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

XLII
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
15 травня 2024 р.

Київ – 2024

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 №5 від 30 квітня 2024 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 XLII 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 15, 2024 / PIMEE of NAS of Ukraine. - 2024. - 171 p.

Збірник матеріалів XLII Науково-технічної конференції молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, м. Київ, 15 травня 2024 р. / ІПМЕ ім. Г.Є. Пухова НАН України. – 2024. – 171 с.

© Автори публікацій, 2024
© Інститут проблем моделювання в енергетиці
ім. Г.Є. Пухова НАН України, 2024

ЗМІСТ

Ф.О. Коробейніков
РЕЗИЛЬЄНТНІСТЬ В КОНТЕКСТІ КОНЦЕПЦІЇ ТРІАДИ ЧАСУ 7

S.O. Grechko
AI-COMPLETENESS 10

В.В. Зубок
ПОБУДОВА РЕЗИЛЬЄНТНИХ ERP-СИСТЕМ 14

П.С. Шпилюр, Ю.І. Дзюбан
ВИКОРИСТАННЯ ХОЛОДОАГЕНТУ (R290) ПРОПАН В ТЕПЛОВИХ НАСОСАХ 18

Ю.І. Дзюбан, П.С. Шпилюр
ВИКОРИСТАННЯ МАТЕРІАЛІВ ІЗ ФАЗОВИМ ПЕРЕХОДОМ У ТЕПЛОПОСТАЧАННІ ТА ОХОЛОДЖЕННІ 20

Д.В. Кулида
ВПРОВАДЖЕННЯ ТЕПЛОВИХ НАСОСІВ ТА ФОТОВОЛЬТАЇЧНОЇ СИСТЕМ В ТЕПЛО- ТА ЕНЕРГОЗАБЕЗПЕЧЕННЯ БУДИНКІВ 22

С.П. Данилів
МОДЕРНІЗАЦІЯ СИСТЕМ ЦЕНТРАЛІЗОВАНОГО ТЕПЛОПОСТАЧАННЯ З ВИКОРИСТАННЯМ ТЕПЛОВИХ НАСОСІВ 23

В.О. Верпета, А.О. Запорожець
ПЕРЕВАГИ ПРОГНОЗУВАННЯ ШВИДКОСТІ ВІТРУ НА ОСНОВІ ГІБРИДНИХ ПІДХОДІВ 27

Д.О. Євстаф'єв, А.О. Запорожець
ПЕРЕВАГИ ВИКОРИСТАННЯ УТЕПЛЮЮЧИХ МАТЕРІАЛІВ ІЗ ПЕРЕРОБЛЕНИХ ВІДХОДІВ ТЕКСТИЛЬНОГО ВИРОБНИЦТВА 29

Г.П. Костенко
ВИЗНАЧЕННЯ ТЕРМІНУ СЛУЖБИ ВТОРИННИХ БАТАРЕЙ ЕЛЕКТРОТРАНСПОРТУ В СИСТЕМАХ ЗБЕРІГАННЯ ЕНЕРГІЇ 31

В.В. Оранський
ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ ТЕПЛОВИХ НАСОСІВ ЯК ОСНОВНОГО ДЖЕРЕЛА ДЛЯ ТЕПЛОПОСТАЧАННЯ ТА ГАРЯЧОГО ВОДОПОСТАЧАННЯ ДЛЯ ВЕЛИКИХ ОБ'ЄКТІВ 35

D.V. Ratush
DESIGN OF INTELLIGENT AGENT FOR PROTECTION SYSTEM AND OPERATING SYSTEM DIAGNOSTICS 38

Д.П. Сінько
ПРОБЛЕМА РОЗДІЛЕННЯ МЕРЕЖІ В КОНТЕКСТІ РЕЗИЛЬЄНТНОСТІ КЛАСТЕРНИХ СИСТЕМ 40

Т.В. Пучко
МУРАШИНІ АЛГОРИТМИ В ЗАДАЧАХ ПЛАНУВАННЯ РОЗГОРТАННЯ ГЕНЕРУЮЧИХ ПОТУЖНОСТЕЙ ЕЛЕКТРОЕНЕРГЕТИЧНИХ СИСТЕМ 42

І.М. Корнієнко, О.О. Кузнєцова, Л.С. Ястремська, М.М. Барановський
БІОТЕХНОЛОГІЧНІ ПІДХОДИ ПЕРЕРОБКИ ОРГАНІЧНИХ ВІДХОДІВ – ПЕРСПЕКТИВНИЙ РОЗВИТОК БІОЕНЕРГЕТИКИ В КРАЇНАХ ЄС ТА УКРАЇНІ 45

М.Л. Дранік
ТЕПЛОВИЙ НАСОС ТА СОНЯЧНІ ФОТОЕЛЕКТРИЧНІ ПАНЕЛІ. ПРИНЦИПИ СУМІСНОЇ РОБОТИ ТА ОСНОВНІ ПЕРЕВАГИ 49

С.С. Шевченко
ПИТАННЯ БЕЗПЕКИ КОНТЕНТУ ТА ВИХІДНИХ МАТЕРІАЛІВ У ІНТЕРАКТИВНИХ НАВЧАЛЬНИХ СИСТЕМАХ 52

В.В. Шкарупило, О.А. Чемерис, В.В. Душеба
СТРАТИФІКОВАНИЙ ПІДХІД ДО ОПРАЦЮВАННЯ РЕЗИЛІЄНТНОСТІ У ГАЛУЗІ ЕНЕРГЕТИКИ 54

О.В. Харченко
АЛГОРИТМИ ТА ПРОГРАМНІ ЗАСОБИ ПАРАЛЕЛЬНОГО МОДЕЛЮВАННЯ ЗАДАЧ ПЛАНУВАННЯ РОЗВИТКУ ЕЛЕКТРОЕНЕРГЕТИЧНИХ СИСТЕМ 56

O.A. Kravchuk
ADVANCING SWARM INTELLIGENCE: AI WITH UNMANNED VEHICLE SYSTEMS FOR ENHANCED AUTONOMY AND COORDINATION 58

I.O. Dubovkina, A.O. Myronchuk
UNINTERRUPTED ENERGY SAVING MODE of WATER TREATMENT for GROWING CROPS 63

Р.І. Драгунцов
ОСОБЛИВОСТІ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ З ЗАЛУЧЕННЯМ ШКІДЛИВОГО ПЗ В УМОВАХ КІБЕРВІЙНИ – АНАЛІЗ ТА РЕАГУВАННЯ 65

В.М. Губаревич, О.А. Зайченко, Ю.В. Маруня, О.М. Рижков, Н.С. Зайченко
ДОСЛІДЖЕННЯ РОБОТИ ІНДУКТИВНО-ЄМНІСНОГО ПЕРЕТВОРЮВАЧА ЯК ДЖЕРЕЛА СТРУМУ ДЛЯ ТРАНЗИСТОРНОГО МОСТОВОГО ІНВЕРТОРА З ІНДУКТОРОМ 69

І.Е. Фуртат, Ю.О. Фуртат
KINETICS OF ADSORPTION DURING THE DYEING PROCESS 73

В.В. Кучанський, О.М. Коваленко
ЕКОЛОГІЧНІ АСПЕКТИ ДІАГНОСТУВАННЯ ПОВІТРЯНИХ ЛІНІЙ ЕЛЕКТРОПЕРЕДАВАННЯ БЕЗПІЛОТНИМИ ТЕХНІЧНИМИ ЗАСОБАМИ 75

В.В. Кучанський, Ю.Г. Лиховид
АНАЛІЗ ГРАНИЧНИХ РЕЖИМІВ РОБОТИ ЕЛЕКТРОЕНЕРГЕТИЧНИХ СИСТЕМ ЗА НЕПОВНОФАЗНИХ РЕЖИМІВ 77

О.А. Владимирський, І.А. Владимирський, Д.М. Семенюк
ЗАСТОСУВАННЯ ШВИДКОГО ПЕРЕТВОРЕННЯ ФУР'Є У КОРЕЛЯЦІЙНОМУ ПАРАМЕТРИЧНОМУ ТЕЧЕШУКАЧІ 80

О.А. Владимирський, І.А. Владимирський, І.П. Криворучко, Г.В. Анфімова
РОЗРОБКА СИЛОВИМІРЮВАЛЬНОЇ СИСТЕМИ МАНЕКЕН 1.03 84

С.Я. Гільгурт, А.В. Ковилін
ЗАСТОСУВАННЯ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ В ЕНЕРГЕТИЧНИХ СИСТЕМАХ 88

А.В. Давидюк
АКТИВНИЙ КІБЕРЗАХИСТ ДАТАЦЕНТРІВ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ 92

Н.В. Заїка, М.Ю. Комаров, Д.В. Ковалик
ВИКОРИСТАННЯ БПЛА ЯК ЕЛЕМЕНТ ТЕХНІЧНОГО ЗАХИСТУ НА ПІДПРИЄМСТВАХ ТА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ..... 97

Д.А. Коваль
МАТЕМАТИЧНА МОДЕЛЬ ДЛЯ ЧИСЛОВИХ РОЗРАХУНКІВ ЕЛЕКТРОМАГНІТНИХ ТА ЕЛЕКТРОМЕХАНІЧНИХ ПЕРЕХІДНИХ ПРОЦЕСІВ В СХЕМІ ГЕНЕРАЦІЇ ТА ВИДАЧІ ПОТУЖНОСТІ АЕС 100

О.О. Огір
ЕВОЛЮЦІЯ МЕТОДІВ ФОРМУВАННЯ АКУСТИЧНИХ ЗОБРАЖЕНЬ ДЕФЕКТІВ У СКАНОВАНИХ СЕРЕДОВИЩАХ: АНАЛІЗ ТА ПЕРСПЕКТИВИ ВИКОРИСТАННЯ СУЧАСНИХ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ 104

А.О. Лєпатьєв
ОПИС РОБОЧОЇ ДІЯЛЬНОСТІ РОЗРОБКИ ТРЕНАЖЕРНИХ ЗАНЯТЬ ДЛЯ ОПЕРАТИВНОГО ПЕРСОНАЛУ ПІДПРИЄМСТВ РОЗПОДІЛЬЧИХ МЕРЕЖ 107

Ю.А. Матвєєва, Е.І. Богдан
ВПЛИВ ДІДЖИТАЛІЗАЦІЇ НА ВПРОВАДЖЕННЯ ПРИНЦИПІВ БЕЗВУГЛЕЦЕВОЇ ЕКОНОМІКИ 109

О.С. Потенко, О.М. Дибач, С.Ф. Гончар
ЗАСІБ ОЦІНЮВАННЯ СУМИ РИЗИКІВ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ..... 113

В.С. Ракович, В.В. Цуркан
СПОСІБ ЗАХИЩАННЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ НА ОСНОВІ ЗАМКІВ ВИСОКОЇ БЕЗПЕКИ ЗА ТЕХНОЛОГІЄЮ ДОПОВНЕНОЇ РЕАЛЬНОСТІ 115

Д.М. Семенюк
МЕТОД ВИЯВЛЕННЯ ПРИХОВАНИХ ВИТОКІВ В НЕ НАПІРНИХ ПОЛІМЕРНИХ ТРУБОПРОВОДАХ ФІЛЬТРАЦІЇ БАСЕЙНІВ ЗА ДОПОМОГОЮ АКУСТИЧНОГО ТЕЧЕШУКАЧА А-10Т3 118

А.В. Полухін, Я.П. Лукашевич
АЛЬТЕРНАТИВНА ГЕНЕРАЦІЯ ЯК ШЛЯХ ДО РОЗВИТКУ РОЗПОДІЛЕНОГО ВИРОБНИЦТВА ТА ЕНЕРГЕТИЧНОЇ БЕЗПЕКИ В УКРАЇНІ 121

О.І. Клюзко
МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ЗАКУПІВЕЛЬНОЇ ДІЯЛЬНОСТІ КОМПАНІЇ-ПОСТАЧАЛЬНИКА ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ..... 127

В.В. Сичова
ЗАСТОСУВАННЯ ЙМОВІРНІСНИХ НЕЙРОННИХ МЕРЕЖ ДЛЯ ПРОГНОЗУВАННЯ ОБСЯГУ ПОПИТУ НА ПОСЛУГУ БАЛАНСУВАННЯ 130

А.І. Швайка, В.О. Артемчук, В.О. Бабак
АРХІТЕКТУРА MQTT БРОКЕРА TBMQ 134

О.І. Грамак, М.М. Ліневич
СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ПРОЦЕСІ ПРИЙНЯТТЯ РІШЕНЬ. КІБЕРБЕЗПЕКА ТА ШТУЧНИЙ ІНТЕЛЕКТ В ЕНЕРГЕТИЦІ 137

П.В. Шиманюк
SMART GRID МОДЕЛЬ ДЛЯ ОПЕРАТИВНОГО КЕРУВАННЯ РОЗПОДІЛЬНИМИ МЕРЕЖАМИ НА ОСНОВІ МЕТОДІВ ШТУЧНОГО ІНТЕЛЕКТУ 140

A.O. Kharlamova
ENSURING CYBER RESILIENCE IN THE ENERGY SECTOR: CHALLENGES, STRATEGIES AND EXAMPLES OF SUCCESSFUL IMPLEMENTATIONS 144

В.Р. Герасимов, В.В. Душеба
ОСНОВНІ ПІДХОДИ ТА ПРИНЦИПИ ОПТИМІЗАЦІЇ РОБОТИ РЕЛЯЦІЙНИХ БАЗ ДАНИХ 146

А.О. Тарановський
ПЕРСПЕКТИВИ ВИКОРИСТАННЯ АВТОНОМНИХ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ ДЛЯ СТВОРЕННЯ ТЕСТОВИХ ЗАВДАНЬ НА ПРИКЛАДІ LLAMA 149

О.О. Ципляк, В.О. Артемчук
ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ АВТОНОМНИХ НЕЙРОННИХ МЕРЕЖ АРХІТЕКТУРИ LLAMA ДЛЯ ПОБУДОВИ ГРАФІВ ЗНАНЬ 152

Д.І. Швайка, В.О. Артемчук
ДИНАМІЧНА СЕРІАЛІЗАЦІЯ PROTOCOL BUFFERS У IOT ПЛАТФОРМІ THINGSBOARD: НОВІ МОЖЛИВОСТІ 156

Є.С. Сметана
ОПИС ДІЯЛЬНОСТІ ДИСПЕТЧЕРА РОЗПОДІЛЬЧОЇ ЕЛЕКТРОМЕРЕЖІ ПРИ ОРГАНІЗАЦІЇ ПРОТИАВАРІЙНОГО ТРЕНУВАННЯ 158

Д.Р. Цвілій
ПОБУДОВА СТРУКТУРИ БАЗИ ДАНИХ ОБРОБКИ ФАКТОРНИХ ОЗНАК ДЛЯ ПРОГНОЗУВАННЯ ПОКАЗНИКІВ РОБОТИ ЕНЕРГЕТИЧНОГО РИНКУ 162

В.В. Станиціна, В.О. Артемчук, Н.П. Іваненко
ПЕРСПЕКТИВНІ НАПРЯМИ ДЕКАРБОНІЗАЦІЇ ВИРОБНИЦТВА ЦЕМЕНТУ В УКРАЇНІ 165

В.О. Артемчук, Ю.О. Гарбуз
РОЗВИТОК МЕТОДІВ І ЗАСОБІВ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ТА РЕЗИЛЬЄНТНОСТІ ЛОКАЛЬНИХ ДЕЦЕНТРАЛІЗОВАНИХ ЕЛЕКТРОЕНЕРГЕТИЧНИХ СИСТЕМ В УКРАЇНІ 166

М.В. Антонішин, Є.М. Харламов
РИЗИКИ ВИКОРИСТАННЯ МОБІЛЬНИХ ПРОГРАМНИХ ЗАСТОСУНКІВ В ЕНЕРГЕТИЧНІЙ СФЕРІ 169

Ф.О. Коробейніков

РЕЗИЛЬЄНТНІСТЬ В КОНТЕКСТІ КОНЦЕПЦІЇ ТРІАДИ ЧАСУ

Сучасне академічне та практичне осмислення резильєнтності продовжує бути центром активних наукових дебатів і багатоаспектних досліджень.

