої статорної напруги. Передбачено використання цього способу формування сигналів управління КД для забезпечення коливального руху, як основного типу механічного переміщення каретки віброкалібрувальної установки [1].

- [1] Владимирський О.А., Владимирський І.А., Івашенко А.П., Криворучко І.П., Розробка структури низькочастотної автоматизованої вібро-калібрувальної установки НАВКУ-3. Моделювання та інформаційні технології. Збірник наукових праць. Інститут проблем моделювання в енергетиці НАН України. Вип. 89, Київ, 2019 р.-с.45-49.
- [2] Кавалеров Б.В, Фалалеев Д.В. Линеаризация математической модели гибридного шагового двигателя // Вестник ПНИПУ. Электротехника, информационные технологии, системы управления. – 2021. - №40. с.130-148
- [3] Степочкин А.О. Моделирование работы шагового электрического двигателя гибридного типа в пакете Simulink // Известия ТГУ. Технические науки. - 2018. - №8. с. 308 – 315.

КОНЦЕПЦІЯ ПОБУДОВИ ЖОРСТКО РЕЗИЛЬЄНТНОЇ ЕЛЕКТРОЕНЕРГЕТИЧНОЇ СИСТЕМИ УКРАЇНИ

Забезпечення надійного, безпечного та доступного постачання електроенергії має важливе значення для економічного зростання та розвитку. Зазвичай енергосистема знаходиться під постійними загрозами низки природних, технологічних і антропогенних дій, які можуть спричинити будь-що: від перебоїв у електропостачанні до хронічного дефіциту обсягів електропостачання. Для розробників політики, планувальників і системних операторів надзвичайно важливо захистити свої системи, планувати та інвестувати в підвищення стійкості енергетичного сектора у своїх країнах.

Завдяки цілісному плануванню стійкості можна передбачати загрози та навантаження на енергосистему, готуватися і адаптуватися до них. Планування стійкості енергосистеми передбачає визначення загроз, впливів та вразливих місць, а також розробку стратегії пом'якшення таких загроз.

Стійкість (resilience) енергетичного сектору – це його здатність передбачати, готуватися та адаптуватися до мінливих умов, а також протистояти, реагувати та швидко відновлюватися після збоїв за допомогою адаптивного та цілісного планування та технічних рішень [2].

Таке визначення стійкості не враховує терористичних та мілітарних загроз енергетичному сектору, які спостерігаються та реалізуються в багатьох країнах сучасного світу [1].

Враховуючи винятковий характер дії таких загроз введемо поняття жорсткої стійкості (жорсткої резильєнтності) енергетичного сектору – це його стійкість не лише до загроз низки природних, технологічних і антропогенних дій, а й до загроз терористичних та мілітарних дій, спрямованих на масштабне руйнування енергетичної інфраструктури.

Енергетичний сектор, якому властива жорстка стійкість будемо називати жорстко стійким (жорстко резильєнтним), а належну йому електроенергетичну систему (ЕЕС) – жорстко резильєнтною або, надалі коротко, резильєнтною.

Декарбонізація є базовою стратегією розвитку ЕЕС розвинених країн світу. В умовах руйнівних дій РФ така стратегія розвитку ЕЕС України не є самодостатньою. Потребує обов'язкового втілення ще одна енергетична стратегія - побудова резильєнтної ЕЕС, тобто такої ЕЕС, потенційні масштаби ураження якої є суттєво обмеженими, а наслідки ураження ліквідуються значно швидше ніж в сьогоdnішніх умовах.

Нижче представлена концепція резильєнтності як стратегія випередження викликів і загроз, умову збереження і розвитку електроенергетичного сектору України.

Побудову резильєнтної ЕЕС необхідно починати з регіонального рівня. В кожній регіональній ЕЕС має бути встановлений такий обсяг генераторів

(СЕС, ВЕС, АЕС на малих модульних реакторах (МР) або мікро-МР) та систем зберігання енергії (ГАЕС (нові), ВАЕС, Li-Ion батареї, гравітаційні системи зберігання енергії, водневі накопичувачі), 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 ЕЕС України або таких дій на сусідні регіональні ЕЕС.

Визначення меж ЕЕС регіону встановлюється відповідно до таких двох чинників. Відповідно до вимог безпеки резильєнтність ЕЕС є більшою у разі поділу всієї системи на регіональні ЕЕС меншого розміру. Разом з тим, кожна регіональна ЕЕС повинна задовольняти попит на електроенергію споживачів, які спроможні відшкодувати експлуатаційні та капітальні витрати регіональних енергетичних компаній. Таким чином межі ЕЕС регіону встановлюються на основі компромісу між зазначеними вимогами.

Кожна регіональна ЕЕС має можливість працювати ізольовано або у складі ЕЕС України.

ЕЕС України підтримує регіональні ЕЕС узгодженими обсягами маневрових потужностей і їх резерву та забезпечує постачання електроенергії підприємствам промислової, будівельної, транспортної та іншим видам економічної діяльності, які не приєднані до регіональних ЕЕС. У випадках руйнування окремих регіональних ЕЕС загальнодержавна ЕЕС України забезпечує нагальні потреби таких регіонів в електроенергії.

В резильєнтній ЕЕС України механізми управління господарською діяльністю енергетичних компаній мають бути єдиними для всіх учасників ринку як на загальносистемному, так і на регіональному рівнях. При цьому можуть застосовуватись механізми декомпозиції торговельних площадок.

Розроблення математичних моделей регіональних ЕЕС та моделі резильєнтної ЕЕС України є необхідною умовою планування їх оптимального розвитку. На сьогодні завершено розроблення математичної моделі регіональних ЕЕС з великими частками виробництва електроенергії установками ВЕС, СЕС, АЕС на малих- або мікро-МР, а також наявності систем збереження енергії. Таким чином створено інструмент планування розвитку генеруючих потужностей та систем збереження енергії в перспективних регіональних ЕЕС.

- [1] Mitoulis S.-A., Argyroudis S., Panteli M., Fuggini C., Valkaniotis S., Hynes W., Linkov I. Conflict-resilience framework for critical infrastructure peacebuilding // Sustainable Cities and Society. – 2023. – vol. 91, 104405. URL <https://doi.org/10.1016/j.scs.2023.104405>.
- [2] 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>.

А.В. Давидюк

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДАНИХ ДАТАЦЕНТРІВ В УМОВАХ ВОЄННОГО СТАНУ

Забезпечення інформаційної безпеки та кібербезпеки є одним з основних завдань національної безпеки України [3]. З розвитком інформаційних процесів та їх автоматизації збільшуються обсяги даних, які потрібно обробляти та зберігати. Для задоволення потреб у роботі з великими обсягами даних ринком послуг була створена інфраструктура центрів збереження даних (датацентрів). Датацентри пропонують клієнтам ряд послуг для роботи з даними з використанням технологій хмарних обчислень, зокрема інфраструктура як послуга (IaaS), платформа як послуга (PaaS), програмне забезпечення як послуга (SaaS), безпека як послуга (SECaaS) [5].

Використання хмарних ресурсів дало змогу оперативно масштабувати IT інфраструктуру організації під збільшення її потреб та планувати витрати на IT та кібербезпеку. Водночас використання хмарних сервісів дає змогу економити багато фінансових ресурсів. Це все робить популярним використання послуг датацентрів. Користувачами датацентрів є державні та приватні організації, об'єкти критичної інфраструктури, ряд державних органів мають або створюють власні центри обробки даних [4].

В умовах мирного часу використання датацентрів, що відповідають вимогам TIER є досить надійним рішенням для роботи з даними [1]. Однак в умовах війни з РФ виникають додаткові ризики для роботи датацентрів. До таких ризиків можна віднести проблеми електропостачання, Інтернет доступу, проблеми обслуговування (спеціалісти, доставка обладнання, сервісні центри), ракетні обстріли, захоплення ворогом приміщень та обладнання датацентрів тощо.

Виникає питання оброблення таких ризиків. Одним з найнефективніших шляхів такого управління ризиками є резервування за кордом. Однак і це має ряд проблем, зокрема значні фінансові витрати, обчислювальні можливості закордонних датацентрів, пропускну спроможність каналів передачі даних тощо. Окремою проблемою є резервування даних з обмеженим доступом, так як існує заборона щодо використання незахищених каналів передачі даних при їх обробці [2]. Додатковою проблемою є пріоритизація інформаційних активів в датацентрах, зокрема адміністратор датацентру не має доступу до логічного контейнера (тенанта) клієнта, і не може вирішити, яку інформацію потрібно зберегти першочергово в умовах обмеженого часу для створення бекапу. Також не вирішеним є питання щодо дій у випадку настання ризиків захоплення ворогом, а саме в тому, що матиме менші наслідки самому знищити датацентр чи залишити ворогу.

Всі ці проблеми спонукають до постановки задачі з забезпечення стійкості датацентрів в Україні. В рамках цієї задачі доцільно розглядати інформацію як певну матерію, що має об'єм - B_{inf} , який постійно зростає з певною швидкістю - V_{inf} . Інфраструктуру датацентрів (обчислювальні

потужності) – як контейнер для цієї матерії, об'єм B_{dc} якого збільшується з меншою швидкістю V_{dc} ніж обсяг даних.

Такий підхід дає можливість описати перелік станів стійкості до ризику втрати даних датацентрів. Наприклад стан, за якого $B_{dc} > B_{inf}$ та $V_{inf} > V_{dc}$ вважається сталим функціонуванням датацентру. Однак в умовах реалізації вищевказаних ризиків воєнного стану можливі такі умови, коли $B_{inf} > B_{dc}$ та $V_{inf} > V_{dc}$, що не дасть можливості зберегти дані і вони будуть втрачені. Рішенням такої проблеми можуть бути процедури вивільнення ресурсів датацентру, або їх швидке нарощування. Швидко збільшити ресурси в умовах воєнного стану є складним завданням з урахуванням термінів поставок необхідного обладнання. Вивільнення ресурсів, шляхом видалення чи перенесення даних також займе чимало часу. Також варто зазначити, що майже не можливо передбачити всі наслідки втрати даних.

Таким чином доцільно розглядати можливості державно-приватного партнерства для забезпечення стійкості інфраструктури датацентрів, зокрема механізми надання обладнання, обчислювальних потужностей датацентрами один одному з метою найшвидшого вирішення кризових ситуацій. Механізми такої взаємодії можна описати в рамках концепції стійкості датацентрів в умовах воєнного стану. В даній концепції необхідно врахувати ризики розміщення датацентрів, фізичні загрози, ризики безпеки, оцінки ресурсів для оброблення ризиків, необхідні кооперації заради стійкості.

Концепція повинна стати основою для розробки процедур евакуації, знищення з метою недопущення захоплення, резервування персоналу, резервування обладнання, переміщення обладнання з подальшим розгортанням на резервному майданчику (наприклад іншого датацентру) шляхом інтеграції власної інфраструктури в існуючу.

Досвід таких процедур може стати унікальним для України та інших країн, на території яких ведуться бойові дії, є частими стихійні лиха чи наявні кліматичні проблеми.

- [1] Tier certification overview. Digital Infrastructure Authority | Tier Certification & Training | Uptime Institute. URL: <https://uptimeinstitute.com/tier-certification>
- [2] Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : Постанова Каб. Міністрів України від 29.03.2006 р. № 373 : станом на 21 жовт. 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/373-2006-п#Text>
- [3] Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII : станом на 31 берез. 2023 р. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>
- [4] Про реалізацію експериментального проекту щодо функціонування Національного центру резервування державних інформаційних ресурсів : Постанова КМУ від 08.02.2021 р. № 94 : станом на 11 квіт. 2023 р.
- [5] Про хмарні послуги : Закон України від 17.02.2022 р. № 2075-IX. URL: <https://zakon.rada.gov.ua/laws/show/2075-20#Text> (дата звернення: 24.04.2023).

ЗАХИСТ ВІД АТАК ПІДРОБКИ ТА ПЕРЕХОПЛЕННЯ ЗА ДОПОМОГОЮ JWT ДЛЯ НЕКОНФІДЕЦІЙНОЇ ІНФОРМАЦІЇ

У сучасному світі інформаційних технологій та веб-додатків, безпека даних та їх передача зіграють важливу роль у функціонуванні систем. Одним з ключових інструментів для забезпечення безпеки даних є JSON Web Token (JWT). JWT використовується в якості механізму аутентифікації, а також для передачі та зберігання інформації [2]. В цій статті ми розглянемо аспекти використання JWT для запобігання атакам типу «spoofing attack» та «Man-in-the-Middle» (MITM) у контексті передачі неконфіденційної інформації між об'єктами електроенергетичної інфраструктури. Також обговоримо структуру JWT, його переваги та недоліки, а також особливості використання асиметричних підписів для забезпечення безпеки токенів.

Атака підробки

Так, існує такий вид хакерської атаки, як передача недостовірної інформації в систему, маскуючись під існуючого користувача. Цей вид атаки називається атакою підробки (spoofing attack).

Атака підробки полягає у тому, що зловмисник використовує підроблені дані, щоб приховати свою справжню ідентичність та пройти автентифікацію як інший користувач. Такі атаки полягають у підробленні чи модифікації інформації, що передається між об'єктами електричної інфраструктури, з метою отримання несанкціонованого доступу або внесення змін у роботу системи.

Атака перехоплення, також відома, як Man-In-The-Middle (MITM)

Атака перехоплення, або Man-In-The-Middle (MITM) атака, відбувається, коли зловмисник незаконно втручається в процес передачі інформації між двома об'єктами електричної інфраструктури. Ці об'єкти можуть включати різні елементи, такі як сенсори, пристрої збору даних, контролери та системи управління. У контексті електричної інфраструктури, MITM атаки представляють особливу загрозу, оскільки вони можуть призвести до перешкод у роботі систем, неправильного управління ресурсами та, у крайньому випадку, до аварій чи збоїв у системі електропостачання.

Зловмисник, який виконує MITM атаку, може перехоплювати, зчитувати, модифікувати або відправляти фальшиві дані, що передаються між об'єктами електричної інфраструктури. Це може включати перехоплення команд управління, зміну інформації про споживання електроенергії або навіть введення шкідливих команд для завдання шкоди системі.

Наслідки

У випадку spoofing атак, зловмисник може змінювати інформацію, яка передається між лічильником та сервером, щоб спотворити дані про споживання електроенергії або навіть створити ілюзію, що електроенергія

споживається, коли фактично ніякої споживання не було. Це може призвести до збитків для електропостачальної компанії та недостовірної звітності для споживачів. Крім того такі атаки в комбінації можуть призвести до ситуації, коли якийсь об'єкт критичної інфраструктури зруйновано, але дані за нього передаються схожі на правдоподібні, але від хакерської групи. При цьому хакер може передавати сигнал небезпеки від працюючого об'єкта для того, щоб заплутати ремонтні бригади і збільшити час на відновлення системи. А також це може призвести до помилкових відключень працюючих систем і не відключень зруйнованих систем. Наслідки таких ситуацій передбачити майже неможливо. [4]

Для захисту від такого типу атак при передачі інформації можна використати JWT (або JSON Web Token) [5] - це стандарт відкритого формату для представлення токенів доступу, що передаються між сторонами у форматі JSON. JWT зазвичай використовуються для аутентифікації та авторизації користувачів в розподілених системах, таких як мікросервіси та веб-додатки.

Приклад JWT:

```
eyJhbGciOiJIUzUxMiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxNDQ0MTEyMzY3O  
DkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoiYWRtaW4iOnRydWU9ImhhdCI6MTUxNjI  
zOTAyMn0.Ut-yp7_LSREtYEEVFaf1oPDF2QB0EobqDCMmpptzkBuP2dZtbcJb  
JFBEv1R1w81rBo83McxSSxyGDPpwiDTIP3v3rpRrdgurqNAXNd4Yj1uFcKMa7  
ik3GIAU7g9Qsc2I3wDeYs3FV8OOKXHB69jddlQxWJ6t01oZedUTgqZnvH6psm  
a6g5RhvR331jvb7FWUYH1Yz2KbspNrgCNGdkr4CXEDxEtUeCuVUoc1JxQkIo  
s5g9eHujeebdnjfL9reGCcKmVEfdwf0ENAB_9wLoU0kS7AEvH2Dd0o2sCxAgz  
F9TQeBXCLEFAD_yA4RbQ1kOW_3TEg3cd3gbNNea_Wjzud_w
```

JWT складається з трьох частин: заголовку, корисної навантаження та підпису. Вони розділені символом крапка: «.». У заголовку міститься тип токена та алгоритм шифрування, який використовується для створення підпису. Корисна навантаження містить інформацію про користувача та додаткову інформацію, яку можна передавати за бажанням. Підпис складається з хешу заголовку та корисної навантаження, заснованого на використаному алгоритмі шифрування.

JWT є популярним засобом забезпечення безпеки веб-додатків та мікросервісів через свою простоту та ефективність. Використання JWT дозволяє зменшити навантаження на сервер, оскільки вся необхідна інформація про користувача міститься в токені, що передається у кожен запит.

JWT можна використовувати для запобігання атак типу spoofing attack та MITM.

Для захисту від атаки spoofing attack, JWT можна використовувати для передачі токенів доступу замість використання реп'яшків (cookies). Куки можуть бути підмінені або викрадені, що може дозволити зловмиснику використовувати токени доступу. З використанням JWT, токени зберігаються на стороні клієнта, наприклад, в локальному сховищі, і передаються з кожним запитом на сервер. За допомогою цього підходу можна зменшити

ризик підміни токенів доступу, оскільки токени зберігаються на стороні клієнта, а не сервера.

Для запобігання spoofing attack JWT можна захистити, використовуючи підпис та перевірку цілісності. При створенні токена, корисна навантаження та заголовок включаються до підпису, що гарантує, що токен було створено легітимною стороною та ніхто не може змінити корисну навантаження. При отриманні токена, сервер може перевірити підпис, щоб забезпечити, що токен було створено дійсною стороною і не було змінено під час передачі. А це критично для відбиття зазначених вище атак.