Досі не існує уніфікованого визначення суті резильєнтності, а для її концептуалізації переважно використовують три принципово різних типи візуальних образів:

1. Графічне зображення послідовних реакцій системи на критичні інциденти: очікування, абсорбція, відновлення, адаптація (Рис. 1);

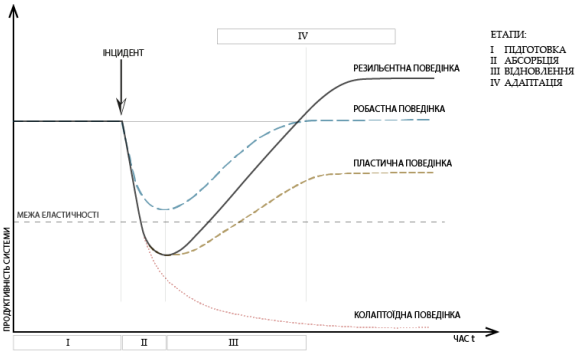


Рис. 1 – Графічне відображення послідовних етапів резильєнтної поведінки

2. Циклічні моделі таких реакцій, які містять елементи процесів, що багаторазово повторюються, базуючись на принципі зворотного зв'язку, як, наприклад, у зображенні адаптивного циклу Голлінга [1], циклу Бойда [2] або моделі Демінга (Рис. 2);

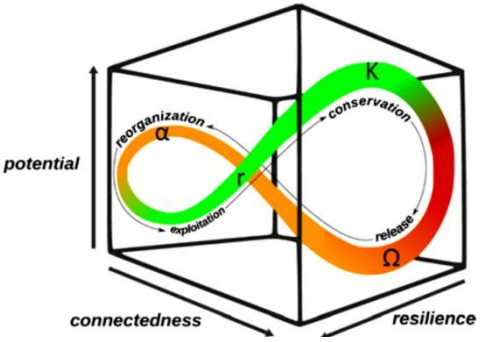


Рис. 2 – Еволюційний цикл Голлінга [3]

3. Візуальні подання критичних інцидентів, як точок біфуркації для ілюстрації моментів еволюційних змін в системі внаслідок адаптації до загроз, з якими ці інциденти пов'язані (Рис. 3).

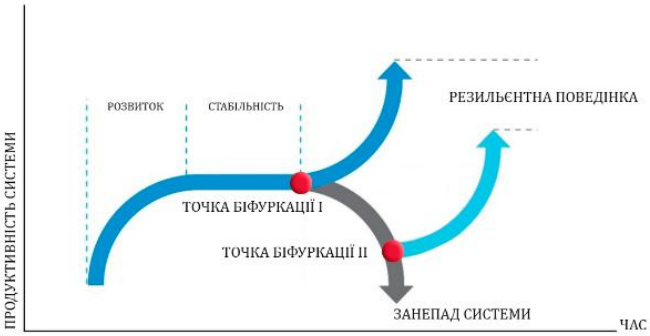


Рис. 3 – Біфуркаційна модель резильєнтності

Попри візуальні та концептуальні відмінності між різними підходами до моделювання резильєнтності, їх об'єднує включення *темпоральної компоненти*, характер і форма якої істотно різняться залежно від моделі:

- В моделях, що описують послідовні етапи реакції системи, часову структуру подано як лінійну незворотну "стрілу часу".
- У циклічних підходах час "закільцьовано" в періодичному відтворенні процесів, що підкреслює незмінність і передбачуваність системних операцій.
- У моделях, ґрунтованих на точках біфуркації, часовий аспект асоціюється з моментами критичних, потенційно трансформативних змін, коли система здатна до радикального перевизначення своїх функцій і параметрів.

Саме темпоральна компонента надає унікальну можливість для інтеграції трьох *різних, але концептуально не суперечливих* одна одній моделей резильєнтності.

Як об'єднуючу теоретичну основу пропонується використовувати античну філософську тріаду Хронос – Циклос – Кайрос [4, 5], що слугувала фундаментом для розуміння часу давньогрецькими вченими, філософами, жерцями і воєначальниками - усіма тими, хто мав ухвалювати важливі стратегічні рішення.

Між проявами часу в сучасних теоріях резильєнтності та античними поняттями часу можна простежити явний концептуальний паралелізм:

- *Хронос* (χρόνος) в античній філософії символізував невблаганну й послідовну течію часу, що регулює перебіг універсальних закономірностей і природних процесів. Цей аспект часу в сучасному контексті відображається в тих моделях резильєнтності, які використовують лінійні часові рамки, фокусуючись на послідовному прогресі. Вони забезпечують ефективність і передбачуваність, але можуть бути обмежені своєю ригідністю і нездатністю

до самоорганізації.

- *Циклос* (κύκλος) являє собою концепцію циклічного часу, що характеризується періодичністю і повторюваністю як природних, так і космічних процесів. Це трактування часу можна аналітично співставити із сучасними теоретичними моделями резильєнтності, в яких періодичне відновлення процесів у системі виконує критичну роль у підтримці її стабільності та здатності до адаптації.

- *Кайрос* (καιρός) – для античних філософів уособлював концепцію критичного або оптимального моменту, коли умови стають найсприятливішими для дій, що призводять до значних змін. Цей аспект часу набуває ключового значення в сучасних моделях резильєнтності, де здатність системи до адаптації та еволюції у відповідь на кризи залежить від точного визначення та використання таких моментів. Зокрема, Кайрос може бути асоційований із точками біфуркації [6], в яких система досягає максимально нестабільного стану, що дає змогу для переходу системи в якісно інший стан.

Розглянута темпоральна концепція не тільки ілюструє різні аспекти часу: лінійне продовження, циклічне повторення та оптимальні моменти для змін, але також надає методологічну рамку як для поєднання розрізнених концепцій, так і для синтезу дивергентних підходів до вивчення резильєнтної поведінки складних систем. Таким чином, глибоке розуміння і аналітичне застосування кожного з розглянутих аспектів часу та їхньої взаємодії може сприяти розробленню комплексних стратегій резильєнтності, які враховують як сталість і циклічність умов, так і можливості для стратегічних перетворень.

[1] Holling, C. S. 1986. Resilience of ecosystems; local surprise and global change. pp. 292-317 in Sustainable Development of the Biosphere, W. C. Clark and R. E. Munn, editors. Cambridge University Press, Cambridge.

[2] Ryder, M., & Downs, C. (2022). Rethinking reflective practice: John Boyd's OODA loop as an alternative to Kolb. The International Journal of Management Education, 20(3), 100703. https://doi.org/10.1016/j.ijme.2022.100703

[3] Castell, W. z., & Schrenk, H. (2020). Computing the adaptive cycle. Scientific Reports, 10(1). https://doi.org/10.1038/s41598-020-74888-y

[4] Ramalho, W. (2021). Reinterpreting the "times of crisis" based on the asymmetry between chronos and kairos. História da Historiografia: International Journal of Theory and History of Historiography, 14(35), 115–144. https://doi.org/10.15848/hh.v14i35.1733

[5] Orvain, J., & Gentil, S. (2024). Intertwining Times Structures: Assembling Chronos and Kairos. Research Gate. https://www.researchgate.net/publication/379512839_Intertwining_Times_Structures_Assembling_Chronos_and_Kairos

[6] Prigogine, Ilya; Nicolis, G. (1977). Self-Organization in Non-Equilibrium Systems. Wiley. ISBN 0-471-02401-5.

S.O. Grechko

AI-COMPLETENESS

In the exploration of intellect, delving into its structure, behaviors, and ultimate aspirations, we embark on a journey through the intricacies of cognition and understanding [1]. This text delves into the fundamental concepts of intensional versus extensional equality, contemplating intellect as a dynamic process navigating towards defined states. As we navigate through the labyrinth of intellect, we grapple with questions of self-awareness, problem-solving, and the inherent limitations that shape our cognitive landscapes.

Defining the structure of intellect inevitably leads to structural equality: two intellects are considered equal if all their structural components are equal. This implies the existence of an (efficient) algorithm for comparing all sub-structures with each other. Providing a (mathematically) precise description of the structure of intellect, whether natural or artificial, seems daunting, if possible at all.

However, another approach is conceivable: instead of attempting to exhaustively describe the internal structure of intellect, attention can be shifted to its external manifestations. The essence lies in the idea that if two intellects are indistinguishable to an external observer, then they are equal:

```
Goal
  (* Given any type and two arbitrary elements of it... *)
  forall (T : Type) (x y : T),
    (* ...if these two are equal up to an arbitrary predicate... *)
    (forall (P : T -> Prop), P x = P y) ->
    (* ...then they have to equal by construction too! *)
    x = y.
Proof.
  intros T x y H.
  specialize H with (fun z => x = z) ; simpl in H.
  rewrite <- H.
  reflexivity.
Qed.
```

As evident from the above proof, from a constructivist perspective, extensional equality implies intensional equality. Conversely, the reverse is also demonstrable:

```
Goal
  (* Given again any type and two arbitrary elements of it... *)
  forall (T : Type) (x y : T),
    (* ...if these two are structurally equal... *)
    x = y ->
    (* ...then the extensional equality of both is implied! *)
```

```
  forall (P : T -> Prop), P x = P y.
Proof.
 intros T x y Hxy P.
 rewrite <- Hxy.
 reflexivity.
Qed.
```

Does the second approach become more appealing? Purely mathematically, extensional equality implies iteration over all possible predicates:

forall (P : T -> Prop), P x = P y.

This would mean that the hypothetical "external observer" must ascertain the indistinguishability of two intellects in all their possible manifestations. In this formulation, the problem seems no easier than in the previous one. The following question arises: is it possible to conceive of intellect as a process that moves in a certain direction and aims to achieve some stable state?

The established term "machine learning" clearly indicates its process-oriented nature: after all, learning is an action extended over time. Viewing intellect as a (developing) process raises questions not only about the manner of this development but also about its goals. This allows us to reformulate the question posed above in the following terms: if intellect is a process and a target state is defined, which it seeks to achieve in its development (and through its development), can we operate with the Levenshtein distance equivalent to compare intellects with each other and calculate their equality (among other things)?

The answer to this question should consist of two fundamental parts:

1. An algorithmically resolvable description of possible states of intellect, primarily the current and target states.

2. An algorithm for computing the edit distance between any two states, primarily, again, the current and target states.

If both fundamental parts are given, then any two intellects will be equal if and only if:

— They are aimed at achieving the same state, and

— They are equidistant from it (that is, their current states are equally distant from the target state).

The reasoning above inevitably leads to a new question: how do we define such a "state" and how do we define the "target" state?

When considering this topic, it's necessary to note that a "state" becomes a kind of instantaneous atomic "snapshot" of intellect at a specific point (in time, or even broader – in its life and development). This resembles the "limit of a function at a point." In this context, it's appropriate to define a state as a finite set of propositions that the specific intellect subjectively attributes as "true" (in this specific state). Then, the process of (self-)learning is nothing but a transition from one finite set of subjectively true propositions to another.

The mention of a finite set automatically implies structural equality - if the number of elements is finite, comparing two such sets becomes trivial:

def eq(X, Y):

```
    if len(X) != len(Y):
      return False
    for x in X:
      if x not in Y:
        return False
  return True
```

When discussing intellect, it's implied that eventually intellect fully realizes its potential. In the context of the preceding discussion, this means that eventually the set of subjectively true propositions completely coincides with a subset of the set of objectively true propositions. Referring to a "subset of the set of objectively true propositions" assumes that the world is objectively knowable and that there are infinitely many truths that can potentially be "known" (for example, any arbitrarily large natural number is knowable, and there are infinitely many such numbers); however, due to the natural limitations of any intellect – reflected in the formal requirement of the finiteness of any state at any moment of development – no intellect is capable of knowing all objective truths, but only some subset of them.

In practice, following the theory of computational complexity and, in particular, mimicking the definition of NP-complete problems, it makes sense to identify the "most complex" true propositions – those whose invention and understanding require the greatest intellectual resources. Then, the concept of algorithmically efficient reduction turns into something like "if intellect I is able to understand the truth of any AI-complete proposition, then such intellect is sufficiently powerful to understand the truth of any other proposition from the set of objective truths within a finite time." The attachment to finite time is a projection of the concept of algorithmic solvability into the world of intellectual systems [2]: an intellect capable of understanding any truth in an infinite number of steps is as paradoxical as a function, by Gödel's incompleteness theorem [3], proving any statement:

Fixpoint Absurd : Type := Absurd.

Thanks to Coq's type system, the definition beneath is rejected. If that wouldn't be the case, literally any Type would have been inhabited, and thus every statement would have been provable within that system.

What is "AI-complete"? Which specific true propositions should be included in this class?

Searching for true propositions based on already known true propositions is akin to seeking proof based on axioms. It's known to be a semidecidable problem: if such a proof exists, it can be found within a finite number of iterations through lexicographic enumeration of all possible proofs. If such a proof does not exist (either because the intellect lacks certain axioms in its current state or because the statement is objectively undecidable within the deduction framework employed by the intellect), then such a search "loops" indefinitely.

Does this allow us to judge as follows: the main danger for intellect is the inability to distinguish between decidable problems and undecidable ones, the pursuit of solutions to which is inherently futile and, in practice, leads to stagnation

or the demise of intellect?

It turns out that the question of searching for and realizing the subjective boundaries of knowledge is a matter of "life or death" and is conditioned by:

— the objective limitations of deduction as a means of knowledge (the first and second incompleteness theorems of Gödel and all that follows from them),

— as well as the subjective skills in mastering this deduction by a specific intellect, the presence in its memory of all necessary axioms for solving a particular problem (for example, if an intellect has not yet grasped the concept of multiplying natural numbers, understanding exponentiation is automatically beyond its reach).

In that case, it's evident that any viable intellect primarily seeks to understand its boundaries?

If so, this allows us to judge the content of the target state: let not entirely, but at least some subset of it consist exclusively of propositions:

— "I know for sure that this problem has no solution" – this knowledge safeguards the intellect from stagnation and death;

— "I don't know if this problem has a solution" – this is the "space of doubts," the exploration of which leads to the intellect's development, enriching it with newly acquired truths: informally speaking, the wider it is, the less mature the intellect and the more work on itself lies ahead;

— "I know for sure that this problem is solvable..."

— "...but I don't have a solution yet" – in this case, finding a solution is nothing more than a matter of time and resources due to 2.3, or

— "...and I already have a solution" – which means that the intellect has successfully tackled this problem.

Conclusion: In conclusion, our exploration into the realms of intellect has illuminated fundamental concepts regarding its structure, behaviors, and intrinsic limitations. From the dichotomy of intensional and extensional equality to the pursuit of understanding the boundaries of knowledge, we have delved deep into the essence of cognition and self-awareness and introduced the “AI-completeness” phenomena aiming to capture the (theoretical) essence of intellect.

[1] Turing, A. M. (1950). "Computing Machinery and Intelligence." Mind, 59(236), 433-460.

[2] Minsky, M. L. (1967). "Computation: Finite and Infinite Machines." Prentice-Hall.

[3] Penrose, R. (1989). "The Emperor's New Mind: Concerning Computers, Minds, and The Laws of Physics." Oxford University Press.

В.В. Зубок

ПОБУДОВА РЕЗИЛЬЄНТНИХ ERP-СИСТЕМ

Системи планування ресурсів підприємства (ERP) є класом інтегрованих інформаційних систем, розроблених для автоматизації та оптимізації управління різними аспектами діяльності підприємства. Ці системи інтегрують фінанси, облік, управління виробництвом та ланцюжками постачання, кадровими ресурсами та іншими процесами. В результаті ERP-система здатна забезпечити учасників управління актуальною та однорідною інформацією.

Основні завдання ERP-системи можна сформулювати наступним чином:

— зниження дублювання даних,
— підвищення ефективності операцій,
— покращення прийняття рішень та, як наслідок, підвищення конкурентоспроможності підприємства.

Сучасна архітектура ERP-системи орієнтована на забезпечення максимальної гнучкості, швидкості та інтеграції з іншими технологіями та системами. Широке *використання хмарних рішень* забезпечує гнучкість та зменшення витрат на інфраструктуру ERP-системи. Сучасні ERP-системи використовують *мікросервісну архітектуру*, яка дозволяє розділити функціональність на невеликі незалежні компоненти. Це полегшує розробку, розгортання та масштабування системи. Разом з цим, наявність добре документованих *програмних інтерфейсів* (API) дозволяє легко інтегрувати ERP-систему з іншими застосунками та сервісами для забезпечення обміну даними з іншими системами. Протягом останніх років невід'ємною складовою архітектури ERP стали *засоби штучного інтелекту*, які широко використовуються для аналізу даних підприємства.

Незамінність ERP-системи для забезпечення безперервності бізнес процесів, а також чутливість даних, які обробляються в них, робить максимально актуальним завдання забезпечення стійкості ERP-систем у світлі зростаючих загроз кібератак і природних лих, а також в умовах мілітарних загроз, спрямованих на руйнування критичної інфраструктури та, як наслідку, проблем з електропостачанням. Збій чи відмова ERP призводить до серйозних втрат для підприємства через порушення виробничих процесів, руйнування ланцюгів постачання і т.і. Крім прямих фінансових збитків це призводить до репутаційних втрат. Тому ключове завдання - розробити та впровадити стратегії резильєнтності ERP-систем.

Найбільш широке визначення резильєнтності полягає в тому, що це здатність реагувати, поглинати, адаптуватися, відновлюватися та реконфігуруватися під час руйнівної події [1]. При визначенні резильєнтності розподілених комп'ютерних систем використовують такі характеристики як доступність (availability), стійкість до відмов (fault tolerance) та стійкість в умовах відмов (availability tolerance) [2]. Заходи із забезпечення

резильєнтності інформаційних систем завжди є багатодоменною структурою, яка включає в себе розроблення та реалізацію стратегій поводження з даними (data protection), резервного копіювання, призначення повноважень, надійної автентифікації, управління змінами та оновленнями (патчами), складання та тестування планів аварійного відновлення (DRP), та, не в останню чергу, навчанням персоналу. Деякі з цих питань розглядаються як заходи захисту інформації та кіберзахисту, втім, дві основних відмінності вирізняють резильєнтні системи – це здатність відновлюватись після критичних впливів та здатність реконфігуруватись, тобто забезпечити достатній рівень функцій за рахунок архітектурних змін.

Для ERP-систем традиційними є два архітектурні рішення. Перша архітектура – це розгортання системи на власному програмно-апаратному обладнанні підприємства. Це може відбуватись у власному приміщенні підприємства (in-premises) чи в спеціалізованому приміщенні постачальника послуг центру обробки даних (ЦОД). Ці варіанти характеризуються різними ризиками, але найбільш важливим буде порівняння з другим архітектурним рішенням – хмарною ERP-системою.

Хмарна система, або система технологій хмарних обчислень, є моделлю забезпечення «доступу на вимогу» до загального пулу конфігуровних обчислювальних ресурсів, які можуть бути оперативно надані і звільнені з мінімальними експлуатаційними витратами [3]. Хмарна система відноситься до обчислювальних компонентів (апаратне та програмне забезпечення, інфраструктура), які забезпечують надання послуг хмарних обчислень, таких як Програмне забезпечення як Послуга (SaaS), Платформа як Послуга (PaaS) та Інфраструктура як Послуга (IaaS).

Хмарні ERP-системи широко пропонуються та використовуються за моделлю SaaS та PaaS [4,5]. Так само локальні (in-premise) рішення ERP широко розповсюджені – їх використовує 25% компаній [6]. Для визначення переваг та недоліків цих архітектур в умовах існуючих загроз пропонується наступний SWOT-аналіз.

1. Сильні сторони локальної ERP:

1.1. Контроль над чутливими даними. Дані зберігаються, передаються та обробляються всередині інфраструктури, повний контроль над якою належить підприємству, і лише від підприємства залежить розроблення та реалізація політик захисту даних.

1.2. Можливість максимальної кастомізації. Налаштування: ці системи часто дозволяють широко налаштовувати відповідно до конкретних потреб організації, пропонуючи гнучкість у адаптації до унікальних бізнес-процесів.

1.3. Інтеграція з «спадковими» системами. В разі розгортання локальної ERP можна тісно інтегруватись з існуючими застарілими (legacy) системами та програмами, забезпечуючи безперебійний потік даних і взаємодію всередині організації.

1.4. Регуляторний вплив. Компаніям, які працюють у нормативно регульованих галузях, може бути легше підтримувати відповідність галузевим нормам і стандартам. Так, атестація систем захисту інформації, яка

обробляється в сторонній хмарі, буде обтяжена додатковими складнощами.

2. Слабкі сторони локального ERP:

2.1. Високі початкові витрати. Впровадження локальної ERP-системи зазвичай потребує значних початкових інвестицій в апаратне забезпечення, ліцензії на програмне забезпечення та налаштування інфраструктури.

2.2. Додаткові витрати на обслуговування обладнання та програмного забезпечення. Підприємства відповідають за поточне технічне обслуговування, оновлення та усунення несправностей, що може бути ресурсомістким і вимагати спеціалізованих IT-спеціалістів.

2.3. Масштабування локальної ERP-системи для зростання бізнесу може бути складним і дорогим, оскільки часто потребує придбання додаткового обладнання та розширення інфраструктури.

2.4. Обмежений доступ: доступ до локальних систем ERP може бути обмежений для користувачів у мережі компанії, що обмежує віддалений доступ і гнучкість для співробітників, які працюють поза офісом.

3. Переваги хмарних ERP:

3.1. Економічна ефективність. Хмарні ERP-системи зазвичай оплачуються за моделлю абонплати, яка залежить від набору доступних засобів та кількості акаунтів. Такий підхід зменшує початкові витрати та дозволяє підприємствам платити лише за ті ресурси, які вони використовують. Це робить хмарні системи економічно ефективнішими для малих і середніх підприємств (SME).

3.2. Масштабування хмарних ERP відбувається за вимогою, без фізичної перебудови інфраструктури і без потреби значних капіталовкладень.

3.3. Доступність. Хмарні ERP-системи за визначенням забезпечують віддалений доступ і питання надійності доступу у постачальників послуг ЦОД, як правило, вирішуються ефективно.

3.4. Автоматичні оновлення програмного забезпечення ERP, як і в принципі витрати на підтримання її функціонування, знаходяться в зоні відповідальності постачальника хмарної послуги.

4. Загрози хмарних ERP:

4.1. Проблеми з безпекою конфіденційних бізнес-даних, які довіряються стороннім хмарним провайдерам. Це може викликати проблеми відповідності рівня захисту постачальника послуг ЦОД та ризику несанкціонованого доступу або витоку даних.

4.2. Залежність від підключення до Інтернету, бо іншого способу доступу (типу спеціальні приміщення для стороннього персоналу) в хмарах відсутні.

4.3. Прив’язка до постачальника: перехід від хмарного постачальника ERP може бути складним через проблеми з переносом даних і залежність від власних технологій, що призводить до прив’язки до постачальника та зниження гнучкості.

4.4. Гнучкість налаштувань: хоча хмарні системи ERP пропонують певну гнучкість конфігурації, вони можуть не підтримувати широкі параметри налаштування порівняно з локальними рішеннями, що потенційно

обмежує їх придатність для підприємств із вузькоспеціалізованими вимогами.

За результатами проведеного аналізу можна виділити якості двох типових архітектурних рішень ERP, доступність, стійкість до відмов, стійкість в умовах відмов, а також окремо проаналізувати ці властивості архітектур з точки зору кращих практик кіберрезильєнтності [7].

[1] Linkov I and Trump B D 2019 The Science and Practice of Resilience Risk, Systems and Decisions (Cham:Springer) ISBN 978-3-030-04565-4. URL: https://doi.org/10.1007/978-3-030-04565-4

[2] Data centre facilities and infrastructures — Part 31: Key performance indicators for resilience (2023). Technical Specification ISO/IEC TS 22237-31. Informationtechnology — ISO/IEC.

[3] Liu, F. , Tong, J. , Mao, J. , Bohn, R. , Messina, J. , Badger, M. and Leaf, D. (2011), NIST Cloud Computing Reference Architecture, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD. DOI:10.6028/NIST.SP.500-292

[4] Forbes Advisor. Best Cloud ERP Software Of 2024 [online]. URL: https://www.forbes.com/advisor/business/software/best-cloud-erp-software/ (Accessed on 02/05/2024)

[5] Gartner Peer Insights. Cloud ERP for Product-Centric Enterprises reviews and Ratings [online]. URL: https://www.gartner.com/reviews/market/cloud-erp-for-product-centric-enterprises (Accessed on 03/05/2024)

[6] Instinctools. Cloud ERP vs. On-Premise ERP: Which One Wins the Duel?| Expert's Opinion [online]. URL: https://www.instinctools.com/blog/cloud-erp-vs-on-premise-erp-which-one-wins-the-duel-expert-s-opinion/ (Accessed on 04/05/2024)

[7] Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., and McQuaid, R. (2021), NIST Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD. DOI:10.6028/NIST.SP.800-160v2r1

П.С. Шпилюр, Ю.І. Дзюбан

ВИКОРИСТАННЯ ХОЛОДОАГЕНТУ (R290) ПРОПАН В ТЕПЛОВИХ НАСОСАХ

Пропан може бути використаний у теплових насосах як альтернативне паливо або робоча речовина, особливо в контексті геотермальних теплових насосів. Основні переваги використання пропану в теплових насосах:

1. Екологічність: пропан є відносно чистим паливом і не викидає в атмосферу таку кількість забруднюючих речовин, як інші види палива. Не шкодить озоновому шару.

2. Енергоефективність: пропан має високу енергетичну потужність, що дозволяє ефективно використовувати його у теплових насосах для опалення та гарячого водопостачання.

3. Доступність: пропан легко доступний і має широку мережу постачання, що дозволяє забезпечити його для використання у різних географічних регіонах.

4. Ефективність в низькі температури: пропан може ефективно працювати при низьких температурах, що робить його ідеальним вибором для об'єктів зимового опалення.

Ураховуючи ці переваги, використання пропану в теплових насосах може бути ефективним рішенням для забезпечення енергоефективного та екологічно чистого опалення.

На сьогоднішній день існує обмеження орієнтовно у 80 грам пропану у компресорах теплових насосів через вибухонебезпечність.

Таким чином, R290 - найпоширеніший і безпечний для навколишнього середовища холодоагент в світі. Виробництво R290 не вимагає великих витрат, його легко виділити з природного газу. Він не надає руйнівної дії на озоновий шар (ODP = 0) і має надзвичайно низький потенціал впливу на глобальне потепління (GWP = 3). Широту його використання в галузі холодильної техніки і кондиціювання повітря обмежує лише високий рівень займання.

Перспективним також вбачається використання не тільки окремих вуглеводнів в якості холодоагента, а й їх сумішей. Так використання суміші пропан-етан у пропановій холодильній установці низькотемпературної конденсації природного газу значно знижує температурний рівень роботи установки, дозволяє диференціювати температурні рівні ряду процесів і в цілому призводить до підвищення загальної термодинамічної ефективності процесів теплообміну в апаратах установки низькотемпературної конденсації природного газу.

— Низькі експлуатаційні витрати завдяки високій ефективності та надійності
— Температура подачі 70 °C при зовнішній температурі мінус 15 °C
— Можна використовувати існуючі радіатори; не потрібно

переобладнати підлогове опалення
- — Привабливий, високоякісний дизайн внутрішнього та зовнішнього блоків
- — Удосконалена акустична конструкція для низького рівня шуму під час роботи
- — Площа для встановлення лише 0,52 м² (Vitocal 252-A)
- — Екологічно безпечний холодоагент R290 з GWP = 3
- — Добре працює в поєднанні з існуючою конденсаторною системою
- — Просте керування завдяки вбудованому інтерфейсу WiFi через додаток
- — Замкнутий холодильний контур: для встановлення не потрібен холодильний сертифікат.

[1] Тепловий насос на пропані. https://www.viessmann.ua/uk/porady/tekhnolohiya-i-systemy/teplovi-nasosy/propan.html
[2] Compressors for air conditioning and heating. https://www.danfoss.com/en/products/dcs/compressors/compressors-for-air-conditioning-and-heating/#tab-overview

Ю.І. Дзюбан, П.С. Шпилюр

ВИКОРИСТАННЯ МАТЕРІАЛІВ ІЗ ФАЗОВИМ ПЕРЕХОДОМ У ТЕПЛОПОСТАЧАННІ ТА ОХОЛОДЖЕННІ

Тривале та ефективне зберігання теплової енергії, отриманої від відновлювальних джерел енергії, таких як сонце чи геотермальна енергія є ключовим фактором впливу на сталий розвиток теплотехніки. Одним з рішень, що може значно покращити ситуацію в цьому напрямку є використання фазового переходу речовин, який супроводжується поглинанням або виділенням значної кількості теплоти. При цьому енергія зберігатиметься у вигляді прихованого тепла, що значно знижує тепловтрати під час накопичення та зберігання енергії.

Приховане акумулювання дає змогу зберігати набагато більше енергії в порівнянні з звичайним баками, що використовують воду. Технології з використанням фазового переходу постійно розвиваються та приймають нові форми.

Одним з цікавих рішень вдосконалення традиційних систем акумулювання теплової енергії стали продукти «HeatSel» або «HeatStixx» (рисунок 1), що дозволяють в 3-4 рази підвищити теплову чи холодильну ємність баку. «HeatSel» та «HeatStixx» представляють собою полімерні модулі, що наповнюються відповідним матеріалом із зміною фази PCM (Phase Change Material). Зміна фази тут грає вирішальну роль. Залежно від матеріалу PCM (парафіни, гідрати солі тощо) при досягненні відповідної температури відбувається плавлення матеріалу (танення) і проходить процес акумуляції тепла. Таке латентне (приховане) зберігання енергії дозволяє накопичити значну кількість тепла та характерне відсутністю тепловтрат.

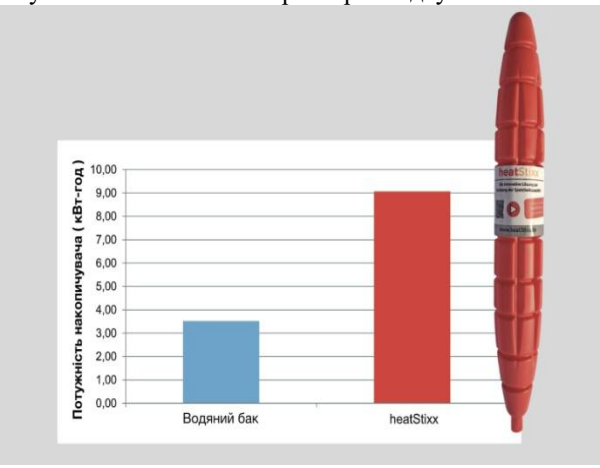


Рисунок 1. При зніманні тепла PCM знову твердне і цикл повторюється знову.

HeatStixx і HeatSel розроблені таким чином, що, крім великої площі поверхні, товщина шару PCM є дуже тонкою, що забезпечує участь всієї маси матеріалу у процесі фазової зміни, таким чином забезпечуючи ефективну передачу тепла (швидке заряджання та розрядження) навіть при дельтах з дуже низькою температурою. Завдяки роботі з водяним зберіганням, таке гібридне рішення надає максимально можливу динаміку процесам, і тому підходить для великої кількості застосувань у системах охолодження / кондиціонування та опалення.

HeatStixx розроблений спеціально для використання в стандартних накопичувальних баках. Сигароподібні еліпсоїди можна легко інтегрувати в будь-який бак, використовуючи стандартні патрубки підключення. Власники таких модернізованих систем можуть отримати додаткову вигоду за рахунок збільшення теплоємності своїх існуючих баків та оптимізації процесів накопичення та споживання енергії (наприклад запобігати кипінню (стагнації) сонячних установок)

[1] Нові матеріали з фазовим переходом. https://сахара.ua/kompaniya-statti-novi-materiali-z-fazovim-perehodom-heatsel-ta-heatstixx-dlja-vdoskonalennja
[2] HeatStixx®. https://www.axiotherm.de/de/produkte/heatstixx®/

Д.В. Кулида

ВПРОВАДЖЕННЯ ТЕПЛОВИХ НАСОСІВ ТА ФОТОВОЛЬТАЇЧНОЇ СИСТЕМ В ТЕПЛО- ТА ЕНЕРГОЗАБЕЗПЕЧЕННЯ БУДИНКІВ

В сучасних умовах, коли питання енергоефективності та екологічності стають все більш актуальними, використання теплового насосу в поєднанні з фотовольтаїчними панелями для приватних осель є необхідним кроком у напрямку створення сталого та ефективного енергетичного забезпечення. Ця комбінація технологій дозволяє оптимізувати використання сонячної енергії для не лише генерації електроенергії, але й для забезпечення опалення та гарячого водопостачання в будинку.