Крім того для створення підпису можна використовувати алгоритми з асиметричними ключами. Наприклад RS512. Він є одним з алгоритмів підпису для JWT, що використовує асиметричний шифрування. Асиметричний криптографічний ключ, також відомий як пара ключів, складається з двох ключів: приватного та публічного. Приватний ключ залишається в таємниці, тоді як публічний ключ може бути опублікований. Використання JWT з асиметричним підписом має кілька переваг:

Легкість використання: JWT є простим у використанні і легко інтегрується з більшістю сучасних технологій.

Розширюваність: JWT дозволяє передавати будь-яку корисну інформацію у вигляді токена, включаючи інформацію про систему, яка надсилає повідомлення, власне дані, які необхідно передати.

Швидкість: У порівнянні з шифруванням, асиметричний підпис JWT швидший, оскільки не потребує розшифрування даних, тільки перевірку цифрового підпису [1]

Безпека: забезпечує дуже високий рівень безпеки, оскільки підписання відбувається приватним ключем, а перевірка - публічним ключем. Це означає, що навіть якщо хакер підкупить або вкраде публічний ключ, він не зможе створити власний підпис і підробити JWT.

Надійність: JWT дозволяє перевіряти токен на стороні сервера, що дозволяє перевірити цілісність даних, що передаються.

Сумісність: Це означає, що його можна використовувати з великою кількістю мов програмування [3].

Але використання JWT в контексті передачі інформації має також деякі недоліки:

1. JWT не підтримує шифрування, тому конфіденційна інформація, що міститься в JWT, може бути доступна для всіх сторін, які мають доступ до токена.

2. JWT може стати засобом зловмисників, якщо використовується не належним чином. Недостатня перевірка токенів та незахищене зберігання ключів може призвести до підроблення токенів та вторгнення в систему.

3. Підпис може складати відчутну частину об'єму даних

ВИСНОВОК

JWT підходить для запобігання атакам типу spoofing attack та MITM в контексті передачі неконфіденційної інформації. Але у випадку, коли інформація конфіденційна, потрібно використовувати шифрування.

- [1] A. Rahmatulloh, R. Gunawan, F. M. S. Nursuwars Performance comparison of signed algorithms on JSON Web Token. The 1st Siliwangi International Conference on Innovation in Research 2018 (SICIR) 14 August 2018, Bandung, Indonesia /IOP Conference Series Materials Science and Engineering / Vol.550
- [2] URL: (PDF) Performance comparison of signed algorithms on JSON Web Token (researchgate.net) (date of access: 10.04.2023).
- [3] Json Web Token
- [4] URL: <http://jwt.io> (date of access: 10.04.2023).
- [5] Libraries for Token Signing/Verification
- [6] URL: <https://jwt.io/libraries> (date of access: 10.04.2023).
- [7] Mark E. Beatty, Scot Phelps Blackout of 2003: Public Health Effects and Emergency Response. Public Health Reports. 2006 Jan-Feb; Vol. 121, no. 1. P. 36-44.
- [8] URL: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1497795/> (date of access: 10.04.2023).
- [9] Yinhao Xiao, Yizhen Jia, Chunchi Liu, Xiuzhen Cheng Edge Computing Security: State-of-The-Art and Challenges. Proceedings of the IEEE. 2019. Vol. 107, Issue 8. P. 1608-1631
- [10] URL: <https://ieeexplore.ieee.org/document/8741060> (date of access: 10.04.2023).

АНАЛІЗ ВИЗНАЧЕНЬ ТЕРМІНА "РЕЗИЛЬЄНТНІСТЬ" ТА ЙОГО ІНТЕРПРЕТАЦІЙ У МІЖНАРОДНИХ СТАНДАРТАХ

Анотація

У цій доповіді розглядається термін "резильєнтність" (англ. resilience), як він визначається в різних міжнародних стандартах, з акцентом на стандартах, розроблених Міжнародною організацією зі стандартизації (ISO) та Національним інститутом стандартів і технологій (NIST). Аналізом контекстів, в яких ці організації використовують термін "резильєнтність", і наданням прямих цитат зі стандартів, забезпечується комплексне розуміння змісту його різних інтерпретацій і застосувань.

Вступ

Резильєнтність стала критично важливою концепцією в різних галузях, включаючи інформаційну безпеку, енергетику, державне управління, інженерію, екологічний менеджмент та управління ризиками. Розуміння того, як міжнародні стандарти застосовують і трактують резильєнтність, може дати уявлення про розробку більш надійних і адаптивних систем. У цьому дослідженні розглядається використання терміну "резильєнтність" у міжнародних стандартах, зосереджуючись на системах ISO та NIST, та висувається і доводиться теза, що резильєнтність, хоч і застосовується в різних контекстах, послідовно підкреслює здатність відновлюватися, адаптуватися і пристосовуватися до атак, несприятливих обставин, внутрішніх збоїв або змін. Можливість абсорбувати будь-які негативні впливи, спрямовані на порушення гомеостазу, вміння видозмінюватися й адаптуватися на шляху до мети.

При цьому, на відміну від стійкості, резильєнтність - поняття динамічне, що передбачає не лише подолання негативного впливу шляхом зміни стандартних процесів на стресогенні стратегії, із подальшим поверненням до стійкого стану, але й більш ефективний розвиток, завдяки імплементації нових стратегій і набутих властивостей.

Розуміння концепції резильєнтності та її різних інтерпретацій у міжнародних стандартах має важливе значення з кількох причин:

а) Зростаюча складність систем: Оскільки технологічний прогрес продовжує збільшувати складність систем, організацій та інфраструктури, потенціал для збоїв та викликів також зростає. Чітке розуміння резильєнтності як концепції дозволяє зацікавленим сторонам краще розробляти, управляти і підтримувати системи, які можуть адаптуватися і відновлюватися після збоїв, забезпечуючи стабільність і безперервність.

б) Глобалізація та взаємопов'язаність: У сучасному взаємопов'язаному світі події в одному регіоні чи галузі можуть мати далекосяжні наслідки. Резильєнтні системи та організації можуть пом'якшити потенційний

негативний вплив цих подій, що призведе до створення більш надійних глобальних мереж і ланцюгів поставок.

в) Зміна клімату та стихійні лиха: Зі збільшенням частоти і тяжкості стихійних лих та екстремальних погодних явищ, спричинених зміною клімату, потреба у резильєнтних системах, інфраструктурі та організаціях є як ніколи актуальною. Поява концепції резильєнтності в міжнародних стандартах може стати основою для стратегій, спрямованих на мінімізацію наслідків таких подій і сприяння сталому розвитку.

г) Загрози кібербезпеці: Оскільки цифрові технології стають все більш поширеними, зростає ризик кібератак і порушень безпеки. Резильєнтність в контексті кібербезпеки є життєво важливою для забезпечення того, щоб системи та організації могли передбачати, протистояти та відновлюватися після таких загроз.

г) Безперервність бізнесу та антикризове управління: Здатність організацій підтримувати основні функції та послуги під час і після руйнівних подій, внаслідок війн та терористичних актів має вирішальне значення для їхнього довгострокового успіху. Розуміючи резильєнтність у контексті міжнародних стандартів, організації можуть розробити ефективні плани безперервності бізнесу та антикризового управління.

д) Конкурентна перевага: в умовах зростаючої конкуренції на світовому ринку організації та держави, які дотримуються принципів резильєнтності, мають кращі можливості для адаптації до мінливих ринкових умов і викликів, що забезпечує їхню довгострокову життєздатність та успіх.

Загалом, актуальність теми цієї доповіді полягає в тому, що вона може сприяти розвитку більш стійких систем, організацій та інфраструктури, які можуть краще протистояти та відновлюватися після збоїв, викликів та загроз. Завдяки комплексному розумінню резильєнтності, як вона трактується і застосовується в міжнародних стандартах, зацікавлені сторони можуть приймати обґрунтовані рішення і розробляти стратегії, які включають принципи резильєнтності в свою діяльність, управління ризиками і стратегічне планування.

Методологія

Для виявлення стандартів, що містять термін "резильєнтність", було проведено пошук публікацій ISO та NIST, які присвячені цій тематиці, щоб зрозуміти тлумачення та застосування резильєнтності в кожному контексті, з наведенням прямих цитат для ілюстрації визначень. Крім того, для ширшої перспективи були включені інші відомі організації, такі як Американський національний інститут стандартів (ANSI) та Британський інститут стандартів (BSI).

Результати дослідження

Стандарти ISO

a) ISO 22300:2021 Security and resilience - Vocabulary

цей стандарт надає декілька визначень терміну

i) Резильєнтність: "Здатність поглинати та адаптуватися в мінливому середовищі"

(resilience: ability to absorb and adapt in a changing environment [1]).

ii) Організаційна резильєнтність: "Здатність організації сприймати та адаптуватися в мінливому середовищі".

(organizational resilience: ability of an organization to absorb and adapt in a changing environment [1])

iii) Урбаністична резильєнтність: "Здатність будь-якої міської системи та її мешканців у мінливому середовищі передбачати, готуватися, реагувати та поглинати потрясіння, позитивно адаптуватися та трансформуватися перед обличчям стресів та викликів, сприяючи при цьому інклюзивному та сталому розвитку".

(urban resilience: ability of any urban system , with its inhabitants, in a changing environment, to anticipate, prepare, respond to and absorb shocks , positively adapt and transform in the face of stresses and challenges , while facilitating inclusive and sustainable development [1])

б) ISO 31000:2018 - Risk management - Guidelines

Хоча документ не дає прямого визначення резильєнтності, він згадує цю концепцію у зв'язку з управлінням ризиками: "Організація також повинна враховувати свою резильєнтність, яка є її здатністю справлятися з впливом ризикової події та відновлюватися після нього". (An organization should also consider its resilience, being its ability to cope with, and recover from, the impact of a risk event [2])

в) ISO 22316:2017 Security and resilience - Organizational resilience - Principles and attributes

Стандарт дає таке визначення резильєнтності: "Здатність організації абсорбувати та адаптуватися в мінливому середовищі, що дозволяє їй досягати своїх цілей, виживати та процвітати. Організаційна резильєнтність є результатом усіх аспектів діяльності організації і є емерджентною властивістю системи управління організацією". (The ability of an organization to absorb and adapt in a changing environment to enable it to deliver its objectives and to survive and prosper. Organizational resilience results from all aspects of the organization's performance and is an emergent property of the organization's management system [3])

г) Інші стандарти ISO серії Security and Resilience:

Документи не містить власного окремого визначення резильєнтності, але надають настанови щодо підвищення резильєнтності, посилаючись на визначення терміну в ISO 22300:2021 [1], враховуючи менеджмент, стратегію, ресурси та процеси.

Стандарти NIST

а) NIST SP 800-160 Vol. 2 Developing Cyber-Resilient Systems: A Systems Security Engineering Approach

Цей документ дає ґрунтовне визначення поняття резильєнтність, яке можна застосувати до проблемного домену кібербезпеки:

"Кіберрезильєнтність - це здатність передбачати, витримувати, відновлюватися та адаптуватися до несприятливих умов, навантажень, атак або компрометації систем, які використовують або підтримуються кіберресурсами" (Cyber resiliency is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. [4])

б) *NIST SP 800-184 Guide for Cybersecurity Event Recovery* спирається на визначення резильєнтності, наведене в DHS Risk Lexicon [5], який визначає резильєнтність як "здатність адаптуватися до мінливих умов і готуватися, витримувати і швидко відновлюватися після потрясінь. Розширене визначення: здатність систем, інфраструктур, уряду, бізнесу, громад та окремих осіб протистояти, терпіти, поглинати, відновлюватися після, готуватися до або адаптуватися до несприятливої події, яка спричиняє шкоду, руйнування або втрати. "

(ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption.

Extended Definition: ability of systems, infrastructures, government, business, communities, and individuals to resist, tolerate, absorb, recover from, prepare for, or adapt to an adverse occurrence that causes harm, destruction, or loss [6])

Інші стандарти

а) *ANSI/ASIS SPC.1-2009 Organizational Resilience: Security, Preparedness, and Continuity Management Systems*

"Резильєнтність: Здатність організації виявляти, запобігати та реагувати на руйнівні події, а також відновлюватися після них, підтримуючи безперервність діяльності та відновлюючи і вдосконалюючи свої можливості" (Resilience: The ability of an organization to identify, prevent, and respond to disruptive events and recover from them by maintaining continuity of operations and by restoring and improving its capabilities. [7])

б) *PAS 200:2011: crisis management – Guidance and good practice*

"Резильєнтність: Здатність організації передбачати, готуватися, реагувати та адаптуватися до поступових змін та раптових збоїв, щоб вижити та процвітати". (Resilience: The ability of an organization to anticipate, prepare for, respond and adapt to incremental change and sudden disruptions in order to survive and prosper [8])

Висновки

Розглядаючи термін "резильєнтність" у різних міжнародних стандартах, стає зрозуміло, що ця концепція охоплює широкий спектр застосувань і контекстів. Однак основні принципи резильєнтності залишаються незмінними, наголошуючи на адаптивності, відновленні та збереженні основної функціональності. Хоча інтерпретації можуть відрізнятися залежно від конкретного фокусу, в основі резильєнтності лежить здатність організації або системи адаптуватися, протистояти і відновлюватися після несприятливих подій, забезпечуючи безперервність основних функцій і

послуг.

Зважаючи на змістовну унікальність базового сенсу терміну «resilience», доцільним виглядає застосовувати в українському науковому вокабулярі кальку «резильєнтність», використовуючи визначення, наведені у вищезазначених міжнародних стандартах.

- [1] ISO 22300:2021 - Security and resilience – Vocabulary, (3.1.167, 3.1.206, 3.1.284) <https://www.iso.org/obp/ui/#iso:std:iso:22300:ed-3:v1:en>
- [2] ISO 31000:2018 - Risk management – Guidelines, [iso.org/standard/65694.html](https://www.iso.org/standard/65694.html)
- [3] ISO 22316:2017 Security and resilience - Organizational resilience - Principles and attributes (Introduction) <https://www.iso.org/obp/ui/#iso:std:iso:22316:ed-1:v1:en>
- [4] NIST SP 800-160 Vol. 2 - Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems, (Introduction). <https://csrc.nist.gov/publications/detail/sp/800-160/vol-2-rev-1/final>
- [5] Department of Homeland Security (DHS), DHS Risk Lexicon, 2010 Edition, September 2010. <https://www.dhs.gov/dhs-risk-lexicon> [accessed 12/12/16]
- [6] NIST SP 800-184 - Guide for Cybersecurity Event Recovery (2.1)
- [7] ANSI/ASIS SPC.1-2009 - Organizational Resilience Standard (D50)
- [8] BSI PAS 200:2011 - Crisis Management - Guidance and good practice

РЕЗИЛЬЄНТНІСТЬ ЕНЕРГЕТИЧНОЇ СИСТЕМИ УКРАЇНИ: ОСНОВНІ ПРИНЦИПИ ТА ПОНЯТТЯ

Енергетична система України почала своє формування в середині минулого століття, та продовжувала фактично до початку до 24.02.2022 року, а саме дати початку масштабного вторгнення РФ в Україну. Вже станом на липень 2022 року в матеріалах робочої групи «Енергетична безпека» до проекту Плану відновлення України зазначалось, що близько 4% генеруючої потужності зруйновано під час бойових дій, ще 35% потужності знаходиться на окупованих територіях.[2] Після цього а саме з середини жовтня 2022 по лютий 2023 енергетична система була майже головною ціллю для масованих ракетних атак ворога. Точну оцінку пошкоджень та руйнувань офіційні джерела не публікували, але за оцінками експертного середовища процент зруйнованих об'єктів на початок березня 2023 року може становити від 25 - 30% від потужностей на 24.02.2022.

Оскільки створення сучасної енергетичної системи України проходило без урахування таких негативних факторів як масштабне руйнування (внаслідок масованих обстрілів), швидка втрата потужностей (внаслідок руйнувань чи окупації ворогом) та неможливість оперетивно проводити роботи по відновленню систем (небезпека роботи персоналу в потенціально небезпечних локаціях через загрозу для життя), то через ці виклики потрібно відновлювати саму систему, а також розглядати нові критерії оцінки її роботи.

Одним з таких критеріїв може стати резильєнтність (від. англ. resilience – резильєнтність, стійкість, відмовостійкість, життєстійкість, спроможність відновлюватись).

Для того, щоб сформувані комплекс оцінки резильєнтності енергетичної системи потрібно провести аналіз того, яким чином резильєнтність пов'язана з базовими поняттями роботи системи, які актуальні на даний момент часу, як їх структурувати та співвіднести один з одним в новому комплексі оцінки. Після того, це буде структуровано, то можливо проводити аналіз та розробляти певні математичні та програмні методи оцінювання резильєнтності системи.

Поки що для оцінки використовують багато критеріїв, наприклад – стійкість Згідно публікації в Економічній правді від 1 грудня 2022 року стійкість енергетичної системи України на день публікації була лише 15% [1]. При цьому система працювала. Як факт, ця інформація прийнятна, але не дає відповіді на такі питання: 1) чи буде система працювати, якщо її стійкість буде зменшуватись? 2) чи здатна система самовідновлюватись в цих умовах? тощо.

Імовірно, що в майбутньому будуть знайдені більш точніші дефініції та критерії оцінки резильєнтності, однак вже сьогодні є можливість починати

вводити певні математичні та програмні засоби оцінювання резильєнтності об'єктів енергетики. Для цього треба, по-перше, здійснити критичний аналіз сучасних наукових підходів та нормативного забезпечення в сфері резильєнтності об'єктів енергетики.

Умови військового часу, з одного боку, є фактором, який створює перепони для будь-яких досліджень, але, з іншого боку, спонукає якнайшвидше реагувати на виклики, скільки отримання актуальних даних є запорукою успіху в керуванні енергетичною системою. Також це дозволить залишатися прогнозованим партнером в рамках синхронії ОЕС України та ENTSO-E [3, 4].