Використання теплового насосу у поєднанні з фотовольтаїчними панелями має ряд переваг. По-перше, це дозволяє зменшити залежність від традиційних джерел енергії, таких як газ чи електрика, тим самим знижуючи ризик зростання енергетичних витрат. По-друге, така система сприяє зменшенню викидів CO_2, оскільки використання сонячної енергії є екологічно чистим джерелом енергії. Крім того, забезпечується стабільне енергетичне забезпечення навіть у випадку відключення мережі.

Розвиток та впровадження таких систем є ключовим етапом в переході до сталого енергетичного майбутнього. Враховуючи зростаючі енергетичні потреби та загрозу зміни клімату, використання теплового насосу в поєднанні з фотовольтаїчними панелями для приватних осель стає ефективним та екологічно безпечним рішенням, спрямованим на створення енергоефективних та стало енергетичних систем для житлових будівель.

С.П. Данилів

МОДЕРНІЗАЦІЯ СИСТЕМ ЦЕНТРАЛІЗОВАНОГО ТЕПЛОПОСТАЧАННЯ З ВИКОРИСТАННЯМ ТЕПЛОВИХ НАСОСІВ

Переважна більшість систем централізованого теплопостачання в Україні потребують нагальної модернізації. Понад 75% котелень, що використовують стандартні газові котли не відповідають вимогам енергоефективності та екологічності. Близько 20% загальної кількості котлів експлуатуються понад 25 років та потребують заміни. [1]

Зношеність теплових мереж має критичні масштаби - 38 % (понад 7,5 тис.км) теплових мереж перебувають в аварійному стані. Середні теплові втрати в тепломережах досягають 20%, а в окремих випадках перевищують 40%. Рівень аварійності теплових мереж надзвичайно високий і наприклад: в Києві перевищує 2 пошкодження на рік на 1 км трубопроводу (в той же час, в більшості європейських країн цей показник не перевищує 0,1). [1]

Всі дані чітко демонструють нагальну необхідність комплексної модернізації систем централізованого теплопостачання. Потрібна не просто заміна обладнання та мереж, а створення нової системи теплопостачання з використанням відновлювальних джерел енергії та нових методів управління. Застосування ВДЕ в межах існуючих котелень в Україні не вирішить проблему зношених мереж, високих тепловтрат, значних витрат електроенергії для роботи потужних циркуляційних насосів, затрат на підготовку підживлювальної води.

Пропонується модернізувати існуючі системи централізованого теплопостачання шляхом створення локальних районних, квартальних, відомчих та будинкових теплопунктів на основі теплових насосів. Використовуючи теплові насоси різних типів та комбінацію декількох джерел низькопотенційного тепла для їх роботи, можна побудувати стійкі, високоефективні та екологічні системи, що забезпечать користувачів опаленням та гарячою водою за найнижчим тарифом. [2] Враховуючи нові чинники, спричинені війною, перехід до децентралізованих локальних систем, окрім економічних та екологічних вигод, зробить мережі теплопостачання більш стійкими та надійнішими. Теплові насоси також повністю відповідають стратегії електрифікації [3] всіх галузей економіки.

Децентралізація систем теплопостачання та перехід на відновлювальні джерела енергії може здійснюватись з використанням різних схем та комбінацій теплонасосного обладнання, основні з яких це:

— встановлення локальних теплових насосів повітря/вода;
— встановлення геотермальних теплових насосів, що використовують в якості джерела тепла «холодну тепломережу»;
— локальні теплопункти з тепловими насосами, що поєднують використання енергії зовнішнього повітря та тепла «холодної

тепломережі».

У випадку модернізації теплопостачання будівель за допомогою теплових насосів повітря/вода, пропонується застосовувати установки, які використовують високотемпературні холодоагенти, такі як наприклад: пропан (R290). [4] Такі системи дають змогу забезпечити об'єкт достатньо високою температурою теплоносія 70-75°С. [5] Відповідно, за умови проведення попередньої термомодернізації будівель (утеплення будинків, заміна вікон тощо), що має знизити початкову потребу в тепловій енергії, використання таких теплових насосів не потребуватиме заміни існуючих систем опалення на основі радіаторів. Вже сьогодні, робота теплового насосу повітря/вода до мінус 25°С температури зовнішнього повітря є стандартом для більшості пристроїв. [6] А річний показник ефективності теплових насосів повітря/вода може сягати 3 - 3,5, [7] тобто щоб забезпечити 3,5 кВт тепла використовується лише 1кВт електроенергії.

Застосування геотермальних теплових насосів робить систему теплопостачання ефективнішою та стійкішою, оскільки в якості джерела тепла використовувується більш стабільне низькопотенційне тепло ґрунту чи води. [8] Ключовим елементом теплонасосної установки є геотермальне поле. Від правильного проектування та експлуатації якого в цілому залежить ефективність та надійність роботи системи тепло- та холодопостачання. Геотермальне поле може мати різноманітні конфігурації: вертикальні грунтові зонди, горизонтальні колектори, енергетичні палі та інші грунтові теплообмінники. [9] Окрім того, геотермальна система може утилізувати тепло стічних вод чи скидне тепло промислових підприємств. Геотермальні системи також можуть будуватись з використанням технології «льодяний бак», яка використовує тепло фазового переходу, що утворюється внаслідок кристалізації води, тобто при її замерзанні. [10]

Всі доступні для теплового насосу джерела енергії поєднуються «холодною тепломережею», яка доправляє низькопотенційне тепло до місця встановлення теплонасосного обладнання. Завдання «холодної тепломережі»перенести необхідну для опалення енергію від джерела тепла до споживача. Але, якщо в класичній системі централізованого опалення використовується вода з температурою від 50°С до іноді більше 100°С, то в альтернативній «холодній» теплотрасі циркулює теплоносій (незамерзаюча гліколева суміш) з температурою від -5 до +20 °С. Перевага такого рішення полягає в тому, що можна бійтися без ізоляції трубопроводів і додатково поглинати енергію землі, адже температура ґрунту, як правило, вища ніж сам теплоносій. [11]

При проектування центрального теплопостачання та охолодження, для декількох багатоквартирних будинків, котеджного містечка, житлового кварталу чи міського району, доцільно застосувати систему з спільним геотермальним полем та локально встановленими тепловими насосами. Таке рішення дасть змогу оптимізувати потужність геотермальної системи та зменшити капітальні затрати. «Холодні тепломережі» міст можуть складатись з десятків чи сотень локальних мережевих кілець (квартальних, районних

«холодних тепломереж»), до яких приєднані теплові насоси, що обігрівають окремі будинки чи групи будівель.

Важливим елементом ефективної роботи таких систем з тепловими насосами має стати розумне керування та диспетчеризація. Практично всі теплові насоси мають функцію SG Ready, яка дозволяє електрогенеруючій компанії віддалено активувати чи вимикати пристрій. [12] Якщо в електромережі з'являється надлишок електроенергії, викликаний, наприклад - високою вітровою чи сонячною генерацією, тепловий насос, завдяки активації функції SG Ready, починає працювати за однією з встановлених стратегій, наприклад - нагрівати буфер чи бойлер до вищої температури. І навпаки, у випадку дефіциту електроенергії, теплонасосні установки можуть перейти на нижче споживання, або взагалі вимикатися, щоб недопустити перевантаження електромережі. Таким чином, системи з тепловими насосами можуть приймати участь в загальному балансуванні електроенергетичної системи.

В процесі модернізації з використанням теплових насосів доцільно провести оснащення будівель фотоелектричними панелями, згенерована електроенергія яких буде використовуватись для покриття роботи теплових насосів. В літній період це дасть змогу досягати періодів повністю автономної роботи з нульовими витратами. Відповідне програмне забезпечення контролера теплового насосу буде синхронізовано з роботою фотоелектричної установки та зможе оптимізовувати нагрів системи виходячи не лише з поточних даних сонячної електрогенерації, але і планувати завчасно, відстежуючи, наприклад: прогноз погоди. [13]

З однієї сторони мова йде про децентралізацію теплопостачання, а з іншої - всі теплові насоси стануть частиною загальної централізованої енергетичної системи. Теплові насоси можуть гнучко реагувати на стан електромережі, допомагаючи її балансуванню. Завдяки розумній мережі, тепловий насос зможе сам планувати свою роботу та самостійно вибирати яку електроенергію споживати: від власної фотоелектричної установки чи з загальної мережі, а можливо придбати необхідні кіловати в іншого власника сонячної установки чи вітрогенератора. Об'єднання на рівні програмного забезпечення та цифрових мереж допоможе забезпечити диспетчеризацію та оперативну сервісну підтримку.

[1] Стан та шляхи розвитку систем централізованого теплостачання в Україні. І. М. Карп, Є. Є. Нікітін, К. Є. П'яних, О. І. Сігал, С. В. Дубовський, Г. Г. Гелетуха, М. В. Тарновський, О. В. Дутка, В. І. Зубенко, І. С. Комков, Є. М. Олійник, Д. Ю. Падерно, К. К. П'яних, О. Е. Силакін, М. В. Степанов, В. М. Федоренко видавництво "Наукова думка" | Національна академія наук України, Інститут газу, Інститут технічної теплофізики. Книга 1 (2020):.С. 9–31.

[2] GreenHP, "GreenHP – Next Generation Heat Pump for Retrofitting Buildings", European funded project under FP7 (GA 308816), 2012 – 2016, https://cordis.europa.eu/project/id/ 308816 (coordinated by AIT), 2016

[3] Сайт Європейської комісії [Електронний ресурс]. Режим доступу: https:// commission.europa.eu/index_en

[4] Heat Pump Systems with Low GWP Refrigerants Task 2: Design guidelines for optimization of components and systems of Low GWP heat pumps . M. Verdnik, R. Rieberer Ch. Köfinger, T. Natiesta, F. Zach. Country Report Austria. Graz University of Technology

[5] Heat Pumps in Multi-Family Buildings. Task 3.1: Optimized refrigeration cycle configuration for Air-Water Heat Pumps for renovated, unrenovated and new MFH A. Zottl, M. Lauermann, S. Zibuschka. Austrian Institute of Technology. 2021

[6] Dynamic modeling and model-free real-time optimization for cold climate heat pumps systems. Dissertation. Wenyi Wang. The University of Texas at Dallas. December 2019

[7] EN 14825, "Air conditioners, liquid chilling packages and heat pumps, with electrically driven compressors, for space heating and cooling - Testing and rating at part load conditions and calculation of seasonal performance", EN standard, 2018

[8] Ground-source heat pumps systems and applications. Abdeen Mustafa Omer. Renewable and Sustainable Energy Reviews Volume 12, Issue 2, February 2008

[9] ДСТУ Б В.2.5-44:2010 Проектування систем опалення будівель з тепловими насосами. Київ Мінрегіонбуд України 2010

[10] Wärmepumpen Planung | optimierung | betrieb | Wartung. Herausgeber: Bundesamt für Energie,Dienst Aus- und Weiterbildung Autoren: Ralf Dott (Gesamtkoordination), Andreas Genkinger, Rita Kobler, Prof. Dr. Zoran Alimpic, Peter Hubacher, Prof. Dr. Thomas Afjei Basierend auf Ausgabe 2008

[11] Сайт Європейської асоціації теплових насосів [Електронний ресурс]. Режим доступу: https://www.ehpa.org/

[12] Flexibility of heat pump pools: The use of SG-Ready from an aggregator's perspective. David Fischera,b*, Tobias Wolfa, Marc-André Triebel. Fraunhofer Institute for Solar Energy Systems. 12 IEA Heat Pump Conference 2017

[13] D. Fischer and H. Madani, "On heat pumps in smart grids: A review," Renew Sustain. Energy Rev., vol. under re, 2016.

В.О. Верпета, А.О. Запорожець

ПЕРЕВАГИ ПРОГНОЗУВАННЯ ШВИДКОСТІ ВІТРУ НА ОСНОВІ ГІБРИДНИХ ПІДХОДІВ

Прогнозування швидкості вітру є ключовим елементом для ефективного функціонування вітрових електростанцій. Далі розглядаються чотири основні методи прогнозування: фізичні моделі, моделі просторової кореляції, традиційні статистичні моделі та штучний інтелект (ШІ), а також нові моделі [1].

Фізичні моделі базуються на знаннях фізичних процесів, які впливають на швидкість вітру. Ці моделі використовують рівняння руху повітря, термодинаміки та інших фізичних принципів. Вони можуть мати досить високу точність, але вимагають значного обчислювального ресурсу та даних.

Моделі просторової кореляції враховують просторові взаємозв'язки між різними точками на земній поверхні. Вони використовують географічні та топографічні дані для прогнозування.

Традиційні статистичні моделі використовують статистичні методи, такі як регресія та аналіз часових рядів. Вони базуються на використанні ретроспективних даних.

Моделі на основі штучного інтелекту використовують алгоритми машинного навчання та глибокого навчання для аналізу та прогнозування швидкості вітру. Ці моделі можуть автоматично адаптуватися до змін у вхідних даних та підвищувати точність прогнозів.

Останнім часом спостерігається значний ріст уваги до гібридних підходів у прогнозуванні об’ємів вироблення вітрової та сонячної енергії [2]. Цей тренд пояснюється декількома ключовими факторами, які роблять гібридні підходи привабливими для дослідників та інженерів.

Гібридні підходи дозволяють об'єднати переваги різних підходів до прогнозування:

- мають вищий рівень адаптивності до змін у вхідних даних чи умов. Це дозволяє їм більш ефективно прогнозувати вироблення електроенергії в умовах змінного середовища;
- допомагають мінімізувати вплив помилок, які можуть виникнути при використанні лише одного методу. Комбінування різних моделей дозволяє згладжувати можливі неточності та підвищувати загальну точність прогнозів;
- здатні інтегрувати різноманітні джерела даних, такі як метеорологічні дані, технічні параметри обладнання, географічні та топографічні характеристики, що робить їх відмінним інструментом для врахування комплексності умов;
- підвищують надійність та ефективність прогнозів, особливо в умовах мінливих погодних умов чи експлуатаційних умов електростанцій.

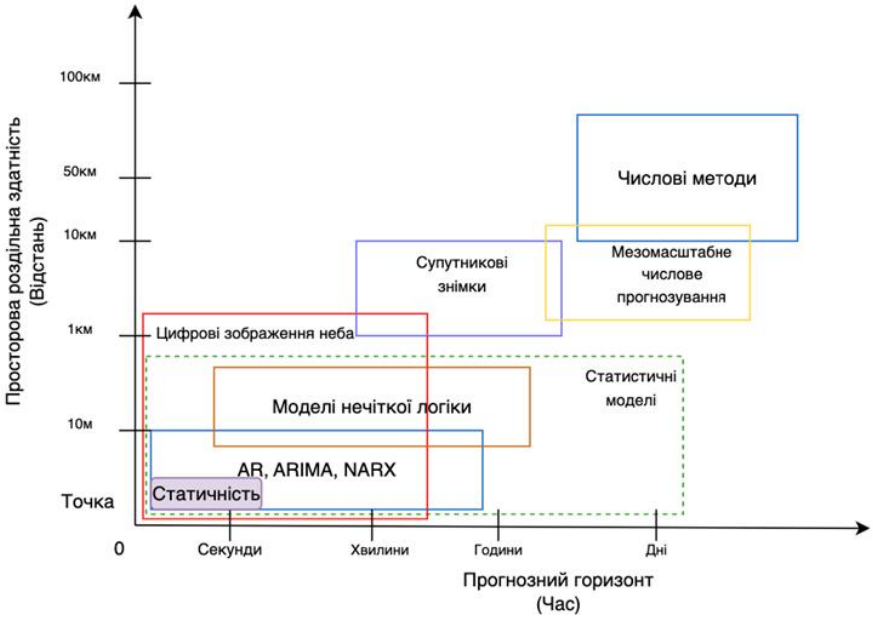


Рис. 1. Класифікація методів прогнозування швидкості вітру на основі просторової та часової роздільної здатності

Сучасна тенденція до використання гібридних підходів, які комбінують переваги різних методів, свідчить про стратегічний розвиток в галузі прогнозування об'ємів вироблення електроенергії від відновлювальних джерел енергії.