Фактор прогнозованого партнерства в галузі енергетики повинен розглядатись не як рух в одному напрямку, тобто Україна оцінює резильєнтність енергетичної системи через військову загрозу, а партнери залишають стару систему оцінки своїх енергетичних систем. Загальна енергетична система з партнерами мусить стати однаково прогнозованою та такою, що враховує і нові реалії існування. Таким чином, розвиток математичних та програмних засобів оцінки у одного з членів «енергетичного суспільства» автоматично буде змушувати інших до подібних кроків, що дає змогу тільки поширювати взаємодію та поглиблювати можливості усієї системи в цілому, в тому числі щодо загальної резильєнтності суспільства.

- [1] Енергетична система України зараз стійка лише на 15% – Економічна правда. Економічна правда – онлайн версія. URL: <https://www.epravda.com.ua/news/2022/12/1/694487/>
- [2] Моїсєєв В., Що являє собою енергосистема України напередодні воєнної зими - The Page, Онлайн газета. URL: <https://thepage.ua/ua/economy/energositema-ukrayini-stan-naperedodni-zimi>
- [3] Continental Europe successful synchronisation with Ukraine and Moldova power systems, The official site of European Network of Transmission System Operators for Electricity (ENTSO-E). URL: <https://www.entsoe.eu/news/2022/03/16/continental-europe-successful-synchronisation-with-ukraine-and-moldova-power-systems/>
- [4] ENTSO-E Member Companies, The official site of European Network of Transmission System Operators for Electricity (ENTSO-E). URL: <https://www.entsoe.eu/about/inside-entsoe/members/>

МОДЕЛІ ТА КОМП'ЮТЕРНІ ЗАСОБИ МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ ПРОЦЕСІВ ФУНКЦІОНУВАННЯ ВЕРСТАТІВ З ЧПК

Верстат з ЧПК є складним та вартісним пристроєм обробки металів. При його роботі виникають навантаження на вузли, які можуть призводити до поломок.

Виникає необхідність розробки математичної моделі роботи багато-осьового верстата з ЧПК, що дозволить враховуючи масово-габаритні властивості вузлів, розраховувати динамічну поведінку цих вузлів, отримувати розрахункові дані прискорень, порівнювати їх з граничними значеннями. Ця математична модель, дозволить, ще на етапі розробки верстатів, отримувати виникаючі динамічні характеристики, та вносити як конструктивні зміни, так і впроваджувати програмні обмеження в системі ЧПК.

Кінематична схема багато-осьового верстата з ЧПК

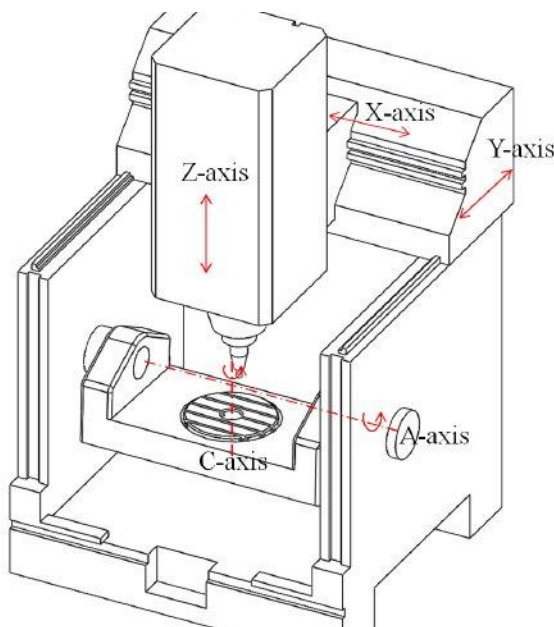


Рисунок 1 Кінематична схема багато-осьового верстата.

Рух вузлів багато-осьового верстата, під час виконання програми. При цьому, інструмент робить не значне переміщення з заданою лінійною

робочою подачею, а вузли верстата виконують переміщення з більшою швидкістю ніж інструмент (Рисунок 2 та 3).

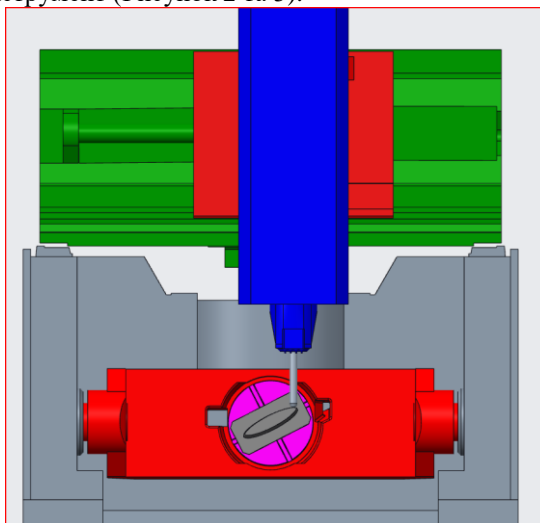


Рисунок 2 Початкове положення інструмента.

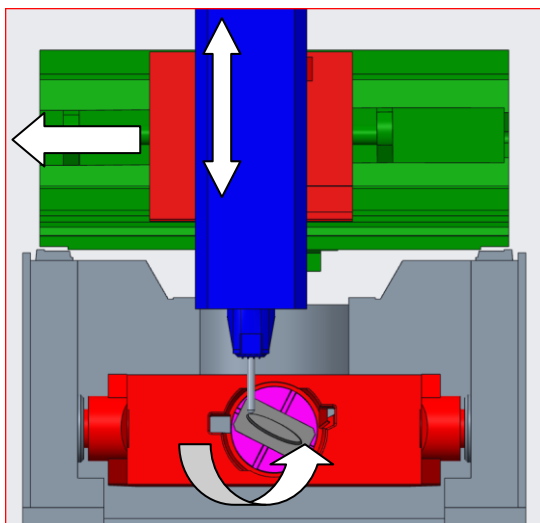


Рисунок 3 Переміщення вузлів верстата.

Математична модель буде використовувати рівняння Лагранжа [1].

[1] Єжов С. М., Макарець М. В., Романенко О. В. Класична механіка. — К. : ВПЦ "Київський університет", 2008. — 480 с.

А.В. Полухін

ПОБУДОВА МАТЕМАТИЧНОЇ МОДЕЛІ ВИЗНАЧЕННЯ ПОГОДИННОГО СПОЖИВАННЯ СПОЖИВАЧІВ З РОЗБИВКОЮ ПО АДМІНІСТРАТИВНИМ ОБЛАСТЯМ УКРАЇНИ

Аналіз та прогноз електроспоживання є одним із фундаментальних принципів, якого необхідно дотримуватись для коректної побудови балансу сукупного фізичного виробництва та споживання в об'єднаній енергетичній системі України. Здійснювати відповідні розрахунки досить легко, якщо всі споживачі, від малих побутових до великих підприємств і заводів, обладнані комерційними точками обліку зі системою АСКОЕ, при чому яка б в автоматичному режимі надсилала дані обліку. Але в Україні подібними системами обліку обладнані крупні споживачі, та і то не всі. Не кажучи навіть про побутових споживачів, загальна частка споживання яких може досягати 35% від загального споживання по країні (приклад профілю електроспоживання за зимні та літні місяці 2019-2021 наведено на рис. 1).

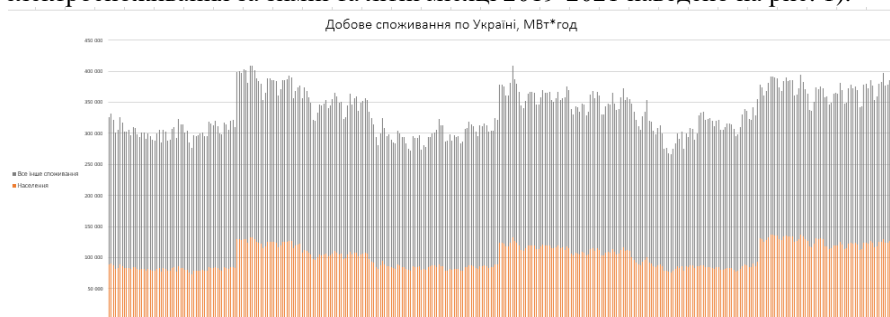


Рис. 1. Структура добового споживання в Україні за лютий і червень 2019 року

Актуальність дослідження обумовлена відсутністю у відкритих джерелах на сьогоднішній день погодинних обсягів споживання електричної енергії в Україні з розбивкою по структурі споживання, наявність чого дозволило більш точно визначати профіль споживання по окремих категоріям та здійснювати аналіз зміни такого споживання електричної енергії та здійснювати відповідні прогностичні розрахунки. Для вирішення цієї проблеми на сьогодні застосовуються різні тимчасові рішення, як, наприклад, профілювання споживачів групи Б, а це необхідно для побудови різних математичних моделей та управління попитом [1]. Окрім цього, відсутній розподіл електроспоживання по адміністративним областям України, щоб дозволило здійснювати прогнозування електроспоживання із врахуванням регіональних особливостей.

Авторами запропоновано здійснити розподіл споживачів електричної енергії за наступними категоріями:

- промисловість;
- сільгоспспоживачі;
- транспорт;
- будівництво;
- комунально-побутові споживачі;
- населення;
- інші споживачі.

Дані категорії відповідають розбивці споживачів, яку здійснює Міністерство енергетики України при публікації місячних показників структури споживання загалом по Україні. Зазначені дані і запропоновано розподіляти по адміністративних областях та розраховувати погодинно.

Для початку розрахунку пропонується розподілити місячний показник за регіональною розбивкою. Для цього запропоновано застосовувати ретроспективні дані щодо структури споживання з регіональною розбивкою, які сформовані за формою енерго-16. Окремо необхідно зазначити, що, оскільки відсутні фактичні обсяги споживання для Донецької, Луганської областей та АР Крим, для цих регіонів розрахунки не здійснюються.

Формульно це можна представити наступним чином:

1. На підставі місячної структури споживання по регіонах за попередні роки ($Cn_{обс,j',m,y-old}^i$) розраховано частку споживання i -го регіону (у розрізі структури j' -го споживання) серед всіх регіонів n для місяця m року $y-old$ за формулою:

$$Cn_{обс,j',m,y-old}^i = \frac{Cn_{обс,j',m,y-old}^i}{\sum_{i=1}^n Cn_{обс,j',m,y-old}^i} \quad (1)$$

2. На підставі розрахунків (1) структура j' -го споживання i -го регіону за досліджувані роки ($y-new$) розподілена у структурі загального місячного m споживання по Україні (n) $Cn_{обс,m,y-new}^n$ за формулою:

$$Cn_{обс,j',m,y-new}^i = Cn_{обс,j',m,y-old}^i * Cn_{обс,m,y-new}^n \quad (2)$$

Окремим питанням побудови погодинних обсягів споживання для всіх днів відповідного місяця на підставі профільованих днів вихідного та робочого дня. Для цього пропонується використовувати наступний експериментальний алгоритм:

- 1) розраховується усереднене погодинне споживання окремо загалом, для вихідних днів та для робочих днів;
- 2) розраховується співвідношення погодинного споживання вихідних днів відповідних годин до загального споживання, і погодинного споживання робочих днів відповідних годин до загального споживання.

3. На підставі погодинного споживання в ОЕС України за ретроспективні роки (за даними ПрАТ «НЕК «Укренерго») визначається усереднене погодинне (h) добове значення споживання місяця (m) за

досліджувані роки (y) в розрізі вихідного дня, робочого дня, загального дня за формулами:

$$Cn_{обс,сер,вих,т,y-new}^{h-вих} = \frac{\sum_{h-вих=1}^{h-вих} Cn_{обс,т,y-new}^{h-вих}}{h-вих} \quad (3)$$

$$Cn_{обс,сер,роб,т,y-new}^{h-роб} = \frac{\sum_{h-роб=1}^{h-роб} Cn_{обс,т,y-new}^{h-роб}}{h-роб} \quad (4)$$

$$Cn_{обс,сер,заг,т,y-new}^{h-заг} = \frac{\sum_{h-заг=1}^{h-заг} Cn_{обс,т,y-new}^{h-заг}}{h-заг} \quad (5)$$

4. Розраховується погодинне співвідношення усередненого погодинного добового споживання годин h -вих і h -роб до усередненого погодинного добового споживання годин h -заг з формул (3-5), а саме робочого дня до загального дня і вихідного дня до загального дня для місяців t років y -new за формулою:

$$Час_{сер,вих,т,y-new}^{h-вих} = \frac{Cn_{обс,сер,вих,т,y-new}^{h-вих}}{Cn_{обс,сер,заг,т,y-new}^{h-заг}} \quad (6)$$

$$Час_{сер,роб,т,y-new}^{h-роб} = \frac{Cn_{обс,сер,роб,т,y-new}^{h-роб}}{Cn_{обс,сер,заг,т,y-new}^{h-заг}} \quad (7)$$

5. Розраховується погодинне співвідношення усередненого погодинного добового споживання годин h -вих і h -роб до погодинних обсягів споживання в ОЕС України у місяцях t роках y -new, співставляючи робочі періоди до робочих та вихідні періоди до вихідних за формулою:

$$Час_{т,y-new}^{h-вих} = \frac{Cn_{обс,сер,вих,т,y-new}^{h-вих}}{Cn_{обс,т,y-new}^{h-вих}} \quad (8)$$

$$Час_{т,y-new}^{h-роб} = \frac{Cn_{обс,сер,роб,т,y-new}^{h-роб}}{Cn_{обс,т,y-new}^{h-роб}} \quad (9)$$

Після розподілу місячних показників за регіональним принципом необхідно профілювати ці обсяги. Для профілювання пропонується використовувати заміри режимних днів для літнього та зимнього місяців для адміністративних областей з виділенням відповідних категорій споживачів окремо для робочих та вихідних днів. Результатом розрахунку буде виділення погодинного типового усередненого робочого та вихідного дня. Формульне представлення нижче.

6. На підставі режимних днів в розрізі вихідного та робочого дня для відповідної структури споживання для відповідних регіонів розраховуються типові погодинні обсяги по структурі споживання одного дня для місяців t

для досліджуваних років y -new для регіонів i по вихідному та робочому дню шляхом профілювання усереднених за 1 день обсягів структури споживання j по регіонах на відповідний режимний день та множення на співвідношення, розраховане за (6-7), за формулою:

$$\frac{Cn_{обс,j,m,y-new}^i}{31} * \frac{Част_{\%min,вих,j,m}^{i,h-вих}}{\sum_{h-вих=1}^{24} Част_{\%min,вих,j,m}^{i,h-вих}} * Част_{сер,вих,m,y-new}^{h-вих} = \quad (10)$$

$$\frac{Cn_{обс,j,m,y-new}^i}{31} * \frac{Част_{\%min,роб,j,m}^{i,h-роб}}{\sum_{h-роб=1}^{24} Част_{\%min,роб,j,m}^{i,h-роб}} * Част_{сер,роб,m,y-new}^{h-роб} = \quad (11)$$

де

$Част_{\%min,роб,j,m}^{i,h-роб}$ – відсоток від максимуму погодинного споживання для режимного дня.

На підставі розрахованих погодинних коефіцієнтів розподіляються профільовані обсяги усередненого типового вихідного та робочого дня. Результатом такого розрахунку є погодинні обсяги споживання з розбивкою по адміністративним областям та категоріям споживачів. За результатами розрахунків та дослідження отримуються профільовані обсяги споживання електричної енергії з розбивкою по категоріям споживачів окремо по регіонам України що дозволяє використовувати такі дані для відповідного аналізу органам моніторингу ринку електричної енергії, а також суб'єктам господарювання, які здійснюють балансування виробництва та споживання на локальних або загальному рівнях.

Досліджена модель може бути використана при розробці інших математичних моделей, необхідних для управління попитом. Додатково до зазначеного, таку модель можна застосовувати при визначенні погодинного попиту при торгівлі на ринку «на добу наперед» для забезпечення максимізації своєї економічної складової [2].

- [1] Мица Н.В. Управління попитом на електроенергію як необхідна передумова ефективної фінансової діяльності енергопостачального підприємства / Н.В. Мица – Хмельницький: Вісник Хмельницького національного університету, 2010. – №6, Т.3. – С. 93-98.
- [2] Полухін А.В. Комп'ютерне моделювання процесів визначення цінової позиції суб'єктів ринку електричної енергії на ринку «на добу наперед». XXXIX Науково-технічна конференція молодих вчених та спеціалістів інституту проблем моделювання в енергетиці ім. Г.С. Пухова НАН України: тези доп.всесукр. наук.-практ. конф.(м. Київ, 12 трав. 2021). Київ, 2021. С. 106-107.

Т.В. Пучко

ПРОБЛЕМА ПІДТРИМАННЯ СУМІСНОСТІ МІЖ НАДАВАЧАМИ ТА КЛІЄНТАМИ ВЕБІНТЕРФЕЙСІВ ПРИКЛАДНОГО ПРОГРАМУВАННЯ

У наш час неможливо уявити розроблення програмного забезпечення без інтерфейсів прикладного програмування (ІПП, англійською API). Розробники використовують їх, щоб викликати функції операційної системи, взаємодіяти з бібліотеками, сполучати частини розподілених програмних систем, і надавати послуги іншим прикладним програмам. Традиційно ІПП надаються бібліотеками підпрограм, програмними каркасами, та наборами засобів розроблення. Сьогодні такі ІПП називаються статичними, щоб відрізнити їх від дистанційних ІПП, які ще називаються вебінтерфейсами прикладного програмування (ВІПП, англійською web API) [1]. Доступ до ВІПП надається через мережу з використанням таких технологій, як HTTP, JSON, та XML. Спершу ВІПП використовувалися лише вебслужбами, але сьогодні, в еру контейнеризації, мікросервісів, та хмарних обчислень, їх можна побачити всюди [2]. Вони не лише сполучають застосунки на пристроях користувачів з необхідними службами, а й дозволяють побудувати розподілені системи, складові частини яких можуть розвиватися незалежно одна від одної.