[1] Very Short-Term Wind Forecasting for Tasmanian Power Generation - https://www.researchgate.net/publication/3267567_Very_Short-Term_Wind_Forecasting_for_Tasmanian_Power_Generation

[2] Dolara, A.; Grimaccia, F.; Leva, S.; Mussetta, M.; Ogliari, E. A physical hybrid artificial neural network for short term forecasting of PV plant power output. Energies 2015, 8, 1138–1153.

Д.О. Євстаф'єв, А.О. Запорожець

ПЕРЕВАГИ ВИКОРИСТАННЯ УТЕПЛЮЮЧИХ МАТЕРІАЛІВ ІЗ ПЕРЕРОБЛЕНИХ ВІДХОДІВ ТЕКСТИЛЬНОГО ВИРОБНИЦТВА

Питання забруднення навколишнього середовища є одними із найголовніших викликів для людства у 21 столітті. Зростаючий попит на нові прогресивні будівельні матеріали вимагає розроблення сучасних екологічно чистих матеріалів. Використання перероблених матеріалів відповідає основним критеріям споживача – необхідні властивості та прийнятна ціна. Таким чином, основна задача матеріалознавства в будівництві є використання відновлюваних ресурсів сировини промислових відходів для розроблення нових конструкційних матеріалів [1].

Один із способів полягає в переробці відходів текстильної промисловості, що сприяє зниженню рівню забруднення навколишнього середовища і вторинному використанню текстильних матеріалів. В даний час одяг виготовляється із синтетичних волокон на основі пластику, і при процесі ткацтва виникає багато тканинних відходів. Переробляючи тканину на теплоізоляційний матеріал, споживачі цього продукту скорочують текстильні відходи у навколишнє середовище. До того, такий матеріал має великий потенціал до збільшення функціональності, щоб задовольнити різні вимоги для кінцевих продуктів.

Текстильні волокнисті вироби, що мають пористу структуру, можуть поглинати звукову енергію та використовуватися як хороші звукопоглинальні матеріали. До параметрів, що можуть впливати на рівень звукопоглинання, належать діаметр, довжина та щільність волокон. Текстильні волокна з високою щільністю можуть підвищити значення звукопоглинання в діапазоні середніх і високих частот. Більш товсті матеріали мають порівняно нижчу повітропроникність, але кращі властивості звукопоглинання. Неткана структура має високі звукопоглинальні властивості в діапазоні середніх і високих частот, проте має низькі звукопоглинальні властивості на нижчих частотах (100–400 Гц).

Передача тепла через волокнисті матеріали залежить від кількості волокон, геометрії упаковки, контакту між волокнами та різниці температур. Теплопередачу через теплопровідність і випромінювання можна зменшити шляхом збільшення товщини волокнистих вузлів. Більш товсті тканини при однаковій площі захоплюють більшу кількість повітря, що зменшує теплопровідність. Більш товсті вузлові з'єднання створюють більш «звивистий» шлях, що зменшує тепловіддачу. Волокнисті ізоляційні матеріали, виготовлені за допомогою нетканих технологій, мають відносно невеликі пустоти із захопленим повітрям, що надійно запобігає конвективному теплообміну. Використання декількох шарів волокнистих матеріалів збільшує кількість повітряних шарів та відповідно товщину без

додавання пропорційної ваги, що підвищує теплоізоляційні властивості цих матеріалів [2].

Оскільки теплоізоляційні властивості матеріалів залежать від їх пористості і звивистості (співвідношення довжини відкритих пор і товщини), текстильні матеріали, що мають велику частку взаємопов'язаних пустот, мають потенціал бути сировиною для виробництва теплоізоляційних матеріалів.

Таким чином, можна зробити висновок, що використання текстильних матеріалів як теплоізоляційних засобів має високий потенціал, та засвідчує про стратегічний розвиток у сфері енергоощадності та будівництва.

[1] Tilioua, A., Libessart, L., & Lassue, S. (2018). Characterization of the thermal properties of fibrous insulation materials made from recycled textile fibers for building applications: Theoretical and experimental analyses. Applied Thermal Engineering, 142, 56-67.

[2] Zdorenko, V., Zashchepkina, N., Barylko, S., Zaporozhets, A., Lisovets, S., & Kiva, I. (2023). Analysis of the Current State of Methods and Means for Monitoring the Technological Parameters of Textile Materials. In Manufacturing Control of Textile Materials: Operational Computerized Non-contact Methods (pp. 1-31). Cham: Springer Nature Switzerland.

Г.П. Костенко

ВИЗНАЧЕННЯ ТЕРМІНУ СЛУЖБИ ВТОРИННИХ БАТАРЕЙ ЕЛЕКТРОТРАНСПОРТУ В СИСТЕМАХ ЗБЕРІГАННЯ ЕНЕРГІЇ

Швидке зростання впровадження електромобілів у всьому світі призвело до значного зростання кількості акумуляторів, термін служби яких добігає кінця. В Україні ця тенденція підтримується зростаючою популярністю електромобілів, що зумовлює необхідність стратегічного підходу до управління батареями, подальша експлуатація яких в електромобілях більше не є енергетично та економічно доцільною. Літій-іонні батареї електромобілів, можуть бути перепрофільовані та повторно використані в системах зберігання енергії різного масштабу, що дає можливість Україні досягти своїх цілей сталого розвитку.

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

Незважаючи на певну невизначеність на ринку щодо частки акумуляторів, придатних для вторинного терміну служби, прогнози свідчать про те, що значна їх кількість може бути перепрофільована [1]. Це ставить перед Україною як виклики, так і можливості. З одного боку, необхідно налагодити ефективні процеси оцінки акумуляторів, їх переробки та інтеграції в нові системи. З іншого боку, це відкриває шляхи для створення нових моделей та систем різного масштабу – від побутових (домогосподарства) до комерційних та промислових систем зберігання енергії.

Динаміка розвитку парку електромобілів в Україні

За останні кілька років, відповідно до світових тенденцій, в Україні спостерігається щорічне збільшення парку електромобілів у десятки разів – з кількох одиниць у 2013 році до десятків тисяч одиниць у 2023 році [2]. Загальна динаміка зростання парку таких електромобілів в Україні (рис. 1) за останні 10 років. За прогнозами та державними програмами, до 2030 року автопарк електромобілів становитиме не менше 15% у всьому автопарку, близько 1,5 млн автомобілів [3]. Переважна більшість (близько 75-80%) електромобілів, що надходять на український ринок, є вживаними та мають середній термін служби 4-5 років. Це значно скорочує запас часу для повноцінного використання АКБ в електромобілі для виконання транспортної функції і підвищує актуальність розробки стратегій їх

подальшого використання. Деградація акумулятора зменшує запас ходу електромобіля, збільшує час заряджання, зменшує можливість регулювання.

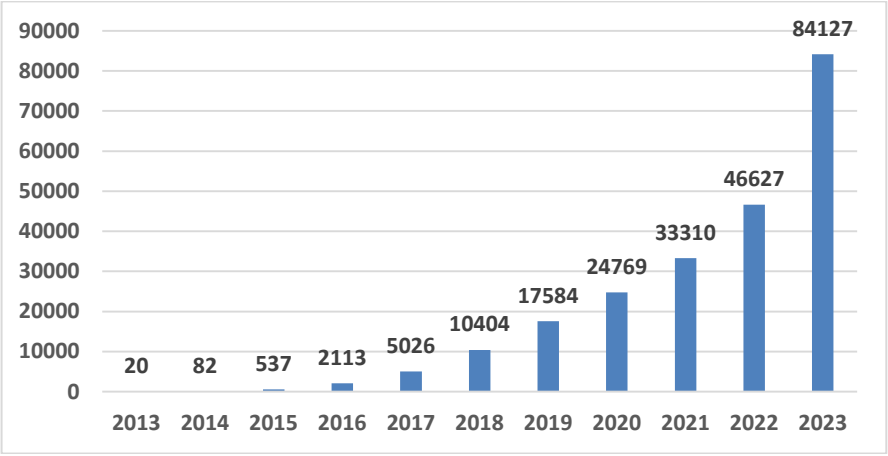


Рисунок 1 – Зростання парку електромобілів в Україні у 2013-2023 рр.

Можна передбачити, що така динаміка розвитку неминуче призведе до великої кількості деградованих акумуляторів вже до 2030 року (рис.2).

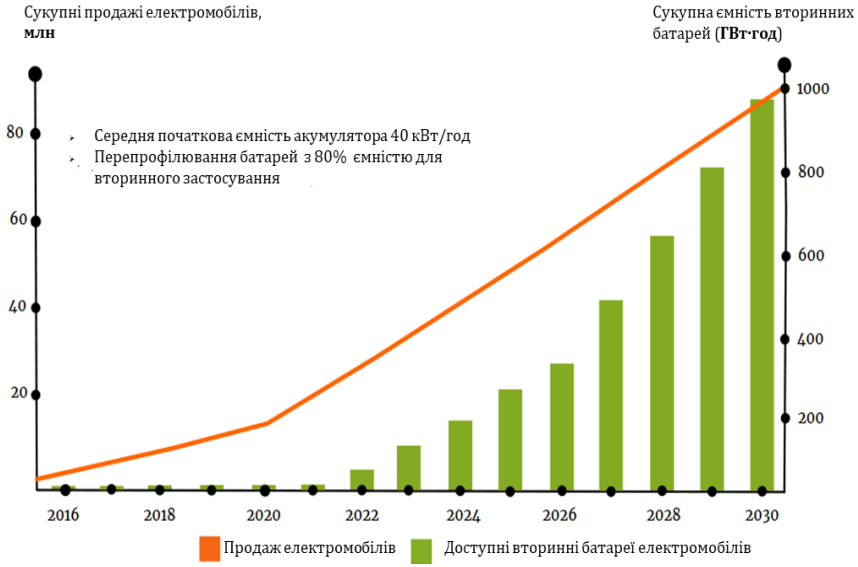


Рисунок 2 – Орієнтовний прогноз доступності вторинних акумуляторів електромобілів в Україні

Можна виділити кілька значних сегментів ринку для вторинного використання акумуляторів електромобілів у пристроях накопичення енергії, таких як домогосподарства, громадські/муніципальні/комерційні споживачі, підтримка ВДЕ-генерації, послуги з підтримки мережі, зарядні станції для електромобілів, тощо

Результати оцінки з урахуванням енергетичних характеристик та потреб споживачів представлені в табл. 1

Таблиця 1 - Оцінка потенційних ринків вторинного застосування батарей електромобілів в Україні

Сфера застосування	**Кількість батарей**	**Обсяг ринку**	**Потужність**	**Енергія**	**Час використання**	**Частота використання**
Домогосподарства	1–2	<250,000	1–10 кВт	5-10 кВт*год	3-4 год	Щоденно
Комунальні/ Громади	10–15	10,000 – 50,000	25–200 кВт	50–100 кВт*год	3-5 год	Щоденно
Офісні будівлі	30–40	<50,000	200–2000 кВт	100-1000 кВт*год	5 год	Щоденно
Торговельні центри	30–40	<100,000	200–250 кВт	500–1000 кВт*год	6-8 год	Щоденно
ВДЕ (ВЕС і СЕС)	500-700	<100	0.5–2.5 МВ	0.5–1 МВт*год	1–10 год	10–20/ міс.
Підтримка мережі	1000s	<10	1-100 МВ	1–10 МВт*год	5 сек-15 хв	5-10/ міс.
Станції заряджання електромобілів	10-50	<500	50-500 кВт	100-500 кВт*год	3-4 год	Щоденно

Щоб оцінити термін служби акумуляторів електромобілів для різних застосувань, необхідно враховувати кілька факторів, таких як очікувана ємність акумулятора після використання в транспортному засобі, частота циклів заряду/розряду, глибина розряду (DoD) та умови експлуатації, включаючи температуру, характер навантаження.

Другий термін служби батарей L пропонується розрахувати наступним чином:

$$\boldsymbol{L = \frac{C_r}{E_c} \times N_c \times D_r} \quad (1)$$

У цьому рівнянні

Cr - залишкова ємність акумулятора після його першого використання;

Ec - середнє споживання енергії за цикл;

Nc - число циклів в році,

Dr - очікуване скорочення ємності на рік.

Беручи за основу дані табл. 1, виконано розрахунки мінімального залишкового терміну служби батарей у різних типах вторинних застосувань, результати яких наведені у табл. 2.

Таблиця 2 - Термін служби вторинних батарей у різних застосуваннях, роки

Сфера застосування	**Термін служби, роки**
Домогосподарства	10
Комунальні/ Громади	7
Офісні будівлі	5
Торговельні центри	5
ВДЕ (ВЕС і СЕС)	7
Підтримка мережі	7…15
Станції заряджання електромобілів	4

Важливо зазначити, що ці оцінки залежать від багатьох змінних, включаючи точний спосіб використання акумулятора, умови заряджання та розряджання, температурні умови, якість керування акумулятором та інші фактори, які можуть вплинути на довговічність акумулятора. Системи керування батареями (BMS) можуть допомогти оптимізувати використання акумуляторів і продовжити термін їх служби. Тому слід зазначити, що оцінка проводилася для досить жорстких умов експлуатації вторинних додатків. Якщо умови експлуатації акумуляторів близькі до оптимальних, термін служби може бути продовжений на 50-75% .

[1] Костенко Г.П. Управління життєвим циклом батарей електротранспорту з урахуванням їх використання в енергетиці// Збірник матеріалів конференції "Енергетичний менеджмент: стан та перспективи розвитку – PEMS 2023", Листопад 22-24, 2023. – Київ, НТУУ КПІ ім.І.Сікорського, 2023. - 226 с. Url: http://pems.kpi.ua/proc/article/view/298526.

[2] Kostenko, G. (2022). Overview of european trends in electric vehicle implementation and the influence on the power system. System Research in Energy, (1 (70), 62-71. https://doi.org/10.15407/srenergy2022.01.062

[3] National Transport Strategy of Ukraine up to 2030. http://publications.chamber.ua/2017/Infrastructure/UDD/National_Transport_Strategy_2030.pdf

В.В. Оранський

ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ ТЕПЛОВИХ НАСОСІВ ЯК ОСНОВНОГО ДЖЕРЕЛА ДЛЯ ТЕПЛОПОСТАЧАННЯ ТА ГАРЯЧОГО ВОДОПОСТАЧАННЯ ДЛЯ ВЕЛИКИХ ОБ'ЄКТІВ

Сучасні теплові насоси мають ряд переваг:

1. Енергоефективність: Теплові насоси можуть забезпечити ефективне використання енергії, перетворюючи тепло з навколишнього середовища (наприклад, землі, води або повітря) у тепло для опалення та гарячої води. Це дозволяє значно зменшити витрати на енергію порівняно з традиційними системами опалення на основі вугілля або природного газу.

2. Низькі експлуатаційні витрати: Після встановлення теплового насосу, експлуатаційні витрати зазвичай нижчі, оскільки вони вимагають менше технічного обслуговування порівняно з традиційними опалювальними системами.

3. Екологічна чистота: Використання теплових насосів допомагає зменшити викиди парникових газів та інших забруднюючих речовин, оскільки вони використовують відновлювану енергію з навколишнього середовища.

4. Гнучкість в пристосуванні: Теплові насоси можуть бути встановлені як у нових будівлях, так і у вже існуючих спорудах, що робить їх привабливим варіантом для реконструкції або модернізації систем опалення.

5. Незалежність від палива: Використання теплових насосів дозволяє уникнути залежності від цін на традиційні джерела палива, такі як природний газ чи нафта, оскільки вони використовують енергію з навколишнього середовища, яка є нескінченною.

Усі ці переваги роблять теплові насоси привабливим варіантом для великих об'єктів, які потребують ефективного, економічного та екологічно чистого теплопостачання та гарячого водопостачання.

Сьогодні все більше проектів застосовують системи на основі теплових насосів для теплопостачання та охолодження будівель. Теплонасосне обладнання широко використовується як в приватному секторі, так і під час зведення комерційних та громадських будівель.Теплові насоси забезпечують мінімальне споживання енергії та гарантують нульові викиди CO_2. Суттєвою перевагою технології теплових насосів є те, що завдяки одному пристрою ми отримуємо три системи: опалення, охолодження та гаряче водопостачання. Хочемо познайомити вас з деякими варіантами використання теплових насосів для великих проектів: офісних центрів, лікарень, громадських будівель, торгово-розважальних центрів та житлових комплексів.

Приклад 1: Холодна тепломережа з індивідуальними тепловими насосами.

Застосування: Житлові квартали, котеджні містечка та багатоквартирні будинки.

Ідея: Концепція «холодної тепломережі» передбачає облаштування центрального геотермального поля. Теплоносій з низькою температурою 0 - 20°C транспортується до окремих домогосподарств за допомогою загальної мережі трубопроводів. Індивідуальні теплові насоси в кожному домі підвищують температуру до рівня, придатного для опалення будівлі. Гаряча вода також готується безпосередньо в кожному будинку. Плюс отримуємо централізовану систему пасивного охолодження. Таким чином усуваються тепловтрати при транспортуванні енергії. Центральна геотермальна система може поєднувати декілька джерел енергії: грунт, підземні води, стоки та енергію сонця.

Рішення: Геотермальні теплові насоси WATERKOTTE з функцією охолодження та приготування гарячої води, серій EcoTouch та Basic Line. Теплові насоси обладнано веб-інтерфейсом для створення системи дистанційного обслуговування WATERKOTTE RemoteCare. Комплексні геотермальні рішення від компанії Frank дозволять створити будь яку конфігурацію геотермального поля для теплових насосів.

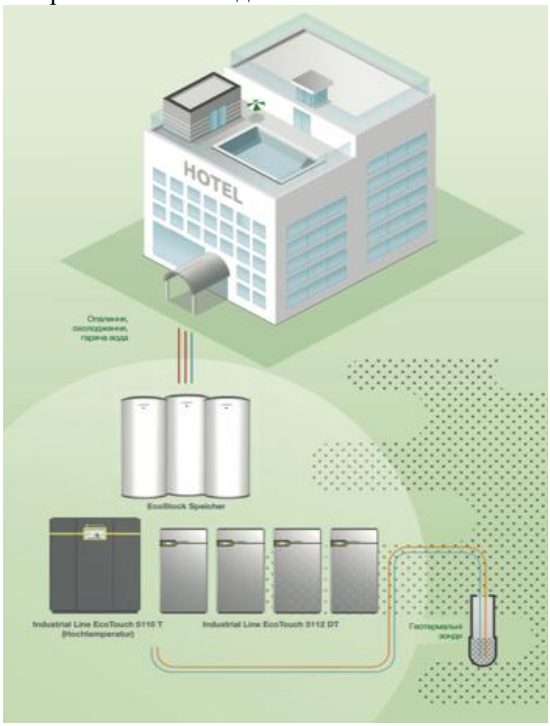


Рисунок 1- Централізоване теплопостачання та децентралізоване гаряче водопостачання Спа - готель

Приклад 2. Надійне опалення та охолодження

Застосування: СПА – готель

Ідея: Використання геотермальної енергії дає змогу отримати систему,

яка забезпечує опалення, охолодження та приготування гарячої води. Завдяки відповідному контролю та зручному регулюванню поєднуються максимальний комфорт та низькі експлуатаційні витрати.

Рішення: Потреби опалення та охолодження забезпечується завдяки центральному теплопункту з каскадом теплових насосів. У готелі є різні температурні зони. Окрім забезпечення готельних номерів, будівля може містити фітнес-зону, оздоровчий центр та басейн. Тому, на додаток до промислового насосу WATERKOTTE EcoTouch 5110T, який бере на себе приготування гарячої води, встановлюються чотири теплові насоси серії 5112DT для різних температурних режимів. У поєднанні з температурними датчиками в окремих функціональних зонах у будівлі, регулятор WATERKOTTE забезпечує правильний клімат у кожному приміщенні. Будівля з тепловими насосами відповідає найсучаснішим будівельним стандартам і забезпечує постійну економію ресурсів.

[1] Інформація та документація. ТОВ Сахара. https://caxapa.ua/pro-nas-statti-pryklady-zastosuvannia-teplovykh-nasosiv-dlia-velykykh-ob-yektiv

[2] Теплові насоси – ключова технологія енергомодернізації будинків. https://aosbb.kiev.ua/teplovi-nasosy-energomodernizatsiya-budynkiv

D.V. Ratush

DESIGN OF INTELLIGENT AGENT FOR PROTECTION SYSTEM AND OPERATING SYSTEM DIAGNOSTICS

The modern development of information technologies opens up numerous opportunities but also poses new challenges and threats to the security and efficiency of computer systems. One of the key tasks in this area is the creation of intelligent agents capable of providing a high level of protection and diagnostics for operating systems.

The process of developing software used to create such agents involves not only programming and maintaining the source code but also includes project planning, assessing its feasibility, analyzing business requirements, as well as testing and releasing the software product. This process also encompasses project management, personnel management, and other organizational functions.

Iterative software development methods significantly enhance the flexibility, efficiency, and adaptability of the process. These methods help implement parallel development and project adaptation according to new requirements and changes. Such an approach will be particularly beneficial in a project involving the development of comprehensive software for diagnosing and optimizing the performance of personal computers. This software will provide users with tools for system analysis, temporary file cleanup, system load monitoring, automatic driver and software updates, which are crucial for maintaining an optimal level of productivity and security. To represent the program's structure, UML class diagrams are used, allowing the identification of key classes and their interactions, facilitating a deep understanding and efficient development planning, especially in complex projects. This includes providing a convenient and clear visual representation of complex structures, promoting effective communication among developers, and helping identify potential issues at early stages of development. The use of Python together with class diagrams significantly contributes to reducing risks of errors in design, improving the quality of software products and ensuring greater flexibility and scalability in project implementation.

Designing an intelligent agent for the protection and diagnostics system of the operating system is a complex task that requires refined architecture and integration of various technologies. Using the Python programming language together with the Unified Modeling Language (UML) methodology can significantly contribute to the successful resolution of this task. Python, with its object-oriented approach and rich library, allows for the rapid implementation of various functional components of the system, while UML facilitates a clear definition of the structure and interactions between them. Figure 1 shows the class diagram of the system, illustrating its internal structure.

The prospects for further research in this field include the development of more complex machine learning models for predicting attacks, improving mechanisms for rapid incident response, and creating adaptive defense systems that

can autonomously adjust to changes in a dangerous environment. Another important direction is the integration of blockchain-based solutions to enhance transparency and data security in the network. These innovative approaches may unlock new opportunities for ensuring more effective and reliable protection of operating systems in the future.

Figure 1 - System Class Diagram

[1] Digitalization (Digitization) - what it is, essence, definition, why it is needed, and how it happens. [Online] - Available at: https://termin.in.ua/tsyfrovizatsiia-didzhytalizatsiia/

[2] Walker A. UML Class Diagram Tutorial: Abstract Class with Examples [Online] / Alissa Walker - Available at: https://www.guru99.com/uml-class-diagram.html

[3] Classes in Python. General Concepts. The keyword class. Class objects. Instance objects [Online] - Available at: https://www.bestprog.net/uk/2020/10/09/python-classes-in-python-general-concepts-class-objects-instance-objects-ua/

Д.П. Сінько

ПРОБЛЕМА РОЗДІЛЕННЯ МЕРЕЖІ В КОНТЕКСТІ РЕЗИЛЬЄНТНОСТІ КЛАСТЕРНИХ СИСТЕМ

Найбільш широке визначення резильєнтності полягає в тому, що це здатність реагувати, поглинати, адаптуватися, відновлюватися та реконфігуруватися під час руйнівної події [1[1]]. При визначенні резильєнтності розподілених комп'ютерних систем використовують такі характеристики як доступність, стійкість до відмов та стійкість в умовах відмов [2[2]].

Висока доступність, особливо в контексті розподілених кластерних систем, має вирішальне значення — користувачі не терпітимуть інформаційну систему, яка працює час від часу. Системи високої доступності гарантують, що бізнес-операції триватимуть із повною прозорістю для клієнтів і користувачів, коли система, програми та мережа виходять з ладу. Висока доступність є компонентом технологічної системи, яка нівелює одиничні збої, щоб забезпечити безперервну роботу або безвідмовну роботу протягом тривалого періоду. Високодоступні системи включають п’ять принципів проектування: автоматичне перемикання після збоїв, автоматичне виявлення та попередження збоїв на рівні застосунків, відсутність втрати даних, автоматичне та швидке перемикання на резервні компоненти, а також швидке відновлення після запланованого обслуговування. Однією з ключових задач забезпечення високої резільєнтності є попередження проблеми розділення мережі (network partition), яка призводить до розділення кластеру на ізольовані кластери-частини (Split-Brain) [3[3]], де кожен кластер, не знаючи про стан іншого, продовжує функціонувати незалежно. Таке розділення може призвести до неконсистентності даних, конфліктів і навіть системних збоїв. Розглянемо ключові аспекти проблеми Split-Brain:

Мережевий розділ - проблема Split-Brain зазвичай починається з мережевого розділу, де канали зв’язку між вузлами порушуються або значно сповільнюються. Це може статися через різні причини, зокрема збої мережі, проблеми з апаратним забезпеченням або неправильні налаштування (в тому числі через хакерські атаки або інсайдерські дії).

Ізольовані кластери - в результаті розділення мережі розподілена система поділяється на ізольовані кластери. У кожному кластері вузли все ще можуть спілкуватися один з одним, але вони відрізані від вузлів в інших кластерах. Ця ізоляція може бути тимчасовою або тривалою залежно від характеру основної проблеми.

Незалежне прийняття рішень - у сценарії Split-Brain вузли в кожному ізольованому кластері продовжують працювати незалежно, приймаючи рішення на основі даних, які їм доступні, особливо для мікросервісних архітектур, що побудовані за шаблоном “база даних на кожен сервіс” (database per service) [4[4]]. Однак їм бракує інформації про стан вузлів в

інших кластерах. Це може призвести до суперечливих рішень і неузгодженості даних.

Неузгодженість даних - коли вузли в різних кластерах здійснюють незалежні оновлення одних і тих же даних, це може призвести до неузгоджених або суперечливих даних. Наприклад, якщо розподілену базу даних розділено, один кластер може отримувати оновлення, тоді як інший кластер не знає про них.

Ризик системних збоїв - проблема Split-Brain створює значний ризик для загальної цілісності та надійності системи. Суперечливі рішення, прийняті на неконсистентних даних, можуть порушити роботу системи, а в деяких випадках призвести до катастрофічних збоїв та наслідків.

Стратегії вирішення - для вирішення проблеми Split-Brain розподілені системи використовують різні стратегії, включно з методами на основі кворуму та алгоритмами консенсусу. Ці механізми допомагають вузлам досягти згоди щодо стану системи та гарантують, що лише один кластер вузлів вважається авторитетним джерелом оновлень, тоді як інші синхронізуються відповідно. Але визначення з допомогою алгоритмів консенсусу певної частини кластеру з як довіреної вимагає часу, якого може не бути, так само як може не вистачити вузлів кластеру для кворуму. Розуміння цього змінює фокус з вирішення проблеми по факту на попередження виникнення проблеми.

Підсумовуючи ключові аспекти проблеми Split-Brain треба сказати, що проблема не є суто теоретичною. Вона може впливати на різні системи, включаючи розподілені бази даних, хмарні служби та кластери серверів. Вирішення цієї проблеми має важливе значення для забезпечення узгодженості даних та надійності системи, що в кінцевому рахунку має безпосередній вплив на резільєнтність кластерних систем. Як було показано, найбільш доцільним сценарієм вирішення проблеми розділення мережі в контексті резільєнтності кластерних систем є попередження таких проблем.

[1] Linkov I and Trump B D 2019 The Science and Practice of Resilience Risk, Systems and Decisions (Cham:Springer) ISBN 978-3-030-04565-4 URL https://doi.org/10.1007/978-3-030-04565-4

[2] Data centre facilities and infrastructures — Part 31: Key performance indicators for resilience (2023). Technical Specification ISO/IEC TS 22237-31. Informationtechnology — ISO/IEC.

[3] Java Code Geeks (2023). The Split-Brain Phenomenon: A Distributed Systems Dilemma. [online] Java Code Geeks. Available at: https://www.javacodegeeks.com/2023/10/the-split-brain-phenomenon-a-distributed-systems-dilemma.html [Accessed 2 May 2024].

[4] Microservices.io. Microservices Pattern: Database per service. [online] Available at: https://microservices.io/patterns/data/database-per-service.html [Accessed 2 May 2024].

Т.В. Пучко

МУРАШИНІ АЛГОРИТМИ В ЗАДАЧАХ ПЛАНУВАННЯ РОЗГОРТАННЯ ГЕНЕРУЮЧИХ ПОТУЖНОСТЕЙ ЕЛЕКТРОЕНЕРГЕТИЧНИХ СИСТЕМ

На сучасному етапі розвитку електроенергетики планування розгортання генеруючих потужностей вимагає нових інструментів для побудови моделей енергетичних систем. Це зумовлено значним зростанням частки виробництва електроенергії з використанням відновлюваних джерел енергії, таких як енергія сонця та вітру [1]. Таке зростання викликане вимогами щодо скорочення викидів діоксиду вуглецю, оксидів сірки та азоту, а також покращенням техніко-економічних показників технологій виробництва електроенергії з відновлюваних джерел енергії. Однак залежність таких джерел енергії від погодних умов не дозволяє визначати режими роботи генеруючого устаткування на тривалу перспективу та використовувати його в добовому регулюванні потужності в енергосистемі. Це значно ускладнює планування розгортання генеруючих потужностей з використанням відновлюваних джерел енергії.

Задачу планування розгортання генеруючих потужностей локальної енергетичної системи можна подати як задачу змішаного цілочисельного лінійного програмування з мінімізацією суми інвестиційних та операційних витрат, де цілочисловими змінними виступають кількість однотипних сонячних і вітрових модулів генерації та модулів акумулювання електроенергії. Ця задача має велику розмірність, бо включає моделювання режимів навантаження устаткування за різних погодних умов. Для зменшення розмірності задачі використовується кластеризація, що дає можливість зменшити кількість характерних графіків виробництва електроенергії. Але кількість таких прогнозних періодів має бути достатньо великою для забезпечення адекватності побудованої моделі [1].

Для розв’язування задач змішаного цілочисельного лінійного програмування великої розмірності можна використовувати як детерміновані методи, так і обчислювальні алгоритми природного походження. Перевагою детермінованих методів, таких, як декомпозиція Бендерса, є те, що більшість із них гарантують глобальну оптимальність. А їхнім недоліком є високі вимоги до часу обчислення та системних ресурсів. Також, багато з них вимагають явного формулювання математичної задачі у потрібній формі. Обчислювальні алгоритми природного походження не гарантують знаходження глобального оптимуму, але часто працюють швидше та не потребують математичного формулювання задачі, а можуть розглядати цільову функцію як “чорну скриньку” [2]. До таких алгоритмів належать мурашині алгоритми.

Біологічні мурахи, шукаючи їжу, спершу рухаються випадковим чином, але, знайшовши її, повертаються до мурашника, залишаючи сліди з

феромонів. Ці сліди приваблюють інших мурах. Коротші шляхи вимагають меншого часу на подорож, тому на них накопичується більше феромонів, тоді як феромони на довших шляхах з часом випаровуються, але рідше оновлюються. В результаті мурахи знаходять оптимальний шлях до їжі.

Використати аналогічний підхід для математичної оптимізації вперше запропонував Marco Dorigo [3]. Спочатку цей метод застосовувався лише для задач комбінаторної оптимізації, таких, як задача комівояжера [4], а пізніше був поширений на задачі з неперервними [5] та цілочисловими змінними [2]. Суть методу полягає в послідовній побудові ймовірних розв'язків задачі, причому ймовірність вибору певного складника розв'язку залежить від феромонового сліду та додаткової евристичної інформації [6]. Коли певну кількість потенційних розв'язків побудовано, для них обчислюється значення цільової функції. Потім кількість феромонів пропорційно зменшується для усіх можливих складників розв'язків та одночасно збільшується для складників найбільш перспективних розв'язків, залежно від обчисленого значення цільової функції. Потім усе повторюється, аж поки не знайдено прийнятний розв'язок або не вичерпано заданий час.