При взаємодії через ВІПП програмні компоненти, такі як прикладні програми чи мікросервіси, можуть мати дві ролі: надавач (англійською provider) надає до використання один або декілька ВІПП, а клієнт їх використовує [3]. Щоб успішно взаємодіяти, надавач та клієнт мають користуватися однаковою описом ВІПП, проте, оскільки компоненти розвиваються незалежно, визначення ВІПП на боці надавача може настільки змінитися, що клієнт не матиме змоги коректно працювати. Ці випадки негативно впливають на задоволення споживача, спричиняють порушення угод про рівень послуг, і вимагають багато зусиль для виправлення наслідків [4]. Оскільки ВІПП стали суттєвою частиною програмного забезпечення, організаціям, що їх розробляють, надзвичайно важливо мати стратегію запобігання таким випадкам. Але підтримання сумісності між надавачами та клієнтами ВІПП вимагає додаткових витрат часу інженерів, тому перед цими організаціями постає питання, як зменшити такі витрати. Щоб побудувати стратегію, яка мінімізує витрати часу, необхідно розуміти, як і чому ВІПП змінюються, який вплив мають ці зміни на клієнтів, і які існують методи та технічні прийоми, щоб зменшити кількість роботи, що необхідно виконувати для підтримання сумісності.

На перший погляд, ВІПП не мають змінюватися, але на практиці при створенні нового ВІПП розробники ще недостатньо добре знають свою предметну область і не мають усіх вимог від своїх клієнтів, тому перша версія ВІПП зазвичай недосконала. Але з часом навіть якісний ВІПП вимагає змін: з'являються нові поняття предметної області, відбуваються зміни в

законодавстві, і клієнти починають просити нові функціональні можливості. З точки зору клієнтів зміни поділяються на такі, що ламають інтерфейс (англійською breaking) та ті, які залишають можливість взаємодії (англійською non-breaking), до того ж перші можуть впливати або на синтаксис ВПП, або на поведінку [5]. А з точки зору надавачів ВПП зміни класифікуються або залежно від того, що їх спричиняє (нові функції, прагнення до простоти, виправлення помилок), або залежно від змінених елементів (методи, атрибути), або залежно від виконаних дій над елементами (додавання, перейменування, видалення) [5]. Несумісні зміни у ВПП негативно впливають на клієнтів. Зазвичай прикладні програми не готові до таких змін. Отримавши неочікувану відповідь, програма може відразу завершитися, показати повідомлення про несподівану помилку, знехтувати отриманою відповіддю, або навіть залишитися у стані завантаження [6].

Існують такі типові методи підтримання сумісності [3]:

- Опис ВПП, який має включати як технічні деталі, так і таку додаткову інформацію, як приклади використання.
- Ідентифікатор версії, за допомогою якого клієнт може зрозуміти, які можливості надає поточна версія ВПП.
- Семантичне версіонування, яке дає клієнтам можливість визначити, чи зміни зворотно сумісні.
- Обмежений термін служби, який дає можливість клієнтам планувати перехід на іншу версію ВПП.
- Вічний термін служби, який гарантує клієнтам відсутність необхідності адаптації до змін.
- Паралельні версії, що дозволяють клієнтам переходити на нову версію ВПП за власним графіком.
- Агресивне застарівання, яке дозволяє надавачам економити ресурси на підтримку попередніх версій ВПП.
- Експериментальна версія, яка дозволяє додавати нові можливості з меншим ризиком для клієнтів.

Популярним прийомом, який дає можливість одночасно змінювати ВПП і гарантувати їхню стабільність для клієнтів, є перетворення запитів до різних версій ВПП на запити до однієї версії [7] [8]. Таке перетворення можна здійснювати на різних рівнях: між надавачем та клієнтом ВПП, на боці надавача, або навіть на боці клієнта.

Отже, загалом проблема підтримання сумісності між надавачами та клієнтами ВПП актуальна, а оптимізація витрат часу на це має практичну цінність для організацій, що розробляють ВПП. Найвні методи та прийоми дають можливість зменшити витрати часу, але постає завдання їх вибору та комбінування. Необхідні подальші дослідження, щоб сформулювати економічні критерії і розробити на їхній основі оптимізаційну модель пошуку ефективних рішень з підтримання сумісності між надавачами та клієнтами ВПП.

- [1] Raatikainen M., Kettunen E., Salonen A., Komssi M., Mikkonen T., Lehtonen T. (2021) State of the Practice in Application Programming Interfaces (APIs): A Case Study. In: Biffl S., Navarro E., Löwe W., Sirjani M., Mirandola R., Weyns D. (eds) Software Architecture. ECSA 2021. Lecture Notes in Computer Science, vol 12857, pp 191-206. https://doi.org/10.1007/978-3-030-86044-8_14
- [2] Bonorden L., Riebisch M. (2022) API Deprecation: A Systematic Mapping Study. In: 2022 48th Euromicro Conference on Software Engineering and Advanced Applications (SEAA 2022), pp 451-458. <https://doi.org/10.1109/SEAA56994.2022.00076>
- [3] Lübke D., Zimmermann O., Pautasso C., Zdun U., Stocker M. (2019) Interface evolution patterns: Balancing compatibility and extensibility across service life cycles. In: Proceedings of the 24th European Conference on Pattern Languages of Programs, article no 15, pp 1-24. <https://doi.org/10.1145/3361149.3361164>
- [4] Godefroid P., Lehmann D., Polishchuk M. (2020) Differential regression testing for REST APIs. In: Khurshid S., Păsăreanu C. S. (eds) Proceedings of the 29th ACM SIGSOFT International Symposium on Software Testing and Analysis, pp 312-323. <https://doi.org/10.1145/3395363.3397374>
- [5] Koçi R., Franch X., Jovanovic P., Abelló A. (2019) Classification of changes in API evolution. In: 2019 IEEE 23rd International Enterprise Distributed Object Computing Conference (EDOC), pp 243-249. <https://doi.org/10.1109/EDOC.2019.00037>
- [6] Espinha T., Zaidman A., Gross H.-G. (2015) Web API Fragility: How Robust is Your Mobile Application? In: 2015 2nd ACM International Conference on Mobile Software Engineering and Systems, pp 12-21. <https://doi.org/10.1109/MobileSoft.2015.9>
- [7] Beurer-Kellner L., von Pilgrim J., Tsigkanos C., Kehrer T. (2022) A Transformational Approach to Managing Data Model Evolution of Web Services. In: IEEE Transactions on Services Computing, vol 16, no 1, pp 65-79. <https://doi.org/10.1109/TSC.2022.3144613>
- [8] Campinhos J., Seco J. C., Cunha J. (2017) Type-Safe Evolution of Web Services. In: 2017 IEEE/ACM 2nd International Workshop on Variability and Complexity in Software Design (VACE), pp. 20-26. <https://doi.org/10.1109/VACE.2017.6>

ПРОБЛЕМА ПАРТИЦІОНУВАННЯ КЛАСТЕРУ ТА АКТУАЛЬНІСТЬ ЇЇ ВИРІШЕННЯ НА ПРИКЛАДІ АККА-CLUSTER FRAMEWORK

Партиціонування кластеру, також відоме як *split-brain scenarios (SBS)*, — в інформатиці, стан розподіленої системи, коли за певних причин вона розпадається на дві чи більше частин і кожна частина продовжує функціонувати незалежно як окремий кластер, в результаті чого виникають колізії даних, що ускладнює, або навіть робить неможливим їх зворотнє об'єднання в єдину систему [2].

Наприклад є кластер з 11 вузлів і раптом мережа розділяється таким чином, що 6 вузлів втрачають зв'язок з іншими 5-ма. Після певної кількості невдалих спроб поновити зв'язок отримуємо два незалежних кластера — 6-вузловий і 5-вузловий. При чому кожен кластер буде вважати, що він єдиний функціонуючий і продовжуватиме працювати. Це все потенційна небезпека узгодженості даних.

Підходи розв'язання SBS поділяються на два типи: оптимістичний та песимістичний [4]:

- Оптимістичний дозволяє розділеним вузлам працювати у звичайному режимі — це забезпечує вищий рівень доступності за рахунок коректності даних. Щойно зв'язок поновлюється, виникає необхідність в автоматичному чи ручному узгодженню даних.
- Песимістичний підхід найвищим пріоритетом ставить консистентність даних за рахунок доступності. Щойно кластер розділяється, вводяться заборони на будь-які дії, що можуть призвести до втрати цілісності даних.

Розглянемо проблему SBS на прикладі фреймворку Akka Cluster [1]. Даний фреймворк надає відмовостійку децентралізовану службу членства в кластері без єдиної точки відмови. Що досягається за допомогою протоколу пліток (*gossip protocol*) [5] та автоматичного детектора відмов (*failure detector*) [3]. Кластер складається з набору вузлів-членів, а додаток, що побудований з використання Akka-фреймворку, може бути розподілений по кластеру, при цьому кожен вузол буде містити певну частину програми.

Як і всім іншим розподіленим системам, додатку створеному на основі Akka Cluster будуть притаманні, як проблема мережевого розділу, так і ситуації з відмовою в роботі частини вузлів системи з апаратних чи програмних причин, таких як наприклад перевантаження (*overload*), ресурсний голод (*starvation*) або навіть довгі паузи збирання сміття (*garbage collection pauses*) віртуальної машини [2]. І в першому, і в другому випадку певні вузли стають не доступними принаймні на деякий час, але працюючі вузли не можуть відрізнити дані ситуації одна від одної. Іншими словами, вузол розподіленої системи може помічати коли стається проблема з іншим

вузлом цієї ж системи, але він не може сказати, що саме було першопричиною, чи це тимчасова проблема з мережею, яка через певний час можливо зникне, чи ж інший вузол повністю вийшов з ладу і його роботу не можливо буде відновити.

У разі критичного програмного збою доцільно якнайшвидше видалити даний вузол з кластеру. У разі ж мережевого розділу, де ця ситуація можливо є тимчасовою і вона може скоро вирішитися, було б доцільніше певний час зачекати з видаленням. Але в певний момент часу, якщо проблема так і не вирішилася, ми повинні відмовитися чекати та продовжити роботу з вузлами з одного боку розділу та видалити вузли з іншого.

Підходи з швидким видаленням та очікуванням є діаметрально протилежними і необхідний компроміс між тим, як швидко треба видалити проблемний вузол з кластеру, і передчасними діями щодо тимчасових мережевих розділів.

Оскільки вузли по різні сторони мережевого розділу не можуть спілкуватися один з одним, треба мати певність, що обидві сторони зможуть прийняти самостійне і не суперечливе рішення, яка частина кластеру продовжить працювати, а яка припинить свою роботу.

Як було зазначено вище, кластер Akka містить детектор збоїв, який помічає мережеві розділи та збої машин (але не може розрізнити їх). Він використовує періодичні повідомлення “серцебиття” між вузлами кластеру, щоб перевірити чи доступні та працездатні інші вузли та відповідно міняти статус цих вузлів.

Розглянемо відомі стратегії для роботи з розділами мережі та вузлами, що не відповідають [2]:

- Стратегія збереження більшості (Keep Majority) – виключає з кластеру недоступні вузли, якщо поточний вузол перебуває у більшості на основі останньої відомої інформації. Або ж виключає з кластеру всі доступні вузли власної частини, якщо це меншість.
- Стратегія статичного кворум (Static Quorum) – виключає з кластеру недоступні вузли, якщо кількість вузлів що залишилась більше або рівна визначеному розміру кворуму. В іншому випадку він виключить доступні вузли, тобто цю сторону розділу.
- Стратегія збереження найстаріших вузлів (Keep Oldest) – виключає з кластеру частину, яка не містить найстарішого члена.
- Стратегія повного вимкнення (Down All) – призводить до вимкнення усіх вузлів кластеру. Ця стратегія може бути безпечною альтернативою, якщо мережеве середовище дуже нестабільне. Через нестабільність існує підвищений ризик різної інформації на різних сторонах розділів, і тому вибір іншої стратегії може призвести до суперечливих рішень. У таких середовищах може бути краще вимкнути всі вузли та запустити новий кластер.
- Стратегія Lease Majority – використовує розподілене блокування щоб вирішити, яким вузлам дозволено залишитись в кластері. Лише одна

сторона зможе отримати об'єкт блокування і залишитись в складі кластеру. Інша ж не отримавши його буде змушена припинити свою роботу. Ця стратегія дуже безпечна, оскільки координацію додає зовнішній арбітр. Але мінус, у порівнянні з іншими стратегіями, полягає в тому, що для реалізації потрібна додаткова інфраструктура.

Слід зазначити, що кожна наведена вище стратегія має свої сценарії провалу [2], коли вона може приймати «неправильне» рішення, тож завжди треба зважено обирати стратегію, яка відповідає характеристикам системи.

Зважаючи на викладене вище вважаємо, що проблема SBR є актуальною для akka-фреймворку, а з огляду на широке застосування зазначеного фреймвоку, завдання запобігання розрізнення кластеру для Akka має практичну цінність.

- [1] Akka Documentation: Cluster Usage
- [2] URL: <https://doc.akka.io/docs/akka/current/typed/cluster.html> (date of access: 14.04.2023).
- [3] Akka Documentation: Split Brain Resolver
- [4] URL: <https://doc.akka.io/docs/akka/current/split-brain-resolver.html> (date of access: 14.04.2023).
- [5] Chandra and Toueg. Unreliable failure detectors for reliable distributed systems. *JACM* 43(2):225–267, 1996
- [6] Davidson, Susan; Garcia-Molina, Hector; Skeen, Dale (1985). "Consistency In A Partitioned Network: A Survey". *ACM Computing Surveys*. 17 (3): 341–370.
- [7] Jelasity, Márk (2011-01-01). In Serugendo, Giovanna Di Marzo; Gleizes, Marie-Pierre; Karageorgos, Anthony (eds.). *Self-organising Software*. Natural Computing Series. Springer Berlin Heidelberg.

ТИПИ ТА ВЛАСТИВОСТІ СИСТЕМ ПЕРЕДАЧІ ПРОМЕНЕВОЇ ЕНЕРГІЇ

Оптична концентрація — єдиний спосіб підвищення енергетичної щільності процесів перетворення сонячної енергії, а отже, підвищення ефективності сонячних установок [1]. Більше того, це дозволить використати енергію інфрачервоних вікон атмосфери, де знаходиться біля половини сонячної променевої енергії.

Сонячний енергетичний концентратор-коліматор створює односпрямований світловий потік підвищеної енергетичної щільності, для передачі його на відстані за допомогою хвилеводу, зі збереженням енергетичної складової випромінювання. Для цього потрібна достатньо якісна колімація [2]. Але таке завдання пов'язане з проблемами, подібними до проблем створення променевої зброї, описаної у фантастичних романах Жюль Верна, Уельса або О.М. Толстого [3].

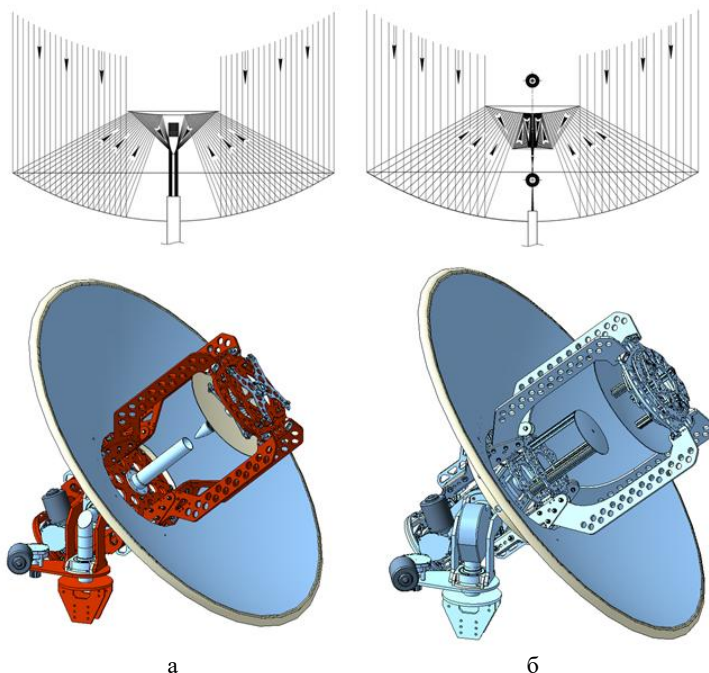


Рис. 1. Схема принципу роботи та зовнішній вигляд енергетичного концентратора сонячного випромінювання: а - на основі апертурного стрижня [4]; б - на основі гіперболоїда [5]

На рис. 1 показано відомі оптичні системи енергетичних концентраторів, які відрізняються способом формування колімованого світлового потоку. Головною їх особливістю є різний концептуальний підхід. Концентратор на основі апертурного стрижня (рис. 1, а) виконано за канонами геометричної оптики, тобто від кожного оптичного елемента, випромінювання відбивається один раз. Від дзеркал гіперболоїда (рис. 1, б) випромінювання відбивається багаторазово, поступово орієнтуючись паралельно оптичній осі. Остання система не підходить для формування зображення, але відмінно пропускає енергетичну складову випромінювання [2]. Отже, ця концепція найбільш перспективна для застосування її в сонячних енергетичних концентраторах.

Гіперболоїд є системою сполучених дзеркал, яка має колімуючі властивості, але він не є виключенням, такими ж властивостями володіє система сполученого еліпсоїда. Тут слід зазначити, що колімуючий ефект зберігається при різних комбінаціях гіперболічних і еліптичних дзеркал, при умові їх сполучення по фокусам. Такі системи можна розділити на два основні типи: імпульзівні (рис. 2, а) і експлозивні (рис. 2, б). Вони відрізняються способом входження випромінювання в систему дзеркал: в систему імпульзівних коліматорів поступає пучок випромінювання, що сходиться, у систему експлозивних — той, що розходить.

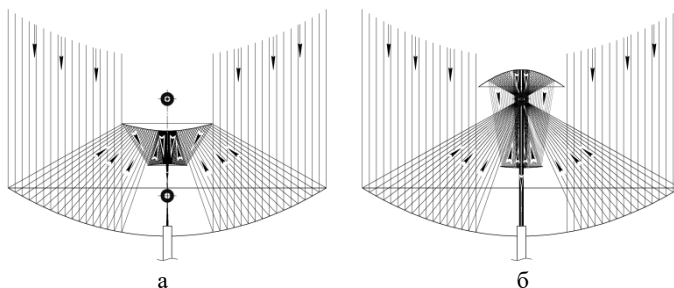


Рис. 2. Основні типи сонячних енергетичних концентраторів-коліматорів : а - імпульзівні коліматори; б - експлозивні коліматори

Експлозивні коліматори дозволяють використовувати еліптичне вторинне дзеркало з негативною кривизною, що відносить такі коліматори до систем за типом Грегорі. Зазначимо, що незважаючи на принципову різницю, при використанні дзеркал другого порядку кривизни імпульзівні і експлозивні системи за абераційними характеристиками абсолютно аналогічні. Але при використанні дзеркал з третім і більш високим порядком кривизни в таких системах проявляється істотна різниця.

В окрему підгрупу варто віднести системи Річі—Кретьєна, які відомі відсутністю коми, при цьому в таких системах застосовано вторинний відбивач з позитивною кривизною. У системах Річі—Кретьєна застосовуються відбивачі з гіперболічною кривизною в якості як основного,

так і вторинного дзеркала. Отже, за характером кривизни основного дзеркала імплізивні коліматори можна розділити на два типи: Кассегрена і Річі—Кретьєна.

У роботі виконано порівняльний аналіз можливих концентраторів-коліматорів по абераційним і поляризаційним характеристикам. Результати будуть корисні при проектуванні систем передачі променевої енергії.

- [1] Ахадов Ж.З. Комбинированная энергоустановка с концентраторами солнечного излучения. LAP LAMBERT Academic Publishing, 2016, 119 с.
- [2] Чернозьомов Є.С. Кобальтовий гіперболоїд. Моделі енергетичного віддзеркалення в області кутів нормального падіння // Електрон. моделювання, 2022, 44, №3, с. 31—41.
- [3] Чернозьомов Є.С. Моделі аберацій гіперболічних відбивачів другого і вищого порядку кривизни в системах передачі променевої енергії // Електрон. моделювання, 2023, 45, №1, с. 27—40.
- [4] Патент на винахід 120802, Україна, МПК (2020.01) F24S 10/00, G02B 6/00, F24S 20/20 (2018.01), F24S 23/00. Пристрій для концентрації і передачі сонячного випромінювання / Чернозьомов Є.С. № а 2018 06907; заяв. 20.06.2018; опубл. 10.02.2020, Бюл. № 3.
- [5] Патент на корисну модель 149777, Україна, МПК (2021.01) F24S 10/00, F24S 20/00, F24S 23/00, G02B 6/00. Концентратор-коліматор сонячного випромінювання на основі гіперболоїда / Чернозьомов Є.С. № u 2021 04520; заяв. 04.08.2021; опубл. 01.12.2021, Бюл. № 48.

ПАРАЛЕЛЬНЕ МОДЕЛЮВАННЯ З ВИКОРИСТАННЯМ РЕАКТИВНИХ ПОТОКІВ

Зі зростанням складності моделювання для їх виконання потрібно все більше і більше обчислювальних ресурсів. Обчислювальна потужність все ще зростає за законом Мура, але зростання зміщене в горизонтальну площину, тобто відбувається за рахунок збільшення кількості паралельних процесорів і їх ядер. Через це існує потреба в розробці паралельних алгоритмів моделювання, здатних використовувати обчислювальні ресурси кількох ЦП.

Сьогодні існує кілька підходів до розпаралелювання симуляцій. Зокрема, можна розглянути алгоритм Time Warp [1], який детально описано в [2]. Цей алгоритм є предметом дослідження протягом багатьох років і має декілька реалізацій у коді [3], [4]. Однак Time Warp використовує власний протокол синхронізації, який є складним і низькорівневим [5].

Програмний каркас RxHLA (реактивна адаптація стандарту IEEE 1516) [6] схожий на Time Warp з точки зору складності та низького рівня.

Інший підхід, заснований на архітектурі CQRS+ES, описаний в [7]. Однак тут автор більше зосереджується на практичних аспектах реалізації без великої теоретичної бази.

Платформа моделювання HPC [8] також є більш практичним описом впровадження паралельного моделювання. Він заснований на акторах і бібліотеці АККА, що є більш консервативним підходом у порівнянні з реактивними потоками.

Ключова ідея цієї статті полягає у використанні протоколу синхронізації загального призначення для розпаралелювання симуляцій. А саме протокол реактивних потоків [9], зокрема його версія, реалізована в бібліотеці АККА [10].

Таким чином, з одного боку, ми маємо класичну математичну модель, з іншого боку, маємо протокол синхронізації загального призначення. І мета цієї роботи – приєднатися до них.

Моделювання — це процес побудови моделі **об'єкта** (у широкому розумінні [11]). Існує багато різновидів моделювання, але в цій статті ми будемо говорити лише про математичне моделювання.

По суті, «модель» — це спеціальний об'єкт (у нашому випадку це математичний об'єкт), який відображає інший об'єкт, який ми будемо називати **моделюваним об'єктом**. Модель відображає сукупність **властивостей** модельованого об'єкта, їх тип, структуру та зв'язки [12].

У фізичному світі будь-які зміни, які відбуваються з будь-яким фізичним об'єктом, вимагають певного **часу**. Тим не менш, при моделюванні в багатьох випадках час можна знехтувати. Особливо в тому випадку, коли модельований об'єкт не є фізичним.

Наприклад, якщо ми моделюємо деяку логічну схему і нас цікавить тільки набір вихідних сигналів щодо набору вхідних сигналів, то часом можна легко знехтувати.

Далі в цій роботі ми будемо розглядати час як одну з властивостей модельованого об'єкта. Час є обов'язковим для фізичних об'єктів, але в загальному випадку він може або не може бути включений у модель.

Побудовану модель можна використовувати в **моделюванні**, яке по суті є імітацією поведінки модельованого об'єкта [13], тобто імітацією зміни його властивостей відносно один одного. У цій роботі ми будемо говорити тільки про числове (комп'ютерне) моделювання.

Наприклад, ми можемо моделювати рухомий фізичний об'єкт, імітуючи зміни його координат відносно часу. Результатом моделювання є сукупність усіх змін, що відбуваються з об'єктом під час моделювання. Цей набір змін можна використовувати для аналізу та прогнозування поведінки об'єкта. Цей результат цінний тим, що він був отриманий без безпосереднього використання самого модельованого об'єкта.

Моделювання та симуляція здійснюються з метою вирішення якоїсь практичної або теоретичної задачі, надалі ми будемо називати цю задачу **задачею моделювання**.

Важливою властивістю моделі є **узгодженість моделі** з модельованим об'єктом. Іншими словами, швидкість відмінності між станом і поведінкою, передбаченими моделлю, від фактичного стану і поведінки модельованого об'єкта.

На практиці ми хотіли б, щоб модель якомога точніше відображала змодельований об'єкт, щоб отримати найточніший результат моделювання. Однак ми обмежені в ресурсах, таких як час для розробки моделі та обчислювальна потужність. Це означає, що побудована модель завжди буде компромісом між точністю та її вартістю. Це означає, що більшість моделей будуть несумісними з модельованим об'єктом, а рівень невідповідності в першу чергу залежатиме від вимог, визначених проблемою, які потрібно вирішити за допомогою моделювання.

Змінна - це математичний об'єкт, який позначається деяким символом і може бути пов'язаний з одним значенням із набору значень. Набір значень, які можна асоціювати зі змінною, будемо називати **областю визначення** змінної.

Ми не накладаємо жодних обмежень на типи значень, включених до домену змінної.

Певний модельований об'єкт може бути математично представлений у вигляді набору змінних, які відображають властивості (атрибути) цього об'єкта [14]. Назвемо такий набір **змінними моделі V**.

У більшості практичних випадків V буде абстрактним. Це означає, що з усіх можливих властивостей модельованого об'єкта ми вибираємо лише ті, які мають значення в контексті проблеми моделювання.

Процес відбору істотних властивостей називається побудовою **концептуальної моделі** [15].

Набір змінних та їх доменів повністю визначається задачею моделювання та відображеними властивостями. Це означає, що повинен існувати спосіб перетворити кількість властивості в значення зі змінної області. Будемо називати таке перетворення **вимірюванням**.

Змінні V можна розділити на три типи:

- **Незалежні змінні X :**
Відображати відомі властивості або вхідні дані. Типовим прикладом є змінна, яка відображає властивість часу.
- **Залежні змінні Y :**
Відображати невідомі властивості або результати. Значення цих змінних змінюються залежно від зміни незалежних змінних. Наприклад, відстань, яку пройде фізичний об'єкт, залежить від часу та його швидкості.
- **Параметри G :**
Значення параметрів не залежать від значень незалежних і залежних змінних. Це означає, що параметри не змінюються протягом симуляції. Як приклад можна розглянути силу тяжіння.

Ми припускаємо, що модельований об'єкт завжди має певний стан, тобто кожна властивість об'єкта має певну величину. Це можна представити як набір конкретних значень v_i з доменів V_i пов'язаних із набором змінних v_i . Будемо називати такий набір асоційованих значень **станом моделі \mathfrak{B}** .

Ми можемо графічно показати стан \mathfrak{B} як точку у фазовому просторі [16], яка визначається набором змінних V . А поведінку модельованого об'єкта як траєкторію, утворену переходами від поточного \mathfrak{B}_i до наступного \mathfrak{B}_{i+1} .

Якщо ми можемо пройти через усі можливі набори значень змінних V Якщо ми можемо пройти через усі можливі набори значень змінних \mathfrak{B} , то отримаємо набір станів, які фактично утворюють фазовий простір. Такий набір станів будемо називати **простором станів** і позначати символом V^n де n — розмірність простору.

Кожен стан \mathfrak{B} можна представити як набір **під-станів**, коли кожен із під-станів визначає лише частину значень $v_i \in \mathfrak{B}$. Повинен існувати спосіб визначити, які під-стани належать до певного V . Одним із варіантів досягнення цього є використання унікального **ключа**, щоб позначити всі під-стани належать до певного \mathfrak{B} .

Для деякого стану \mathfrak{B} , ми маємо набір під-станів $\{\mathfrak{S}_q^{\mathfrak{K}}\}$ з однаковим ключем \mathfrak{K} . и позначатимемо такий набір жирним $\mathfrak{S}^{\mathfrak{K}}$. При такому представленні стану \mathfrak{B} , необхідно переконатися, що всі $\mathfrak{S}_q^{\mathfrak{K}}$ позначені одним і тим же \mathfrak{K} не є суперечливими. Пара $\mathfrak{S}_q^{\mathfrak{K}}$ з однаковим ключем \mathfrak{K} , може бути суперечливою, якщо одне або більше значень $v_i \in \mathfrak{S}, \mathfrak{B}$ відрізняються під одним індексом.

Залежність змінних Y від X можна представити у вигляді набору станів $\mathfrak{S}^{\mathfrak{K}}$. Це представлення є альтернативою набору функцій $F(X|\mathfrak{G})$. У цьому

випадку зручно вибрати значення $\mathfrak{X} \in \mathbb{X}^n$ як значення \mathfrak{K} . І підмножину значень $\mathfrak{Y} \in \mathbb{Y}^n$ як значення \mathfrak{S} відповідно (включаючи $\mathfrak{S} = \emptyset$).

Так чи інакше, ми можемо визначити залежності змінних Y від змінних X і G , без безпосереднього вимірювання властивостей модельованого об'єкта [17]. Визначену таким чином залежність будемо називати **моделлю** модельованого об'єкта $\hat{Y}(\bar{X}|G)$.

На множині всіх можливих під-станів $\mathbb{S}^{\mathbb{X}|G}$ можна побудувати систему переходів, додавши її до множини **переходів** [18]. Кожне з яких визначає перехід від одного або кількох **відомих під-станів** $\mathfrak{S}_{q,k=1}^{\mathfrak{X}}, \dots, \mathfrak{S}_{q,k=n}^{\mathfrak{X}}$ до деякого **невідомого під-стану** $\mathfrak{S}_q^{\mathfrak{X}}$ і, можливо, параметризований деякою **підмножиною значень параметрів** із набору G .

На певній множині переходів θ^{l^G} , ми можемо визначити набір **функцій переходів**, кожна з яких описує підмножину множини θ^{l^G} . Іншими словами, функція переходу дозволяє нам знайти деякий перехід θ^{l^D} шляхом отримання або обчислення невідомого під-стану $\mathfrak{S}_q^{\mathfrak{X}} \xleftarrow{\theta^{l^D}}$, на основі набору відомих під-станів $\mathfrak{S}_{q,k=1}^{\mathfrak{X}}, \dots, \mathfrak{S}_{q,k=n}^{\mathfrak{X}} \xrightarrow{\theta^{l^D}}$ використовуючи певне правило побудови, можливо, параметризоване деяким $\mathfrak{D} \subseteq G$.

Ми можемо об'єднати функцію $\Theta^{l^{\mathfrak{B}}}_j \in \Theta^{l^G}$ і набір функцій $\Theta^{l^D}_{i,k=1}, \dots, \Theta^{l^D}_{i,k=n} \in \Theta^{l^G}$, представлених у вигляді графів. Продовжуючи таким же чином, послідовно об'єднуючи функції, що входять до одного набору Θ^{l^G} (можливо, використовуючи ту саму функцію більше одного разу), ми отримуємо деякий DAG. Будемо називати такий **граф переходів** DAG Γ^{l^G} . Крім того, необов'язково ми можемо об'єднати дві або більше кореневих змінних $S_{k,i=1}, \dots, S_{k,i=n}$, які не мають вхідних ребер, тим самим зменшуючи загальну кількість вузлів.

Коли ми об'єднуємо функції переходів Θ^{l^D} , ми також об'єднуємо переходи θ^{l^D} з еквівалентного набору $\theta^{l^D} \Leftrightarrow \Theta^{l^D}$, утворюючи набір більш складних DAG, які мають таку саму структуру, що й граф Γ^{l^G} , але складаються з під-станів $\mathfrak{S}_q^{\mathfrak{X}}$ і переходів θ^{l^D} . Ми будемо називати такі DAG **графами моделювання** γ^{l^G} .

На практиці нам потрібно буде знайти якийсь конкретний графік моделювання $\gamma^{l^G} \in \mathbf{Y}^{l^G} \Leftrightarrow \Gamma^{l^G}$ з деякого відомого набору узгоджених під-станів $\mathfrak{S}^{X|G} \subseteq \mathfrak{S}^{\mathfrak{X}}(\gamma^{l^G})$ пов'язаний із вузлами S графа Γ^{l^G} . Будемо називати такий $\mathfrak{S}^{X|G}$ **початковим набором під-станів**.

Пошук конкретного графа γ^{l^G} з деякою множиною \mathfrak{S}' може бути імперативно представлений як обчислення всіх функцій $\Theta^{l^D} \in \Theta(\Gamma^{l^G})$ з використанням \mathfrak{S}' як початкової аргументи цих функцій.

Представлення $Y = \langle \Gamma^{l^G}, \mathfrak{S}' \rangle^{\mathfrak{X}}$ можна використовувати як реалізацію моделі $\hat{Y}(\bar{X}|G)$, ми називаємо цю реалізацію **графовою моделлю** та позначаємо як

$$\hat{Y}(\bar{X}|\mathfrak{G})^\Gamma = \langle \Gamma^{|\mathfrak{G}}, \mathfrak{S}' \rangle^{\bar{X}} = \hat{Y}.$$

Концепція реактивних потоків була сформульована в 2014 році в маніфесті [9] і розширена розробниками бібліотеки АККА інструментами компонування реактивних потоків в **обчислювальні графи** [10, 19], які вже широко використовуються на практиці [20,8,21]. Вузли графа - це логічні процесори, а ребра - це канали, що представляють потік **повідомлень**, які передають дані, кожен з процесорів перетворює повідомлення тим чи іншим способом. Загалом реактивні потоки є реалізацією відомої парадигми програмування потоку даних [20].

У цьому розділі ми будемо використовувати підхід, описаний у [22], тобто складатимемо обчислювальну систему з невеликих блоків обробки, які обробляють потоки даних. Крім того, ми будемо використовувати реактивні потоки, які зроблять за нас усіх важку роботу з розподілу обчислень і балансування навантаження.

Символом M , будемо позначати повідомлення (значення), символом LP , будемо позначати повідомлення (значення), символом D – канали, що з'єднують процесори, символом, C – числовий граф.