Щоб оцінити ефективність мурашиного алгоритму в задачах планування розгортання генеруючих потужностей електроенергетичних систем, було проведено порівняння ефективності розв'язання такої задачі двома способами. Спершу було сформульовано єдину модель задачі і виміряно час пошуку розв'язку за допомогою ПЗ SCIP [7]. Потім задачу було розділено на головну, яка знаходить оптимальну кількість сонячних, вітрових, та акумуляторних модулів, та допоміжну, яка, для заданої кількості модулів та погодних умов, визначає режими навантаження устаткування та операційні витрати. Для головної задачі було використано ПЗ MIDACO [8], що застосовує мурашиний алгоритм, а для допоміжної - ПЗ SCIP.

В процесі роботи мурашиний алгоритм потребує обчислення значення цільової функції операційних витрат для певної кількості модулів генерації та акумулювання електроенергії. Для цього необхідно розв'язати певну кількість допоміжних задач для різних погодних умов і отримати єдине значення цільової функції відповідно до вагових коефіцієнтів. Оскільки ці задачі не залежать одна від одної, вони розв'язувалися паралельно, що дало змогу прискорити отримання результату. Умовою завершення роботи основного алгоритму було досягнення значення цільової функції, визначеного раніше за допомогою єдиної моделі для SCIP.

В результаті експериментів було виявлено, що для невеликої кількості прогнозних періодів, що відповідають різним погодним умовам, пошук оптимальної кількості устаткування здійснюється швидше за допомогою єдиної моделі, а при збільшенні кількості прогнозних періодів час обчислення єдиної моделі зростає значно швидше, ніж час обчислення розділеної задачі. Тому для більшої кількості прогнозних періодів використання мурашиного алгоритму має перевагу з точки зору швидкості отримання прийнятного результату.

Отже, задача планування розгортання генеруючих потужностей

електроенергетичних систем з використанням енергії сонця та вітру є актуальною і може бути подана як задача змішаного цілочисельного лінійного програмування великої розмірності. Декомпозиція такої задачі і застосування мурашиного алгоритму до головної задачі дозволяють знаходити розв'язок швидше, ніж використання єдиної моделі, у випадках, коли є велика кількість прогнозних періодів для різних погодних умов. Необхідні подальші дослідження для оцінки ефективності детермінованих методів та інших обчислювальних алгоритмів природного походження у задачах планування розгортання генеруючих потужностей електроенергетичних систем.

[1] Saukh, S., & Borysenko, A. (2024). Cluster and Representative Models for Generation Units of Flexible Grids with Small Modular Reactors. Ядерна та радіаційна безпека, (1 (101)), 49-58.
[2] Schlüter, M., Egea, J. A., & Banga, J. R. (2009). Extended ant colony optimization for non-convex mixed integer nonlinear programming. Computers & Operations Research, 36(7), 2217-2229.
[3] Dorigo, M. (1992). Optimization, learning and natural algorithms. Ph. D. Thesis, Politecnico di Milano.
[4] Stützle, T., & Dorigo, M. (1999). ACO algorithms for the traveling salesman problem. Evolutionary algorithms in engineering and computer science, 4, 163-183.
[5] Socha, K., & Dorigo, M. (2008). Ant colony optimization for continuous domains. European journal of operational research, 185(3), 1155-1173.
[6] López-Ibáñez, M., Stützle, T., & Dorigo, M. (2015). Ant Colony Optimization: A Component-Wise Overview.
[7] SCIP Optimization Suite. About. https://www.scipopt.org/index.php#about
[8] MIDACO-SOLVER. About. http://midaco-solver.com/index.php/about

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

БІОТЕХНОЛОГІЧНІ ПІДХОДИ ПЕРЕРОБКИ ОРГАНІЧНИХ ВІДХОДІВ – ПЕРСПЕКТИВНИЙ РОЗВИТОК БІОЕНЕРГЕТИКИ В КРАЇНАХ ЄС ТА УКРАЇНІ

Енергетика перебуває у центрі уваги громадськості, політиків, підприємців багатьох країн, останнім часом з багатьох міркувань. Це і різкі коливання цін на енергоносії, і проблеми надійності поставок і, у ширшому розумінні, завдання забезпечення енергетичної безпеки країн, це використання нових джерел енергії, її економія та екологічні наслідки марнотратного поводження з енергоресурсами. Одним словом, енергетика увійшла до життя кожного з нас і стала важливою складовою міжнародного життя. З цих причин, енергетична політика становить особливий інтерес для дослідження. Від того, наскільки країни та міжнародні організації успішно вирішать поточні проблеми забезпечення економічного розвитку надійним та екологічним енергетичним «підживленням», без перебільшення, багато в чому залежить як майбутнє цих країн та організацій, так і майбутнє людства в цілому. Енергетична політика ЄС – явище багатовимірне. Вона може бути представлена у різних аспектах. Відновлювану енергію одержують із стійких джерел, таких як сонячна енергія, гідроенергія, енергія вітру, геотермальна енергія, біомаса та енергія припливів та відливів. Біомаса може безпосередньо використовуватися для виробництва електроенергії або тепла, або може використовуватися для виробництва газоподібного або рідкого біопалива (наприклад біодизеля і біоетанола), твердого палива.

Біомаса для отримання енергії (біоенергія) продовжує залишатися основним джерелом відновлюваної енергії в ЄС, частка якої становить майже 60% - для виробництва газоподібного або рідкого біопалива (наприклад біодизеля і біоетанола) [1, 2], твердого палива. Враховуючи те, що Україна є членом енергетичного союзу, ми маємо розвиватися у напрямку збільшення використання відновлювальних джерел енергії. В такому випадку біометан може зіграти важливу роль у досягненні цілей плану REPowerEU щодо диверсифікованих поставок газу та зменшення залежності ЄС та України від російського викопного палива.З цією метою видобуток має досягти 35 млрд кубометрів на рік до 2030 року. Щоб досягти цієї амбітної цілі, Комісія представила в травні 2022 року робочий документ персоналу (Staff Working Document), який супроводжує план REPowerEU, що включає низку можливих заходів для розкриття потенціалу біогазу та біометану по всіх країнах ЄС.

Запропоновані дії спрямовані на підтримку виробництва стабільного та максимального потенційного обсягу біогазу для подальшої його модернізації до біометану та спрямування виробництва біометану з відходів і залишків, уникаючи використання харчової та кормової сировини, що призводить до проблем зі зміною землекористування. Ці дії можуть також створити передумови для стійкої модернізації та безпечного закачування біометану в

газову мережу.До 2024 року країни ЄС повинні окремо збирати органічні відходи, що дасть можливість розширити виробництво екологічно чистого біометану та створити можливості для отримання прибутку для фермерів і лісівників.

Прийняття Урядом Енергетичної стратегії України до 2035 року

«Безпека, енергоефективність, конкурентоспроможність» (далі – ЕСУ) було обумовлено нагальною потребою актуалізації головного енергетичного документа країни через його невідповідність реальному стану справ [3-5].

На законодавчому рівні, з метою закріплення нової моделі державної політики у сфері енергоефективності, було прийнято ЗУ «Про енергетичну ефективність» з поправками №1818-IX від 01.01.2023 [4]. Цей Закон визначає правові, економічні та організаційні засади відносин, що виникають у сфері забезпечення енергетичної ефективності під час виробництва, транспортування, передачі, розподілу, постачання та споживання енергії.

Також, для імплементації вимог Директиви 2012/27/EU від 25.10.2012 було прийнято «Розпорядження КМУ від 29.12.2021 № 1803-р "Про Національний план дій з енергоефективності на період до 2030 року».

Отже, Планом заходів з реалізації етапу «Реформування енергетичного сектору (до 2020 року)» Енергетичної стратегії України на період до 2035 року «Безпека, енергоефективність, конкурентоспроможність» передбачено виконання 186 заходів. Головними виконавцями зазначених заходів визначено: Міненерго, Мінрегіон, НКРЕКП, Міндовкілля, Фонд державного майна, Мінекономіки, МОН, Мінфін, Мінсоцполітики, ДАЗВ, Держрезерв, оператор газотранспортної системи України. Біоенергетика є єдиним джерелом відновлюваної енергії, здатним забезпечити три основні джерела енергії, необхідні як окремим особам, так і підприємствам:

— біотепло / охолодження;

— біоенергія;

— біопаливо.

Станом на 30.07.2021 завершено реалізацію 93 заходів Плану, у стадії виконання залишалося ще 93 заходи, з них, відповідно до інформації органів державної влади, виконання 14 заходів Плану втратило актуальність (рис.1).

Для цього в світі використовують біомасу – давно визнаний тренд, котрий дозволяє заміщувати використання дорогого газу, а також зменшувати обсяги викидів вуглекислого газу в атмосферу.

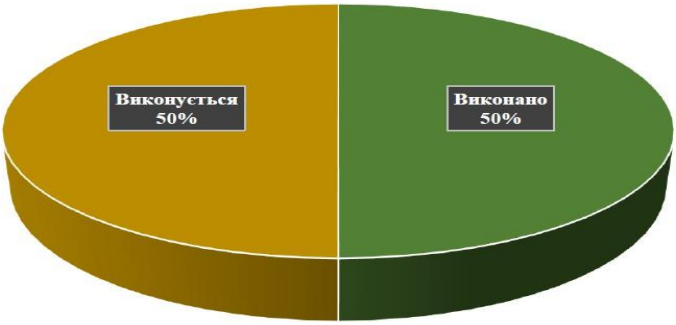


Рисунок 1 - Стан виконання заходів ЕСУ до 2035 року «Безпека, енергоефективність та конкурентоспроможність» [1]

Як паливо, біомаса посідає четверте місце у світі за обсягами виробництва і споживання енергії. Її частка у виробництві первинної енергії сягає 10%:

- біомаса - невикопна біологічно відновлювана речовина органічного походження, здатна до біологічного розкладу, у вигляді продуктів, відходів та залишків лісового та сільського господарства (рослинництва і тваринництва), рибного господарства і технологічно пов'язаних з ними галузей промисловості, а також складова промислових або побутових відходів, здатна до біологічного розкладу;
- біоетанол - спирт етиловий зневоджений, виготовлений з біомаси або спирту етилового-сирцю для використання як біопалива;
- біобутанол - спирт бутиловий, виготовлений з біомаси, що використовується як біопаливо або біокомпонент;
- біодизельне паливо (біодизель) - метилові та/або етилові етери вищих органічних кислот, отриманих з рослинних олій або тваринних жирів, що використовуються як біопаливо або біокомпонент;
- біогаз - газ, отриманий з біомаси, що використовується як паливо;
- біоводень - водень, отриманий з біомаси і є одним з видів біогазу; добавки на основі біоетанолу - біокомпоненти моторного палива, отримані шляхом синтезу із застосуванням біоетанолу або змішуванням біоетанолу з органічними сполуками та паливом, одержаними з вуглеводневої сировини, в яких вміст біоетанолу відповідає вимогам нормативних документів та які належать до біопалива;
- рідке паливо з біомаси - біопаливо дизельне, біоетанол, біобутанол, чиста олія та інші синтетичні палива, виготовлені з біомаси;
- синтетичні біопалива - синтетичні вуглеводні та суміші синтетичних вуглеводнів, виготовлені з біомаси [3].

Згідно з угодою про асоціацію з ЄС Україна має імплементувати

Рамкову Директиву Європейського парламенту та Ради 2008/98/ЄС від 19 листопада 2008 року про відходи.

Враховуючи актуальність даного питання, нині, одним із перспективних шляхів його вирішення - є застосування сучасних біотехнологій переробки органічних відходів із застосуванням специфічного консорціуму мікроорганізмів, які дозволяють в процесі біоконверсії органічних відходів, отримати дигестат та біоводень.

Дана робота проводилася в рамках міжнародного проекту “Clean Energy Technologies and Energy Efficiency: the EU Experience” (Project: 101047602 — EnergyC — ERASMUS-JMO-2021-HEI-TCH-RSCH) за програмою Еразмус+, Жан Моне.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Education and Culture Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

[1] Brief on biomass for energy in the EU. (2019-01-22). https://publications.jrc.ec.europa.eu/repository/handle/JRC109354

[2] The use of woody biomass for energy production in the EU (2021-01-25). https://publications.jrc.ec.europa.eu/repository/ handle/JRC122719

[3] Sustainable and optimal use of biomass for energy in the EU beyond 2020. (2017-10-05). https://energy.ec.europa.eu/sustainable-and- optimal-use-biomass-energy-eu-beyond-2020_en

[4] Рамкова програма клімату та енергетики до 2030. (2019-03-21). https://ec.europa.eu/clima/eu-action/climate-strategies-targets/2030- climate-energy-framework_en

[5] ЗУ «Про внесення змін до деяких законів України щодо удосконалення умов підтримки виробництва електричної енергії з альтернативних джерел енергії» № 810-IX63 від 21 липня 2020 року. (2020-07-21). https://zakon.rada.gov.ua/laws/show/810-20#Text

М.Л. Дранік

ТЕПЛОВИЙ НАСОС ТА СОНЯЧНІ ФОТОЕЛЕКТРИЧНІ ПАНЕЛІ. ПРИНЦИПИ СУМІСНОЇ РОБОТИ ТА ОСНОВНІ ПЕРЕВАГИ

1. Основні положення

Теплові насоси повітря-вода та сонячні фотоелектричні (PV) панелі є двома ефективними технологіями, які використовуються в сучасних будівлях для забезпечення енергоефективності та зменшення впливу на навколишнє середовище.

Основні принципи роботи теплового насосу повітря-вода полягають у використанні тепла з повітря як джерела енергії для нагрівання води, опалення будівлі та гарячого водопостачання. Насос використовує теплообмінник для збору тепла з повітря, яке потім конвертується в тепло, що використовується для потреб системи опалення та гарячого водопостачання. Основними перевагами теплових насосів є енергоефективність, низькі витрати на опалення та виробництво гарячої води, а також зменшення викидів CO_2.

Сонячні фотоелектричні (PV) панелі працюють на принципі перетворення сонячної енергії в електричну енергію за допомогою фотоелектричного ефекту. Коли сонячне світло падає на панелі, вони генерують постійний струм, який може бути використаний для живлення побутових приладів або подачі енергії до електричної мережі. Основними перевагами сонячних PV панелей є безкоштовне джерело енергії, зменшення залежності від комерційних джерел енергії та зменшення викидів CO_2.

Сумісна робота теплових насосів повітря-вода та сонячних PV панелей в приватному житловому будинку може бути організована через інтеграцію систем керування енергією. Наприклад, система керування може автоматично переключати споживання електроенергії між сонячними PV панелями та тепловими насосами в залежності від наявності сонячної енергії та потреб будинку. Це дозволяє оптимізувати використання відновлювальних джерел енергії та зменшити загальні витрати на енергопостачання.

Система, яка поєднує тепловий насос та сонячні панелі для оптимального використання енергії в приватному житловому будинку, може бути складною, але дуже ефективною. Основні складові такої системи:

1. Тепловий насос повітря-вода:
— Тепловий насос з вбудованим бойлером для нагрівання гарячої води.
— Система контролю та автоматизації для оптимального регулювання роботи насосу в залежності від потреб опалення та гарячого водопостачання.
2. Сонячні фотоелектричні (PV) панелі:
— Фотоелектричні панелі з інвертором для перетворення сонячної енергії в електричну енергію.

— Система моніторингу та управління для відстеження виробленої енергії та її розподілу.

3. Батареї або сховище енергії:

— Акумулятори або інші засоби для зберігання зайвої енергії, виробленої сонячними панелями, для використання в періоди низької сонячної активності.

4. Система керування та моніторингу:

— Центральна система керування для координації роботи теплового насосу, сонячних панелей та сховища енергії.

— Датчики для вимірювання температури, вологості та інших параметрів, необхідних для оптимальної роботи системи.

5. Додаткове обладнання:

— Трубопроводи та радіатори для системи опалення.

— Гаряче водопостачання і водонагрівачі для побутового використання.

2. Принцип сумісної роботи

Сумісна робота теплового насосу та сонячних фотоелектричних (PV) систем може бути досить складним, але дуже ефективним способом забезпечення енергоефективності в будівлі. Основні процеси при сумісній роботі цих систем:

1. Збір сонячної енергії:

— Сонячні фотоелектричні (PV) панелі збирають сонячну енергію і перетворюють її на електричну енергію у вигляді постійного струму.

2. Використання сонячної енергії:

— Частина виробленої електроенергії може бути використана безпосередньо в будинку для живлення побутових приладів або освітлення.

— Залишкова електроенергія, яка не використовується негайно, може бути направлена до сховища енергії (батареї або інші засоби зберігання).