Ми можемо перетворити довільну графічну модель $\hat{Y}(\bar{X}|\mathfrak{G})^\Gamma$ на обчислювальний граф C :

1. Для представлення кожного під-стану $\mathfrak{S}^x_q \in \mathfrak{S}^x(\Gamma^{|\mathfrak{G}})$ за допомогою повідомлення $M = [\mathfrak{S}^x_q]$.
2. Щоб замінити всі $\Theta^{|\mathfrak{S}} \in \Theta(\Gamma^{|\mathfrak{G}})$ для яких $S'_{k=1}, \dots, S'_{k=n} \in S(\mathfrak{S}')$ за допомогою повідомлення LP^{eval} :

$$\begin{aligned} S'_{k=1} \Rightarrow D_{k=1}, \dots, S'_{k=n} \Rightarrow \\ \Rightarrow D_{k=n} \xrightarrow{\Theta^{|\mathfrak{S}} \Rightarrow LP^{eval}} \hat{S} \Rightarrow D \end{aligned}$$

. І всі $\Theta^{|\mathfrak{S}}$, для яких $\hat{S} \in S(\mathfrak{S}')$, процесорами LP^{eval} , що еквівалентно оберненим функціям $\Theta^{-1|\mathfrak{S}}$:

$$\begin{aligned} \hat{S}' \Rightarrow D \xrightarrow{\Theta^{|\mathfrak{S}} \Rightarrow \Theta^{-1|\mathfrak{S}} \Rightarrow LP^{eval}} S_{k=1} \Rightarrow \\ \Rightarrow D_{k=1}, \dots, S_{k=n} \Rightarrow D_{k=n} \end{aligned}$$

3. Послідовно замініть усі функції $\Theta^{|\mathfrak{S}} \in \Theta(\Gamma^{|\mathfrak{G}})$, усі аргументи яких $S_{k=1}, \dots, S_{k=n}$ же замінені на канали $D_{k=1}, \dots, D_{k=n}$, що еквівалентно LP^{eval} :

$$D_{k=1}, \dots, D_{k=n} \xrightarrow{\Theta^{|\mathfrak{S}} \Rightarrow LP^{eval}} \hat{S} \Rightarrow D$$

. І послідовно замінити всі $\Theta^{|\mathbb{B}|}$, результат \hat{S} якого вже замінено каналом D , на LP^{eval} що еквівалентно оберненим функціям $\Theta^{-1^{|\mathbb{B}|}}$:

$$D \xrightarrow{\Theta^{|\mathbb{B}|} \Rightarrow \Theta^{-1^{|\mathbb{B}|}} \Rightarrow LP^{eval}} S_{k=1} \Rightarrow \\ \Rightarrow D_{k=1}, \dots, S_{k=n} \Rightarrow D_{k=n}$$

У результаті ми отримуємо граф C , що містить еквівалент LP^{eval} для кожного $\Theta^{|\mathbb{B}|} \in \Theta(\Gamma^{|\mathbb{G}|})$, але, можливо, має іншу структуру порівняно з $\Gamma^{|\mathbb{G}|}$, оскільки його побудова велася починаючи з $S' \in S(\mathfrak{S}')$, а не з кореневих вузлів $S_{root} \in S(\Gamma^{|\mathbb{G}|})$.

Далі кожен кореневий канал $D_{root} \in D(C)$ має бути з'єднаний із логічним процесором LP^{init} завданням якого є надсилання відповідного $M' = [\mathfrak{S}^{x_q}]$ де $\mathfrak{S}^{x_q} \in \mathfrak{S}^x(\mathfrak{S}')$, що запускає процес обчислення.

Крім того, всі або частина каналів $D \in D(C)$ повинні бути з'єднані з одним або декількома $LP^{collect}$, які збиратимуть частину або всі обчислені під-стани $\mathfrak{S}^x_q \in \mathfrak{S}^x(\gamma^{|\mathbb{G}|})$ що належить графу $\gamma^{|\mathbb{G}|} \in \mathcal{Y}^{|\mathbb{G}|} \Leftrightarrow \Gamma^{|\mathbb{G}|}$ заданому множиною початкових станів \mathfrak{S}' .

У найпростішому випадку ми можемо змоделювати модель $\hat{Y}(\bar{X}|\mathbb{G})^\Gamma$ за допомогою побудованого на ній графа C у два етапи:

- Обчислити множину під-станів

$$\mathfrak{S}^{\bar{X}|\mathbb{G}} = \mathfrak{S}^x(\gamma(\Gamma^{|\mathbb{G}|}|\mathfrak{S}'))$$

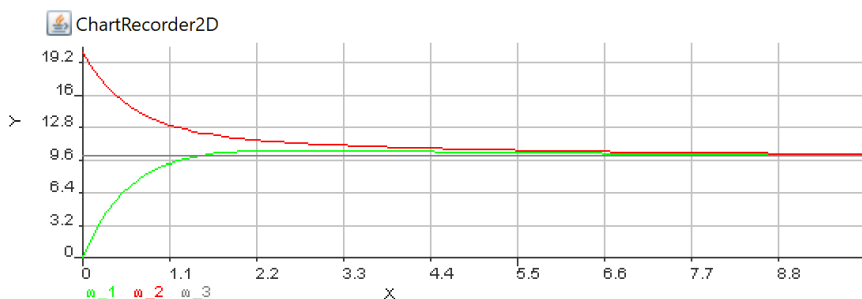
. Для цього ми ініціалізуємо обчислення, надсилаючи M' повідомлень за допомогою процесорів LP^{init} повідомлень за допомогою процесорів $LP^{collect}$ ми збираємо всі обчислені повідомлення $M = [\mathfrak{S}^x_q]$.

- Знайти всі під-стани для кожного ключа $\bar{X} \in \bar{\mathfrak{X}}$ і потім зібрати значення $\mathfrak{Y} \in \mathfrak{Y}$ зі знайдених під-станів.

Розглянемо класичну модель змішування фізіологічного розчину як імітований об'єкт. Будуємо графову модель $\hat{Y}(\bar{X}|\mathbb{G})^\Gamma$ цього об'єкта і обчислювальний граф C .

Використовуючи реактивні потоки з бібліотеки АККА, ми реалізували граф C у наївній формі.

Після виконання цього коду ми отримали результат моделювання (малюнок 1), який такий же, як ми отримали від реалізації моделі $\hat{Y}(\bar{X}|\mathbb{G})^S$.



Малюнок 1, моделювання моделі $\hat{Y}(\bar{X}|\mathcal{G})^{\Gamma}$ за допомогою графіка C

ВИСНОВОК

Графова модель, по суті, що представляє собою безліч функцій переходу між станами фазового простору, може бути реалізована у вигляді обчислювального графу. Кожен із вузлів обчислювального графу реалізує одну або декілька функцій переходу. Ребра обчислювального графа по суті є каналами передачі даних, якими між обчислювальними вузлами передаються початкові та обчислені суб-стану (повідомлення).

Завдяки тому, що Стани (точки фазового простору) розділені на суб-стани, кожен із станів може оброблятися кількома логічними процесорами одночасно. Таким чином досягається розпаралелювання обчислень, і відповідно прискорення процесу моделювання.

Можливість застосування даного підходу на практиці була показана на прикладі паралельного моделювання простої фізичної системи, реалізованого з допомогою програмування Scala і бібліотеки потокової обробки даних AKKA Streams.

- [1] D. R. Jeerson and H. A. Sowizral. Fast Concurrent Simulation using the Time Warp Mechanism, Part I: Local Control. Technical report, The Rand Corp., Santa Monica, CA, Dec 1982.
- [2] Richard M. Fujimoto, Parallel and Distributed Simulation Systems, 2000, p. 97.
- [3] R. Radhakrishnan, D. E. Martin, M. Chetlur, D. M. Rao, and P. A. Wilsey, "An object oriented time warp simulation kernel," in Proceedings of International Symposium on Computing in Object Oriented Parallel Environments, December 1998.
- [4] D. Jefferson, B. Beckman, F. Wieland, L. Blume, M. Diloreto, Time warp operating system, ACM SIGOPS Operating Systems Review, v.21 n.5, p.77-93, Nov. 1987.
- [5] D. M. Nicol and R. M. Fujimoto. Parallel Simulation Today. Annals of Operations Research, vol. 53, pp. 249–286, Dec. 1994.
- [6] Alberto Falcone, Alfredo Garro, Reactive HLA-based Distributed Simulation, Systems with RxHLA, 2018.
- [7] Andrzej Debski, Bartłomiej Szczepanik, Maciej Malawski, A Scalable, Reactive Architecture for Cloud Applications, 2018.

- [8] Jakub Bujas, Dawid Dworak, Wojciech Turek, Aleksander Byrski, High-performance computing framework with desynchronized information propagation for large-scale simulations, 2018.
- [9] Reactive stream initiative: <https://www.reactive-streams.org>.
- [10] The implementation of reactive streams in AKKA: <https://doc.akka.io/docs/akka/current/stream/stream-introduction.html>.
- [11] Peirce, Charles S. "Object". University of Helsinki. Retrieved 2009-03-19.
- [12] Achinstein, P. "Theoretical Models." *The British Journal for the Philosophy of Science* 16 (1965): 102-120.
- [13] J. Banks; J. Carson; B. Nelson; D. Nicol (2001). *Discrete-Event System Simulation*. Prentice Hall. p. 3. ISBN 0-13-088702-1.
- [14] Earl R. Babbie, *The Practice of Social Research*", 12th edition, Wadsworth Publishing, 2009, ISBN 0-495-59841-0, p. 14-18.
- [15] Myshkis A.D., *Elements of the theory of mathematical models*, 2007, p. 9.
- [16] Nolte, D. D. (2010). "The tangled tale of phase space". *Physics Today*. 63 (4): 33–38.
- [17] Myshkis A.D., *Elements of the theory of mathematical models*, 2007, p. 8.
- [18] Robert M. Keller (July 1976) "Formal Verification of Parallel Programs".
- [19] About the graphs in AKKA streams: <https://doc.akka.io/docs/akka/2.5/stream/stream-graphs.html>.
- [20] Zackary Kurima-Blough¹, Mark C. Lewis, Lisa Lacher, *Modern Parallelization for a Dataflow Programming Environment*, 2017.
- [21] Sivaramalingam Kirushanth, Boniface Kabaso, *Designing a Cloud-native Weigh-In-Motion*, 2019.
- [22] Marten Lohstroh, Iñigo Incer Romeo¹, Andr es Goens², Patricia Derler, Jeronimo Castrillon, Edward A. Lee¹, Alberto Sangiovanni-Vincentelli¹, *Reactors: A Deterministic Model for Composable Reactive Systems*, 2018.

ПРО ВІДПОВІДНІСТЬ ПРОЦЕСІВ У БІОЛОГІЧНИХ ТКАНИНАХ ТА НИЗЬКОТЕМПЕРАТУРНІЙ НАПІВПРОВІДНИКОВІЙ ПЛАЗМІ

Представлення сіточних електричних моделей у вигляді твердотілого моделюючого середовища (ТМС) свого часу було запропоновано академіком Г.Є. Пуховим [1]. За визначенням ТМС - це сукупність твердотілих пристроїв які використовують в якості еквівалентних моделюючих пристроїв які вирішують певне завдання. Зацікавленість у дослідженнях процесів у біологічних тканинах спонукало використання еквівалентних схем, зокрема, для визначення провідності біологічних тканин [2]. Результатом було певна еволюція поглядів стосовно побудови еквівалентної схеми провідності тканин та визначено процес формування потенціалу дії. Кількісна оцінка процесу потребувала рішення рівнянь в часткових похідних не вище другого порядку. Теоретичні питання стосовно моделювання кінцево-різницевого операторів резистивними сітками добре досліджені і потрібне визначити їх аксіоматичний характер. У випадку моделювання процесів, що відбуваються у біологічній структурі, з використанням ТМС виникають ускладнення. Переважним методом дослідження біологічних тканин залишається обчислювальний експеримент. В роботі [3] наведено теоретичні засади побудови неврівноваженої квазіаналогової моделі структурного типу з відсутністю в моделі електронних компонент з від'ємним опором. Схемотехнічно це виглядає як подвоєння ТМС, але з погляду інтегральної технології цей фактор ні є критичним, а використання метал-діелектрик-напівпровідник (МДН) структур для отримання ТМС є найбільш привабливим. У питаннях синтезу ТМС для біологічних тканин головним є пошук однозначної відповідності між математичними описом процесів та встановлення електробиологічної аналогії з метою отримання наочних фізичних результатів. Актуальність цього, щодо прикладного завдання, частково розглянуто в [4]. Для нанометрових МДН структур характерним є наявність нанорозмірних ефектів. Дослідження яких також відбувається за допомогою обчислювального експерименту з використанням методів кінцево-різницевої апроксимації, але система рівнянь є більш досконалою. Дещо збігається, але по відношенню до біологічних тканин використання системи рівнянь на основі тільки електротехнічних законів не виглядає як завершене щодо пояснення провідності на мікрорівні. Базовою системою рівнянь для дослідження провідності каналу транзисторної структури є система рівнянь у межах дифузійно-дрейфової моделі руху носіїв заряду у вигляді невиродженої низькотемпературної напівпровідникової плазми. В рамках цієї моделі вдається враховувати різні розмірні ефекти, таблиця 1, і надавати кількісну оцінку на фізичному рівні.

Таблиця 1

Відомі розмірні ефекти у МДН структурах

№	Нанорозмірний ефект
1	Модуляція довжини каналу (CLM ефект)
2	Прокол між стіком та витіком
3	Перекриття збіднених областей стіка та витіка
4	Ефект короткого каналу
5	Зворотний ефект вузького каналу
6	Зменшення рухливості внаслідок вертикальної складової компоненти електричного поля
7	Зменшення поперекової рухливості (насищення дрейфової швидкості носіїв в каналі)
8	Аномальне збільшення рухливості
9	Підпорогова провідність
10	Послідовний опір стік-витік
11	Зниження потенційного бар'єру над заслоном внаслідок напруги на витокі (DIBL-ефект)
12	Статичний зворотний зв'язок
13	Вплив горячих носіїв заряду
14	Ефект впливу підкладки обумовлений її струмом (SCBE ефект)
15	Вплив опору підкладки
16	Струм виток(утечки) індукований заслоном (GIDL/GISL ефект)
17	Ефект збедніння у полікремнієвому заслоні
18	Ефект квантування інверсного шару
19	Ефект неодності легування
20	Струм тунелювання скрізь заслон
21	Динамічний зсув порогової напруги
22	Тунелювання скрізь р-п переходи (TAT ефект)
23	Ніквастатичний ефект
24	Ефект саморозігріву
25	Врахування перекриття заслоном областей витоку і стіку
26	Ефект близькості карману (WPE ефект)
27	Ефект впливу ізоляції мілкими канавками(STE ефект)

У загальному вигляді систему рівнянь побудовано з урахуванням процесів генерації та рекомбінації зарядів, їхньої рухливості, дифузії електронів та дірок та з дотримання законів характерних для електромагнітних явищ. По відношенню до системи рівнянь еквівалентної схеми провідності біологічних структур то вони виглядають явно як недооцінені, хоча і визначають провідність на макроскопічному рівні. Процеси у біологічних тканинах є чутливими до нанорозмірних ефектів і це спонукає до пошуку аналогій з розмірними ефектами подібними до транзисторної структури. Зокрема, у поверхневому шарі транзисторної структури викривлення енергетичних зон супроводжуються зміною зарядового стану самої поверхні, аналогічне явище спостерігають для мембранної оболонки клітин при проходженні потенціалу дії. Встановлення

з'язку між змінами енергетичного стану біологічної структури та зміною енергетичного стану низькотемпературної напівпровідникової плазми може бути аргументом на користь встановлення електробиологічних аналогій для дослідження процесів які відбуваються у біологічних тканин в умовах дії абіотичних факторів. Гіпотетичне уявлення, що біологічним структурам характерна наявність фазових переходів і які характеризуються зміною кінетичних коефіцієнтів та наявністю аномальної поведінки відгуку на вплив зовнішнього фактору потрібно розглядати методом *ab initio*, тобто виходячі з перших принципів.

Проведений аналіз ситуації, з погляду на конвергентну технологію, дозволяє визначити подальший розвиток теоретичних поглядів на з'язок розмірних ефектів нанорівня для МДН структур та біологічних тканин по відношенню до можливості реєстрації відгуків на зовнішні збурення. Визначено які ефекти мають вплив на МДН структури і прояв яких визначають за системою рівнянь для низькотемпературної напівпровідникової плазми. Завданням для подальшого дослідження є виконання узагальнення на основі принципа аналогій та визначення системообразуючих факторів для тканин біологічних об'єктів.

- [1] Пухов Г.Е. Методы анализа и синтеза квазианалоговых электронных цепей – Наукова думка, Киев, 1967. – С. 554 – 559.
- [2] Волков С. И., Бульба Є. М., Смердова Т. А. Аналіз збудження біологічної структури електричними імпульсами. – Вісник Полтавської державної аграрної академії, №2, 2012. – С.190 – 194.
- [3] Осинов С.Н. Метод синтеза многослойной сеточной структуры / Осинов С.Н.//Электроника и связь. – 2010. – №5 – С.69 – 71.
- [4] Осинов С. М., Єрьоменко І. В. Оцінка точності моделювання процесу електричної провідності біологічних тканин. – матеріали ІХ Міжнар. наук. –прак. конф. «АКІТ-2023», м.Київ, 19 квітня 2023р. / НТУУ «КПІ» ім.Горького Сікорського, м.Київ, 2023. – С.47 – 49.

СЦЕНАРІЙ ВИКОРИСТАННЯ МАЛИХ МОДУЛЬНИХ РЕАКТОРІВ З НАКОПИЧУВАЧАМИ ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ В ЗАГАЛЬНОМУ БАЛАНСІ ОЕС УКРАЇНИ

Одну з ключових ролей у забезпеченні функціонування об'єднаної енергетичної системи (ОЕС) України [1] відіграє атомна енергетика, що забезпечує переважну частину покриття базового навантаження в добовому циклі споживання електричної енергії. За існуючих сьогодні обставин функціонування вітчизняної енергетики в умовах бойових дій в Україні, вона не лише продовжує розглядати і використовувати атомну енергію, як одне з ефективних низьковуглецевих джерел виробництва електричної енергії, але й не відмовляється від планів її розвитку під час повоєнного відновлення і будівництва нових атомних енергоблоків.

Важливою проблемою є нестача в ОЕС України маневрових і резервних генеруючих потужностей [2], що обумовлено зростанням частки ВДЕ в загальному балансі ОЕС України [3, 4] і створенням за рахунок ВДЕ додаткових значних небалансів електричної енергії [5, 6]. Це визначає актуальність створення додаткових маневрових та резервних потужностей, які забезпечать сталу роботу ОЕС України, шляхом вирішення проблеми нестачі маневрових та резервних енергоблоків. Для вирішення цієї проблеми є необхідним впровадження нових технологій розподіленої генерації, перш за все маневрових енергетичних установок (МЕУ) на базі малих модульних реакторів (ММР), і акумуляування «надлишкової» електричної енергії в часи зниженого споживання з ефективним її поверненням в ОЕС в часи пікового споживання за рахунок використання систем накопичення електроенергії (СНЕ) [7-9].

Важливою складовою аналізу перспектив використання МЕУ з ММР та СНЕ є розробка сценаріїв участі та імітаційні моделі їх задіяння у різних сегментах ринку електричної енергії України [12], з урахуванням функціонування ОЕС України в умовах ринку електричної енергії [10, 11], які дозволять оцінити ефективність їх використання для балансування ОЕС України.

За результатами проведених досліджень виділені наступні варіанти покриття електроспоживання ОЕС України:

- 1) базовий режим покриття добового графіка електроспоживання;
- 2) режим покриття добового графіка електроспоживання з посиленням для ранкового і вечірнього піків;
- 3) режим компенсації профіциту СЕС у літній період року.

Сценарій покриття навантаження ОЕС України базується на наступних принципах:

- ММР працює в режимі незмінного навантаження протягом розрахункової доби;

- СНЕ здійснює накопичення (заряд) електроенергії у нічний період доби від 23:00 до 7:00 з незмінним максимальним завантаженням;
- СНЕ здійснює відпуск (розряд) електроенергії у денний період доби від 7:00 до 23:00 з рівномірним завантаженням.

Сценарій дозволяє розв'язати задачі загальної оцінки економічної ефективності використання СНЕ з ММР.

Розширення попереднього сценарію покриття навантаження ОЕС України із змінним графіком розряду СНЕ базується на наступних принципах:

- ММР працює в режимі незмінного навантаження протягом розрахункової доби;
- СНЕ здійснює накопичення (заряд) електроенергії у нічний період доби від 23:00 до 7:00 з незмінним максимальним завантаженням;
- СНЕ здійснює відпуск (розряд) електроенергії у денний період доби від 7:00 до 23:00;
- протягом 2-х годин ранкового піку та 2-х годин вечірнього піку (сумарно 4 години за розрахункову добу) СНЕ здійснює відпуск (розряд) електроенергії з максимальним завантаженням;
- протягом 12- годин денного періоду СНЕ здійснює відпуск (розряд) електроенергії в режимі рівномірних витрат накопиченого заряду.

Сценарій дозволяє розв'язати задачу загальної оцінки економічних перспектив надання послуги резерву заміщення на завантаження для Оператора системи передачі.

Режим компенсації профіциту СЕС у літній період року передбачає розширення попереднього сценарію покриття навантаження ОЕС України із змінним графіком розряду СНЕ та базується на наступних принципах:

- ММР працює в режимі незмінного навантаження протягом розрахункової доби;
- СНЕ здійснює накопичення (заряд) електроенергії у нічний період доби від 23:00 до 7:00 з незмінним максимальним завантаженням;
- СНЕ здійснює відпуск (розряд) електроенергії у денний період доби від 7:00 до 23:00;
- протягом годин ранкового піку електроспоживання СНЕ здійснює відпуск (розряд) електроенергії з максимальним завантаженням;
- протягом годин профіциту СЕС (попередньо передбачаються сценарії компенсації протягом 2-х годин з 12:00 до 14:00 та протягом 4-х годин з 11:00 до 15:00) СНЕ компенсаційне накопичення електричної енергії;
- протягом денного періоду до 23:00 СНЕ здійснює відпуск (розряд) електроенергії в режимі рівномірних витрат накопиченого заряду.

Сценарій дозволяє розв'язати задачі оцінки технологічних можливостей СНЕ щодо обсягів компенсації профіциту СЕС у літній період року та оцінки економічних перспектив надання послуги резерву заміщення на розвантаження для Оператора системи передачі [13].

- [1] Кириленко О.В., Павловський, В.В., Блінов, І.В.: Науково-технічне забезпечення організації роботи ОЕС України в синхронному режимі з європейською континентальною енергетичною системою ENTSO-E. Технічна електродинаміка. 2022. № 5, С 59-66. DOI: <https://doi.org/10.15407/techned2022.05.059>
- [2] Звіт з оцінки відповідності (достатності) генеруючих потужностей для покриття прогнозованого попиту на електричну енергію та забезпечення необхідного резерву у 2020 році. НЕК Укренерго. 2020. 122 с.
- [3] Кириленко О.В., Басок Б.І., Базеев С.Т., Блінов І.В. Енергетика України та реалії глобального потепління// Технічна електродинаміка. 2020. № 3. С 52–61. DOI: <https://doi.org/10.15407/techned2020.03.052>
- [4] Басок Б.І., Буткевич О.Ф., Дубовський С.В. Техніко–економічні аспекти оцінювання перспектив декарбонізації об'єднаної енергосистеми України/ Технічна електродинаміка. 2021. №5. С.55–62. doi.org/10.15407/techned2021.05.055.
- [5] Blinov I, Miroshnyk V., Sychova V.. Comparison of models for short-term forecasting of electricity imbalances. 2022 IEEE 8th International Conference on Energy Smart Systems (ESS). IEEE, 2022. DOI: 10.1109/ESS57819.2022.9969288
- [6] Сичова, В. 2022. Прогнозування добових графіків сумарних небалансів електричної енергії в ОЕС України. Технічна електродинаміка. 2022, № 4, С 59-63. DOI:<https://doi.org/10.15407/techned2022.04.059>.
- [7] Кириленко О.В., Блінов І.В., Парус С.В., Трач І.В. Оцінка ефективності використання систем накопичення електроенергії в електричних мережах. Технічна електродинаміка. 2021. № 4. С 44-54. DOI: <https://doi.org/10.15407/techned2021.04.044>
- [8] Парус С.В., Блінов І.В., Олефір Д.О. Оцінка економічного ефекту від надання системами накопичення електричної енергії послуги балансування в ОЕС України. Праці Інституту електродинаміки Національної академії наук України. 2021. №60. С.28-37. DOI: <https://doi.org/10.15407/publishing2021.60.028>
- [9] Blinov I, Trach I, Parus Y., Khomenko V., Kuchanskyu V., Shkarupylo V., "Evaluation of The Efficiency of The Use of Electricity Storage Systems in The Balancing Group and The Small Distribution System," 2021 IEEE 2nd KhPI Week on Advanced Technology (KhPIWeek), 2021, pp. 262-265, doi: 10.1109/KhPIWeek53812.2021.9569981.
- [10] Про ринок електричної енергії: Закон України від 13.04.2017 №2019-VIII.
- [11] Blinov I, Kyrylenko O., Parus E., Rybina O. Decentralized Market Coupling with Taking Account Power Systems Transmission Network Constraints. Power Systems Research and Operation. Studies in Systems, Decision and Control. Vol 388. Springer, 2022. DOI: https://doi.org/10.1007/978-3-030-82926-1_1
- [12] Про затвердження Правил ринку: Постанова НКРЕКП № 307 від 14.03.2018.
- [13] Постанова НКРЕКП «Про затвердження кодексу системи передачі» №309 від 14.03.2018.

СКЛАДОВІ СИСТЕМИ МОНІТОРИНГУ АВАРІЙНИХ СТАНІВ КАБЕЛЬНИХ РОЗПОДІЛЬНИХ ЕЛЕКТРИЧНИХ МЕРЕЖ

Сьогодні одним із важливих напрямків розвитку електроенергетичної галузі як в світі, так і в Україні є удосконалення та побудова електроенергетичних мереж та систем згідно з концепцією Smart Grid. В 2022 році Міністерство енергетики України розробило «Концепцію впровадження “розумних мереж” в Україні до 2035 року» (Розпорядження КМУ № 908-р від 14 жовтня 2022 р.) [1], в якій розкрито поняття «розумних мереж», визначено загальні напрямки впровадження і використання технологій «розумних мереж» в енергетичному секторі України. Зокрема в цій Концепції зазначено, що платформа просування «розумних мереж» [2] в Україні спирається на готовий набір технологій і заходів, визначених у європейських та міжнародних стандартах, які визначають технологічні рішення реалізації для кожного компонента енергетичного сектора, а також готовий набір телекомунікаційних та інформаційних протоколів, що сприяють реалізації цих технологій [3, 4].

Однією із основних складових концепції Smart Grid є діагностування аварійних режимів електричних мереж та точна ідентифікація місць пошкоджень. Це обумовлено тим, що пошкодження електричних мереж позначається на якості та надійності електропостачання споживачів, що обумовлює важливість задачі швидкого і точного визначення місця пошкодження. Ефективне розв'язання цієї задачі дає значний економічний ефект, обумовлений скороченням перерв у електропостачанні, зменшенням транспортних витрат на обхід електричних мереж, мінімізацією загального часу організації ремонтно-відновлюваних робіт [5-7].

Засоби ідентифікації аварійних станів на ділянках як кабельних, так і повітряних електричних мереж знаходять все більше розповсюдження в електричних мережах європейських країн. Використання систем діагностування аварійних станів в електричних мережах підвищує рівень роботи мережі за рахунок оперативного виділення фрагментів електричних мереж, на яких сталася аварія, що набуває особливої актуальності в умовах бойових дій в Україні.

Також використання систем ідентифікації аварійних станів на ділянках електричних мереж поліпшують показники надійності електропостачання, зокрема і SAIDI та ENS, внаслідок зменшення часу пошуку пошкодженої ділянки електричної мережі.

На основі виконаних досліджень визначено, що найбільш функціональні системи моніторингу та визначення місць пошкоджень мають містити [8-13]: індикатори визначення місця пошкоджень для кабельних і повітряних ліній; програмне забезпечення для дистанційного керування і спостереження за мережею; зовнішні станції для дистанційного керування комутаційною апаратурою повітряних ліній електропередачі і підземних кабелів; інтерфейс

для зручної інтеграції з іншими системами диспетчерського керування та збору даних (SCADA); комунікаційну інфраструктуру для різноманітних засобів і протоколів зв'язку.

У відповідності із сформованими вимогами розроблено загальну структуру системи моніторингу аварійних станів з урахуванням використання програм-конверторів повідомлень від індикаторів пошкоджень у відповідні системи SCADA, основні складові якої для кабельної мережі 6-10 кВ наведено на рис.1, на якому: 1 – сенсор (трансформатор струму) індикаторів пошкоджень, 2 – блок управління індикатора, 3 – модуль передавання даних, 4 – прилад збору і передачі даних верхнього рівня (RTU) від індикаторів пошкоджень, 5 – інтерфейс для передачі даних від приладу збору і передачі даних верхнього рівня (RTU) до GSM- модему за допомогою SMS-повідомлень, 6 – GSM- модем, 7 – застосунок-конвертор, 8 – шлюз між користувацькою частиною інтерфейсу системи SCADA та програм-конверторів від індикаторами пошкоджень за протоколом IEC 60870-5-1049, 9 – користувацька частина інтерфейсу системи SCADA, 10.1....10.n – індикатори пошкоджень.

Призначення системи (рис.1) є індикація міжфазних КЗ та замикань на землю в одножильних і трьохжильних кабелях кабельної мережі 6-10 кВ з подальшою передачею інформації про пошкодження на рівень диспетчерського керування та збору даних (SCADA).

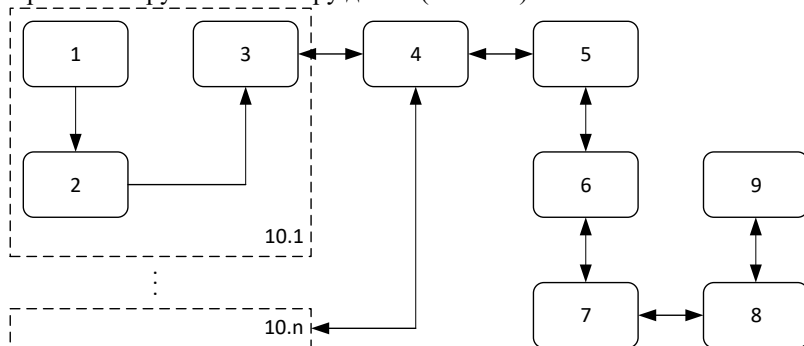


Рис.1. Основні складові системи моніторингу аварійних станів для кабельної мережі 6-10 кВ

У разі виникнення міжфазних КЗ та замикань на землю в кабельній лінії, сенсор (трансформатор струму), що встановлюється на кабельній муфті та може мати різні конфігурації (1), передає сигнал на блок управління індикатора (2). З блоку управління індикатора інформація передається на модуль передавання даних (3), який забезпечує її подальше передавання на прилад збору і передачі даних верхнього рівня за допомогою SMS-повідомлень. В якості протоколу передачі даних доцільно використувати перспективну мережеву технологію LoRaWAN. Використання технології LoRa дозволило значно підвищити чутливість приймача, як індикатора так і

системи контролю завдяки використанню модуляції з розширеним спектром [14]. Далі з приладу збору і передачі даних верхнього рівня (RTU), що агрегує інформацію з декількох модулів передавання даних на верхній рівень, інформація надходить в систему SCADA з використанням GSM-модему.

У SMS-повідомленнях міститься інформація щодо визначення факту спрацювання датчиків КЗ, типу КЗ, факту повернення датчиків у стан очікування КЗ після спрацювання, факту працездатності датчика КЗ у режимі очікування.

Важливо, що використання в загальній системі моніторингу SMS-повідомлень потребує використання застосунок-конверторів таких повідомлень у відповідні системи SCADA. Основним призначенням таких програм є реалізація шлюзу між індикаторами пошкоджень з передачею даних SMS (або TCP/IP) і системою SCADA за протоколом IEC 60870-5-104.

Для прийому та відправки повідомлень на індикатори пошкоджень потрібен тільки стандартний модем, а сама програма встановлюється на робочу станцію, розташовану в корпоративній мережі.

- [1] Про схвалення Концепції впровадження “розумних мереж” в Україні до 2035 року. Розпорядження КМУ № 908-рвід 14 жовтня 2022 р
- [2] IEC/TR 63097:2017 Smart grid standardization roadmap. 2017. 315 p.
- [3] Кириленко О.В., Блінов І.В., Зайцев Є.О. Палачов С.О., Васильченко В.І. Впровадження міжнародних та європейських стандартів для розвитку ОЕС України згідно концепції Smart Grid. Праці Інституту електродинаміки Національної академії наук України. 2022. № 63. С. 5-12. doi: <https://doi.org/10.15407/publishing2022.63.005>
- [4] Танкевич С.Є., Блінов І.В., Кириленко В.В. Україна та світ: нормативне забезпечення інтелектуальних електроенергетичних систем за концепцією Smart Grid. Стандартизація, сертифікація, якість. 2014. №4 (89). С. 38–44.
- [5] Блінов І.В., Парус Є.В., Поліщук О.Ю., Журавльов І.В. Моніторинг стану повітряних ліній електропередачі з використанням індикаторів пошкоджень. Енергетика та електрифікація. 2013. №13. С. 7-11.
- [6] Блінов І.В., Парус Є.В., Рибіна О.Б., Танкевич С.Є. Вибір оптимальної архітектури та складу системи моніторингу аварійних станів розподільних ліній. Праці Інституту електродинаміки Національної академії наук України. 2018. № 50. С. 16-22.
- [7] Бець О.Ю., Блінов І.В., Парус Є.В., Танкевич С.Є. Спосіб оцінки ефективності установки індикаторів пошкодження на воздушних лініях електропередачі. Праці Інституту електродинаміки Національної академії наук України. 2015. № 42. С. 32-36.
- [8] Blinov, I., Zaitsev, I., Parus, E., Bereznychenko, V. (2023). Faults Indicators Applying for Smart Monitoring System for Improving Reliability Electric Power Distribution. In: Kyrylenko, O., Denysiuk, S., Derevianko, D., Blinov, I., Zaitsev, I., Zaporozhets, A. (eds) Power Systems Research and Operation. Studies in Systems, Decision and Control, vol 220. Springer, Cham. doi: https://doi.org/10.1007/978-3-031-17554-1_11
- [9] Blinov I., Zaitsev I., Parus E., Bereznychenko V. Analysis of the effectiveness fault indicators use for control overhead power lines. In Proc. of the IEEE 8th

- International Conference on Energy Smart Systems (ESS-2022), Kyiv, Ukraine, 2022. DOI: 10.1109/ESS57819.2022.9969272
- [10] Кромпляс Б.А., Левицький А.С., Зайцев Є.О. Система автоматизованого налаштування інтелектуалізованих щитових вимірювачів електричних параметрів енергогенеруючих об'єктів. Праці Інституту електродинаміки НАН України. 2021. Вип. 59. С. 64–67. DOI: <https://doi.org/10.15407/publishing2021.59.064>
- [11] Зайцев Є., Березниченко В., Закусило С., Антоненко А. SMART засоби визначення аварійних станів в розподільних електричних мережах міст. Таврійський науковий вісник. Серія: Технічні науки. №5, С. 3-12. DOI: <https://doi.org/10.32851/tnv-tech.2022.5.1>
- [12] Блінов І.В., Зайцев Є.О. Питання актуальності побудови систем та засобів ідентифікації аварійних станів в розподільних електричних мережах України. Тези доповідей XL науково-технічної конференції молодих вчених та спеціалістів інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, 11 травня 2022 р, Київ: К.: ІПМЕ ім. Г.Є. Пухова НАН України, 2022. С.24–25.
- [13] Зайцев Є.О., Блінов І.В., Березниченко В.О., Закусило С.А. Засіб ідентифікації пошкодження лінії електропередавання в розподільчих електричних мережах. Контроль і управління в складних системах (КУСС-2022): Матеріали XIV міжнародної конференції, м. Вінниця, 15-17 листопада 2022 р. Вінниця: ВНТУ, 2022. 6 с. DOI: <https://doi.org/10.31649/mccs2022.21>
- [14] Зайцев Є.О., Закусило С.А., Березниченко В.О., Блінов І.В. Організація інформаційного обміну в системах контролю цілісності ліній розподілених мереж на базі технології LORA. VIII Всеукраїнська науково-практична конференція «Електронні та мехатронні системи: теорія, інновації, практика», 04 листопада 2022 року, м. Полтава. С.58-59.

Д.О. Олефір

ЩОДО ДОБОВОЇ ОПТИМІЗАЦІЇ РОЗПОДІЛУ ГІДРОРЕСУРСІВ ТА ВИРОБНИЧИХ ПОТУЖНОСТЕЙ ГЕС НА РИНКУ «НА ДОБУ НАПЕРЕД»

Сьогодні об'єднана енергетична система (ОЕС) України функціонує в умовах лібералізованого ринку електроенергії [1, 2] та значної частки відновлюваних джерел енергії в її загальному балансі [3]. Небаланси електричної енергії [4, 5], що створюються ВДЕ призводять до необхідності впровадження Оператором системи передачі (ОСП) в Україні (НЕК «Укренерго») [6, 7] технологічних обмежень як на обсяги генерації, так і в частині імпорту/експорту електричної енергії. Також необхідним є пошук нових способів балансування ОЕС України, зокрема за рахунок впровадження систем накопичення електроенергії [8, 9], підвищення точності прогнозування відпуску електричної енергії з ВДЕ, підвищення ефективності роботи існуючих маневрених генеруючих потужностей. Гідроелектростанції (ГЕС) в Україні виконують важливу функцію постачальника для Оператора системи передачі послуг відновлення частоти в ОЕС України. При цьому часто ГЕС отримують аварійні диспетчерські команди, зумовлені критичним дисбалансом обсягів виробництва/споживання електричної енергії в ОЕС України. Активне залучення ГЕС до регулювання режимів ОЕС України спричиняє суттєві відхилення витрат гідроресурсів від планових значень і до порушень технологічних обмежень водного балансу водосховищ [10-11]. Особливість постановки задачі планування витрат гідроресурсів по годинам розрахункової доби полягає у тому, що цільова функція задачі добової оптимізації має здійснювати розподіл гідроресурсів та виробничих потужностей ГЕС, доступних для продажу у сегменті ринку «на добу наперед» (РДН). У той же час баланс гідроресурсів має додатково враховувати витрату води на реалізацію угод, вже укладених в інших ринкових сегментах.

Основна ціль оптимізації полягає у максимізації вигоди електростанції, отриманої в результаті продажу електричної енергії за розрахункову добу. Оскільки на українському ринку електричної енергії укладаються договори з купівлі/продажу погодинних обсягів електричної енергії, то сумарна за добу вигода визначатиметься сумою значень вигоди по кожній годині розрахункової доби:

$$\sum_{h=1}^{24} B_h^{\text{HPS}} \rightarrow \max.$$

Для зменшення розмірності математичної моделі, якою подається задача оптимізації, всі технічні та економічні характеристики приводяться до балансу гідроресурсів на етапі підготовки до оптимізації. Приведена до балансу витрат гідроресурсів цільова функція містить такі змінні оптимізації,

як значення погодинних витрат води ГЕС $F_{\text{витр},h}^{\text{HPS}}$ протягом розрахункової доби. Тоді цільова функція набуває вигляду:

$$\sum_{h=1}^{24} B_h^{\text{HPS}} = \sum_{h=1}^{24} C_h^{\text{HPS}} \cdot F_{\text{витр},h}^{\text{HPS}} \rightarrow \max, \quad (1)$$

де: B_h^{HPS} – погодинна вигода від продажу електричної енергії (грн.); $F_{\text{витр},h}^{\text{HPS}}$ – погодинні витрати води на виробництво електричної енергії (м3); C_h^{HPS} – погодинна вигода від використання 1 м3 води на виробництво електричної енергії генераторами HPS (грн./м3).

Система обмежень для (1) враховує добовий баланс гідроресурсів у комплексі «Водосховище – ГЕС». Передусім така система обмежень має враховувати заданий на розрахункову добу обсяг коригування рівня заповнення водосховища, пов'язаний із річними та сезонними планами накопичення та витрати водних ресурсів. Крім того, якщо в (1) враховуються виключно доступні для продажу на РДН обсяги електричної енергії, то добовий баланс гідроресурсів у комплексі «водосховище – ГЕС» формується з урахуванням всіх витрат води. Зокрема, додатково до погодинних витрат гідроресурсів для продажу на РДН, обсяги яких оптимізуються в (1), слід враховувати і планові витрати води за вже укладеними договорами, наприклад в межах реалізації механізму покладання спеціальних обов'язків.

Добовий баланс погодинних витрат гідроресурсів узгоджується з різницею наповнення водосховища на початку та у кінці розрахункової доби:

$$\sum_{h=1}^{24} (F_{\text{над},h}^{\text{ГЕС}} - F_{\text{уд},h}^{\text{ГЕС}} - F_{\text{уд},h}^{\text{ГЕС}}) = W_{\text{кін}}^{\text{в.сх.}} - W_{\text{поч}}^{\text{в.сх.}}, \quad (2)$$

де: $F_{\text{над},h}^{\text{ГЕС}}$ – прогнозований обсяг надходження води до водосховища у розрахункову годину h (м3); $F_{\text{уд},h}^{\text{ГЕС}}$ – розрахунковий обсяг витрат води на виробництво електричної енергії за вже укладеними договорами у розрахункову годину h (м3); $W_{\text{поч}}^{\text{в.сх.}}$ – рівень заповнення водосховища на початку розрахункової доби (м3); $W_{\text{кін}}^{\text{в.сх.}}$ – рівень заповнення водосховища у кінці розрахункової доби (м3).

Використання значень початкового та кінцевого рівнів заповнення водосховища у (2) дозволяє узгодити добовий план виробничої діяльності ГЕС із сезонними та річними плановими показниками заповнення водосховища. Технічні та режимні обмеження ГЕС на етапі підготовки до оптимізації приводяться до значень мінімальних та максимальних витрат води на кожну годину розрахункової доби. Зокрема, обмеження мінімального та максимального рівнів завантаження генераторів ГЕС подається значеннями мінімальних та максимальних витрат води для забезпечення режимів відповідно мінімальної та максимальної генерації.

У цільовій функції (1) виконується розподіл виробничих потужностей ГЕС, доступних до продажу електричної енергії у сегменті РДН. Обсяг таких потужностей розраховується з урахуванням як вже фактично проданої у сегменті РДД електричної енергії, так і обсягів, зарезервованих під надання допоміжних послуг (РДП).

На кожну годину розрахункової доби рівень заповнення водосховища не повинен бути меншим за технологічний мінімум та не повинен перевищувати технологічний максимум. В обмеженнях водного балансу більш доцільно використовувати в розрахунках значення робочого об'єму водосховища і визначати рівні заповнення такого об'єму.

- [1] Про ринок електричної енергії: Закон України від 13.04.2017 №2019-VIII.
- [2] Про затвердження Правил ринку: Постанова НКРЕКП № 307 від 14.03.2018
- [3] Кириленко О.В., Басок Б.І., Базєєв Є.Т., Блінов І.В. Енергетика України та реалії глобального потепління// Технічна електродинаміка. 2020. № 3. С 52–61. DOI: <https://doi.org/10.15407/techned2020.03.052>
- [4] Blinov I., Miroshnyk V., Sychova V.. Comparison of models for short-term forecasting of electricity imbalances. 2022 IEEE 8th International Conference on Energy Smart Systems (ESS). IEEE, 2022. DOI: 10.1109/ESS57819.2022.9969288
- [5] Сичова, В. 2022. Прогнозування добових графіків сумарних небалансів електричної енергії в ОЕС України. Технічна електродинаміка. 2022, № 4, С 59-63. DOI:<https://doi.org/10.15407/techned2022.04.059>.
- [6] Кириленко О.В., Павловський, В.В., Блінов, І.В.: Науково-технічне забезпечення організації роботи ОЕС України в синхронному режимі з європейською континентальною енергетичною системою ENTSO-E. Технічна електродинаміка. 2022. № 5, С 59-66. DOI: <https://doi.org/10.15407/techned2022.05.059>
- [7] Звіт з оцінки відповідності (достатності) генеруючих потужностей для покриття прогнозованого попиту на електричну енергію та забезпечення необхідного резерву у 2020 році. НЕК Укренерго. 2020. 122 с.
- [8] Парус С.В., Блінов І.В., Олефір Д.О. Оцінка економічного ефекту від надання системами накопичення електричної енергії послуги балансування в ОЕС України. Праці Інституту електродинаміки Національної академії наук України. 2021. №60. С.28-37. DOI: <https://doi.org/10.15407/publishing2021.60.028>
- [9] Blinov I., Trach I., Parus Y., Khomenko V., Kuchansky V., Shkarupylo V., "Evaluation of The Efficiency of The Use of Electricity Storage Systems in The Balancing Group and The Small Distribution System," 2021 IEEE 2nd KhPI Week on Advanced Technology (KhPIWeek), 2021, pp. 262-265, doi: 10.1109/KhPIWeek53812.2021.9569981.
- [10] Олефір Д.О., Бабіч В.Ю, Блінов І.В. Актуальні проблеми забезпечення ОЕС України ресурсами регулювання частоти та потужності // Енергетика: економіка, технології, екологія, 2021, № 3, С. 39-46. DOI: <https://doi.org/10.20535/1813-5420.3.2021.251196>
- [11] Blinov I., Olefir D., Parus E. Model of optimal use of hydro power plants in the electricity market. Technical Electrodynamics. 2022. №2. pp. 60-69. DOI: <https://doi.org/10.15407/techned2022.04.042>

ВИЗНАЧЕННЯ КІЛЬКОСТІ БЛОКІВ ПІДТВЕРДЖЕННЯ У БЛОКЧЕЙНІ, В ЯКОМУ РОЗМІЩЕНО РЕЄСТР ДРУГОГО РІВНЯ У ВИПАДКУ, КОЛИ В ОБОХ БЛОКЧЕЙНАХ ВИКОРИСТОВУЄТЬСЯ ПРОТОКОЛ КОНСЕНСУСУ POS

В Україні відбувається активне формування державних реєстрів у різних галузях життя країни. Найпоширенішою практикою є створення Єдиних державних реєстрів, наприклад:

- Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань;
- Єдиний державний реєстр нерухомого майна;
- Єдиний державний реєстр боржників;
- Єдиний державний реєстр виборців

Питання захищеності державних реєстрів в Україні є доволі актуальним, оскільки такі реєстри містять важливу інформацію про громадян, компанії, нерухомість та інші важливі аспекти життя країни. Ці реєстри є джерелом інформації для проведення операцій з нерухомістю та отримання різного роду дозволів. Захист таких реєстрів є досить важливим завданням, оскільки їх уразливість може призвести до крадіжки особистої інформації, викрадення активів або підміни даних. Викрадення даних чи порушення роботи цих реєстрів може також призвести до фінансових збитків та інших негативних наслідків для громадян та компаній.

Одна з найбільших проблем, пов'язаних зі збереженням інформації у реєстрах, полягає у тому, що на сьогоднішній день не існує єдиної системи контролю існуючих реєстрів. У зв'язку з цим, ми пропонуємо рішення на основі блокчейну. Блокчейн – новий вид зберігання інформації, децентралізована база даних, представлена неперервним ланцюгом зв'язаних між собою блоків. Найбільшими перевагами даної технології є надійність, відмовостійкість та безпека. За невеликий проміжок часу її почали застосовувати для зберігання цифрових активів, ідентифікаційної інформації, захисту авторського права, голосування та інших речей. Все більше розвинутих країн починають використовувати блокчейн у державному секторі, збільшуючи надійність даних та зменшуючи значимість людського фактору, що знижує рівень корупції. Основна відмінність блокчейну від типових баз даних полягає в тому, що бази даних використовують таблиці для зберігання інформації, а блокчейн – блоки, що пов'язані один з одним. Блокчейн – це децентралізована база даних (P2P), у якій вся інформація міститься на великій кількості машин, які можуть знаходитись у будь-якій точці світу, і при цьому головний сервер відсутній. Ці комп'ютери називають вузлами. Блокчейн – прозора система, оскільки кожен бажаючий може отримати інформацію про будь-який блок.

Центральним поняттям блокчейн-технології є поняття так званого консенсусу, згідно якого функціонує певний блокчейн. Консенсус описує основні правила функціонування, в першу чергу – спосіб і правила генерації блоків у ньому. Алгоритм консенсусу – це механізм, який дозволяє користувачам мережі координувати свої дії у розподіленому середовищі.

Найбільш поширеними протоколами консенсусу у блокчейні є протоколи Proof of Work (PoW) та Proof of Stake (PoS). Спираючись на аналіз існуючих протоколів консенсусу в блокчейні, найбільш підходящим рішенням видається побудова каскадного реєстру саме на основі ідеї, запропонованої у протоколі PoP (Proof-of-Proof). Протокол PoP представляє новий тип каскадного блокчейну, який періодично публікує поточний стан одного блокчейну в іншому блокчейні.

Відповідно, модель каскадних реєстрів передбачає використання ієрархічної моделі блокчейнів, в якій на вершині ієрархії знаходиться єдиний державний блокчейн, якому, в свою чергу, підпорядковується мережа існуючих державних реєстрів, які ведуться на окремих блокчейнах.

Ми пропонуємо рішення, в основі якого використовується протокол консенсусу PoP, з наступних причин:

- цей протокол консенсусу розроблений саме для побудови таких каскадних структур (блокчейнів) та забезпечує надійність зберігання інформації у блокчейнах, на які посилається блокчейн вищого рівня, навіть за умови повної недовіри до кожного з блокчейнів, тобто за умови наявності зловмисників у кожному реєстрі, що належить нижчому рівню;

- реєстри нижчого рівня при цьому залишаються незалежними; зокрема, вони можуть базуватись на блокчейнах з різними типами консенсусів;

- єдиний реєстр, стосовно якого ми висуваємо припущення стосовно долі зловмисника – це реєстр самого верхнього рівня, який можна вважати найбільш стійким і з найбільшим ступенем довіри, оскільки він має вестись і підтримуватись якоюсь уповноваженою державною організацією;

- за необхідності, реєстр найвищого рівня, а також деякі з інших реєстрів, можуть бути частково або повністю централізованими або децентралізованими, в залежності від того, яка організація або компанія є відповідальною за цей реєстр і в який спосіб вона бажає його підтримувати (при цьому для параметрів централізованого та децентралізованого реєстру параметри та вимоги будуть, взагалі кажучи, відрізнятись).

Така каскадна структура реєстрів, при правильних параметрах її побудови та використання, забезпечує всі властивості правильного збереження інформації, такі як невідмовність, непідмінність та черговість розміщення в реєстрі.

Введемо наступні визначення: нехай SPB (Security-Providing blockchain) – це головний блокчейн, який відповідає основному реєстру, а SIB (Security Inheriting blockchain) – легкий блокчейн, який відповідає звичайним реєстрам, які взаємодіють з головним.

Блок C у легкому блокчейні є стабільним, якщо блок B у головному блокчейні стабільний, де B – перший блок у головному блокчейні, що посилається на блок C . Тоді щоб «скасувати» блок B в легкому блокчейні потрібно виконати досить довгий форк не тільки в легкому блокчейні, але й в головному блокчейні, що є важким обчислювальним завданням.

У цій роботі ми розглянемо випадок, коли в обох блокчейнах, SIB та SPB, використовується протокол консенсусу PoS. Нижче введемо необхідні позначення і сформулюємо отриманий результат.

Позначимо Δ_P та Δ_I довжини часових проміжків, відведених на формування блоку, у SPB, на якому розміщено реєстр першого рівня, та у SIB, на якому розміщено реєстр другого рівня, відповідно. Позначимо B_I деякий блок, що належить SIB, і в якому зроблено певний запис. Також позначимо $B_P(B_I)$ блок, що належить SPB, і в якому міститься перше (пряме) посилається на блок B_I . Нехай $\gamma \in (0, 1)$ – деяке маленьке число (порядку $10^{-3} - 10^{-4}$), і z_γ – кількість блоків підтвердження, після яких атака на підміну блоку у SPB є меншою за γ (відповідні формули для кількості блоків і імовірності були отримані у [2]).

Теорема.

Якщо після виходу блоку $B_P(B_I)$ у SPB, що містить реєстр 1-го рівня, вийшло не менше за k блоків у SIB, на якому розміщено реєстр другого рівня, то імовірність успіху атаки на підміну запису у блоку B_I не перевищує $P(\gamma, k)$, де

$$P(\gamma, k) = \gamma + e^{-\frac{\Delta_I}{\Delta_P} \cdot k} \cdot \sum_{l=0}^{z_\gamma - 1} \left(\frac{1}{l!} \cdot \left(\frac{\Delta_I}{\Delta_P} \cdot k \right)^l \right). \quad (1)$$

Ця теорема дозволяє визначити, скільки блоків у SIB повинно вийти, щоб імовірність підмінути відповідний блок, або запис у ньому, не перевищувала наперед задану величину, яку користувач задає за своїм бажанням. Тобто кожен може вибирати, виходячи зі своїх побажань, скільки блоків потрібно чекати до того моменту, коли відповідна угода, що була записана нотаріусом у блоку B_I , практично не може бути зміненою зловмисниками (наприклад, рейдерами).

- [1] Achieving Security in Proof-of-Proof Protocol with Non-Zero Synchronization Time / [Kovalchuk L., Kostanda V., Marukhnenko O., Pozhylenkov O.]
- [2] Blockchain technologies: Probability of double-spend attack on a proof-of-stake consensus / [Karpinski M., Kovalchuk L., Kochan R., Rodinko M, Wiclaw L.]

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

ПРИСВЯЧЕНА ДНЮ НАУКИ В УКРАЇНІ

Збірник матеріалів конференції
17 травня 2023 р.

Collection of materials of the XLI Scientific and technical conference of young scientists and specialists of G.E. Pukhov Institute for Modelling in Energy Engineering of National Academy of Sciences of Ukraine, Kyiv, May 17, 2023 / PIMEE of NAS of Ukraine. - 2023. - 191 p.

Зб. матеріалів XLI Науково-технічної конференції молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, м. Київ, 17 травня 2023 р. / ПМЕ ім. Г.Є. Пухова НАН України. – 2023. – 191 с.

Інформаційна підтримка:



[Сторінка конференції на
сайті Інституту](#)

[Telegram канал
РМВ НАН України](#)