3. Сумісне використання з тепловим насосом:

— Якщо в будинку встановлений тепловий насос повітря-вода, електроенергія з сонячних панелей може використовуватися для живлення цього насосу.

— Тепловий насос використовує електроенергію для збору тепла з повітря та нагрівання води для опалення та гарячого водопостачання.

4. Система керування та моніторингу:

— Центральна система керування координує роботу сонячних панелей, теплового насосу та сховища енергії (якщо воно є) для оптимального використання енергії.

— Система моніторингу відстежує вироблену енергію, рівень заряду батарей (якщо вони використовуються) та ефективність роботи всієї системи.

5. Керування енергією:

— В залежності від наявності сонячної енергії, система керування може

автоматично визначати, чи використовувати електроенергію безпосередньо в будинку, чи надсилати її до сховища енергії для подальшого використання.

— У разі недостатку сонячної енергії, система може автоматично переключати споживання електроенергії на інші джерела, наприклад, з мережі електропостачання.

3. Основні переваги

Переваги для власника будинку при використанні такої системи включають:

— Зменшення витрат на електроенергію та опалення за рахунок використання безкоштовної сонячної енергії.

— Збільшення енергоефективності будинку та зменшення викидів CO_2.

— Незалежність від коливань цін на енергоносії.

— Можливість отримання фінансових стимулів чи субсидій за встановлення енергоефективних технологій.

— Підвищення вартості будинку через встановлення сучасних технологій енергоефективності.

[1] Енергетична ефективність парокомпресійних теплових насосів з електричним та когенераційним приводами [Електронний ресурс] / О. П. Остапенко, В. В. Лещенко, Р. О. Тіхоненко // Наукові праці ВНТУ. – 2014. – № 4. – Режим доступу до журн.: http://praci.vntu.edu.ua/index.php/praci/article/view/421/419.

[2] Mills, D. Boom-time for renewable energy in Europe // Solar Progress. – 2015. – Vol. 21, No 2. – p. 14-23.

[3] Степаненко В. А. Тепловые насосы: потенциал для снижения потребления электроэнергии в основных секторах экономики // Тепловые насосы. – 2015.

С.С. Шевченко

ПИТАННЯ БЕЗПЕКИ КОНТЕНТУ ТА ВИХІДНИХ МАТЕРІАЛІВ У ІНТЕРАКТИВНИХ НАВЧАЛЬНИХ СИСТЕМАХ

Під час практичного впровадження системи навчання у правовласників матеріалів, що використовуються для навчання, практично завжди виникає закономірне питання: як забезпечити використання цих матеріалів тільки за призначенням, тобто для навчання. Найчастіше ці матеріали являють собою вихідні дані, що використовуються для виготовлення устаткування: креслення, вихідні 3D-моделі чи CAD-геометрія.

У найпростішому варіанті реалізації систем навчання передбачається, що навчальні матеріали завантажуються на пристрій користувача і там вже з ними відбувається взаємодія: запускаються сценарії, відображаються 3D-моделі і т.ін. Зрозуміло, це відкриває перед недобросовісними експлуатантами таких систем можливості для отримання вихідних даних із навчальних матеріалів з метою використання їх у нелегітимних цілях: від реверсної інженерії обладнання до шахрайства зі сценаріями навчання.

Для повного чи часткового вирішення цих проблем можна застосувати кілька способів. Два з них передбачені в авторській системі навчання “Virtual Mechanics” і коротко описані у відповідному патенті [1].

Перший спосіб – найбільш надійний, але і найбільш ресурсовитратний. Він полягає в тому, щоб не передавати жодних вихідних даних на пристрій користувача, а лише відеопотік згенерованої візуалізації з тренажеру, відображаючи користувачеві на клієнтському пристрої відео з результатами його дій, а назад з клієнтського пристрою надсилаючи на тренажер інформацію про взаємодію користувача з пристроєм. [2] У цьому способі тренажер фізично знаходиться на сервері та виконує візуалізацію, клієнтський пристрій лише транслює результат його роботи користувачеві. Це відрізняється від класичного підходу, в якому тренажер завантажується з усіма навчальними матеріалами на пристрій користувача і там запускається та працює, виконуючи візуалізацію самостійно.

Цей підхід має як плюси, так і мінуси.

З плюсів слід зазначити гарантоване недопущення сторонніх осіб до вихідних матеріалів: всі матеріали залишаються на сервері, стороннім особам видається лише результат симуляції.

З мінусів особливо важливий той факт, що дані системи вимагають набагато більших ресурсів для реалізації: багаторазово зростає навантаження на сервери системи навчання, які змушені проводити візуалізацію та симуляцію на своїх потужностях та забезпечувати симуляції для всіх працюючих користувачів одночасно, тоді як у класичному варіанті навантаження покладається на клієнтський пристрій, який займається візуалізацією та симуляцією лише для свого користувача. Також при даному

підході ускладнюється практична реалізація інтерфейсу користувача: локально обробляти дії користувача при поточних інструментах розробки програмного забезпечення технічно набагато простіше, ніж ці дії зчитувати із взаємодії з відеопотоком та передавати їх на сервер для обробки.

Другий із аналізованих способів полягає у попередній підготовці вихідних матеріалів навчання з метою залишити тільки ту інформацію, яка важлива для конкретного навчального сценарію.

Цей спосіб є особливо важливим для авторів вихідних даних, таких як правовласники конструкторської документації конкретного обладнання. Автором цього дослідження було проведено низку інтерв'ю з такими правовласниками. Найчастіше правовласники відмовляються надати свої матеріали у вигляді вихідних креслень або CAD-моделей, розуміючи, що ці конфіденційні дані, що становлять їхню комерційну таємницю, будуть в повному обсязі завантажені в систему і будуть там, фактично, в сторонніх руках. У разі будь-якого форс-мажору ці дані можуть потрапити до третіх рук і компанія зазнає матеріальних збитків. Підсумком цих інтерв'ю став винахід цього способу.

Спосіб полягає в обробці вихідних матеріалів, відсікаючи будь-яку інформацію, яка не використовується в навчальному сценарії. Наприклад, якщо нутрощі якогось вузла не потрібні в даному сценарії, вони видаляються, залишається лише геометрія зовнішнього корпусу вузла, а сам вузол фактично перетворюється на чорну скриньку. Дані про допуски, точності розмірів також можуть бути видалені, самі розміри можуть бути заокруглені до найближчих значень. У більшості випадків ця інформація є надмірною для навчального сценарію, і її видалення з навчальних матеріалів виявляється достатнім, щоб отримати згоду правовласника на використання цих даних.

Зрозуміло, ці методи – не єдині, які можна застосувати для забезпечення безпеки вихідних матеріалів у системах навчання. За цим напрямком ведеться подальша дослідницька робота.

[1] Shevchenko S.S. Patent UA 149786 U, G09B 19/00, publ. 01.12.2021, Bull. No. 48
[2] TechSoft3D. How HOOPS Communicator can use server side Exchange processes. https://forum.techsoft3d.com/t/how-hoops-communicator-can-use-server-side-exchange-processes/1841

В.В. Шкарупило, О.А. Чемерис, В.В. Душеба

СТРАТИФІКОВАНИЙ ПІДХІД ДО ОПРАЦЮВАННЯ РЕЗИЛІЄНТНОСТІ У ГАЛУЗІ ЕНЕРГЕТИКИ

Результати попередньо проведеного аналізу у частині окреслення поточного стану енергетичного сектору України дають підстави вважати, що доцільним є зміщення акцентів від опрацювання аспектів стійкості у напрямі розвинення засад резилієнтності енергетики держави, ключовим ініціюючим фактором якого стало неспровоковане повномасштабне вторгнення держави-агресора [1]. Факт такого вторгнення можна класифікувати як HILP-подію (High-impact Low-probability), що обумовлює потребу у розробленні і застосуванні нетривіальних, у тому числі предметно-орієнтованих, комплексних підходів до її опрацювання. Варто при цьому зауважити, що вказаній події вже передували подібні за специфікою випадки, серед яких і масштабна за наслідками кібератака на енергосистему України, що мала місце у грудні 2015 р. За результатами цієї кібератаки від енергопостачання було відключено близько 225 тисяч споживачі [2]. Даний прецедент є вагомою підставою доцільності опрацювання резилієнтності енергетики на рівні кібернетичному. У свою чергу, у контексті співставних за масштабами впливу HILP-подій, але вже на рівні фізичному, доречним вбачається навести дані звіту, опублікованого організацією PAX, у кооперації із Центром інформаційної резилієнтності (Centre for Information Resilience), згідно яких лише за період від лютого по листопад 2022 р. близько 40% генеруючих і передавальних складових енергетичної інфраструктури України було фізично зруйновано або пошкоджено [3].

Отже, з урахуванням зауваженого вище, важливості набуває опрацювання резилієнтності і на рівні кібернетичному, і на рівні фізичному. Такий комплексний підхід обумовлює потребу розгляду енергетичної інфраструктури держави як кіберфізичної системи [4]. Рівень складності зазначеної системи спонукає необхідність слідування принципам системного підходу при цьому. У межах представленої праці зазначеного планується досягати, у тому числі, шляхом проведення стратифікації [5]. Цей крок виконується як з метою сприяння адекватності співставлення вже відомих напрацювань у частині забезпечення енергетичної резилієнтності, так і для формування підґрунтя для розроблення нового комплексного рішення, яке б базувалося на наступних основоположних засадах: розгляд енергетичної інфраструктури як кіберфізичної системи; слідування при цьому принципам системного підходу, чого планується досягати, у тому числі, шляхом стратифікації об’єкту дослідження.

Представлений підхід до опрацювання резилієнтності у галузі енергетики пропонується будувати з позиції охоплення наступних концептуальних площин:

1. Площина, на якій висвітлюється принцип дії окремого рішення,

напрямленого на забезпечення резилієнтності енергетичної інфраструктури. У даному контексті, за аналогією до класифікації, проведеної у відповідності до шаблонів проєктування, що рекомендовані до застосування при розробленні складних програмних систем [6], пропонується виокремлювати наступні класи зазначених рішень: такі, що реалізуються у формі відповідних політик та/або стратегій; рішення, що полягають у доопрацюванні та/або створенні нової архітектурної складової досліджуваної системи.

2. Площина, на якій застосовується стратифікація. Пропонується виокремлювати наступні ієрархічні рівні досліджуваної системи: міжнародна, національна та регіональна енергетичні інфраструктури.

3. Площина, на якій охоплюються основоположні складові названої інфраструктури як кіберфізичної системи: і фізичний, і кібернетичний рівні.

Подяки. Роботу проведено у відповідності до планів і вирішуваних задач проєкту W911NF-22-2-0153, а також НДР № 0120U102683 «Розроблення спеціалізованих комп'ютерних технологій моделювання та опрацювання оперативної інформації в задачах енергетики».

[1] Шкарупило, В. В., Душеба, В. В., & Тіменко, А. В. (2023). Огляд рівнів забезпечення резилієнтності у галузі енергетики. Survivability & Resilience – 2023: collection of materials of the international scientific and practical conference (P. 33–34), Kyiv, October 19, 2023, PIMEE of NAS of Ukraine. https://ipme.kiev.ua/konferencii/zhivuchist-ta-rezilyentnist-2023/

[2] Pricop, A.-I., Gavrilaş, M., Sălceanu, A., & Neagu, B.-C. (2023). Power systems resilience against cyber-attacks. A systematic analysis. Proc. 2023 10th International Conference on Modern Power Systems, MPS 2023, Cluj-Napoca, Romania, 21–23 June 2023. https://doi.org/10.1109/MPS58874.2023.10187420

[3] Nikolaieva, I., & Zwijnenburg, W. (2022). Risks and impacts from attacks on energy infrastructure in Ukraine, December 2022. PAX report. https://paxforpeace.nl/media/download/PAX_Ukraine_energy_infrastructure_FIN.pdf

[4] Shkarupylo, V. V., Kudermetov, R. K., & Polska, O. V. (2018). On the approaches to cyber-physical systems simulation. Advances in Cyber-Physical Systems (ACPS), 3(1), 51–54. https://doi.org/10.23939/acps2018.01.051

[5] Mesarovic, M. D., Macko, D., & Takahara, Y. (1970). Theory of hierarchical, multilevel, systems. Academic Press.

[6] Gamma, E., Helm R., Johnson R., & Vlissides, J. (1993). Design Patterns: Abstraction and Reuse of Object-Oriented Design. In Nierstrasz, O.M. (Eds.), ECOOP' 93 – Object-Oriented Programming. ECOOP 1993. Lecture Notes in Computer Science, 707 (P. 406–431). Springer. https://doi.org/10.1007/3-540-47910-4_21

О.В. Харченко

АЛГОРИТМИ ТА ПРОГРАМНІ ЗАСОБИ ПАРАЛЕЛЬНОГО МОДЕЛЮВАННЯ ЗАДАЧ ПЛАНУВАННЯ РОЗВИТКУ ЕЛЕКТРОЕНЕРГЕТИЧНИХ СИСТЕМ

Моделювання планування розвитку електроенергетичних систем є важливим напрямком наукових досліджень, особливо в умовах терористичних та військових загроз, спрямованих на цілеспрямоване руйнування електроенергетичної системи.

Задачі планування розвитку електроенергетичних систем є задачами математичного моделювання множини режимів навантаження енергетичного устаткування, визначених на тривалому прогнозному періоді часу. Такі задачі математичного моделювання є задачами змішаного цілочисельного лінійного програмування великої розмірності.

Розв’язування таких задач, потребує не тільки використання значних обчислювальних ресурсів і потужних солверів, а і досліджень у напрямку ефективності існуючих обчислювальних програмних засобів паралельного розв'язування задач змішаного цілочисельного лінійного програмування великої розмірності.

Наразі, під час дослідження ефективності розв’язування таких задач, проведено аналіз програмних засобів, зокрема, солвера SCIP та наявних в складі пакету програм SCIP Optimization Suite [1] засобів паралелізації розв’язку та обчислень, який спеціалізується на розв'язанні задач змішаного цілочисельного програмування і є відкритим програмним забезпеченням.

Ефективність використання солвера SCIP та UG [2] (високорівневе середовище для паралелізації розв’язку, також входить до складу пакетів SCIP Optimization Suite), оцінено на задачі планування розвитку електроенергетичних систем, сформульованій у вигляді математичній моделі навантаження енергоблоків АЕС та генеруючого устаткування з відновлювальними джерелами енергії [3].

Поточні результати досліджень показали, що паралелізація розв’язку (наявними засобами в складі пакету програм SCIP Optimization Suite) задачі планування розвитку електроенергетичних систем, на обчислювальних ресурсах з багатоядерною архітектурою не завжди підвищує його ефективність.

Отримані результати є проміжними і враховуючи актуальність задач, подальші дослідження спрямовані на розробку паралельних методів розв'язку задач змішаного цілочисельного лінійного програмування великої розмірності з використанням алгоритму декомпозиції Бендерса. Очікується, що запропоновані паралельні методи розв'язку задач змішаного цілочисельного лінійного програмування будуть імплементовані в паралельне моделююче середовище, для розв’язку задач планування розвитку електроенергетичних систем.

[1] Suresh Bolusani, Mathieu Besançon, Ksenia Bestuzheva, et al., “The SCIP Optimization Suite 9.0”, Optimization Online and as ZIB-Report 24-02-29, February 2024. https://nbn-resolving.org/urn:nbn:de:0297-zib-95528

[2] Yuji Shinano, Tobias Achterberg, Timo Berthold, at al., “ParaSCIP – a parallel extension of SCIP”, Competence in High Performance Computing 2010, pages 135–148, Springer, 2012. http://rd.springer.com/chapter/10.1007/978-3-642-24025-6_12

[3] Saukh, S., Borysenko A. (2024). Cluster and Representative Models for Generation Units of Flexible Grids with Small Modular Reactors. Nuclear and Radiation Safety, 1(101), 49-58. https://doi.org/10.32918/nrs.2024.1(101).05

O.A. Kravchuk

ADVANCING SWARM INTELLIGENCE: AI WITH UNMANNED VEHICLE SYSTEMS FOR ENHANCED AUTONOMY AND COORDINATION

Unmanned vehicle swarms function as self-organizing structures, formed by technological agents (drones), which communicate either directly or indirectly. These agents have the ability to adjust to environmental conditions or the requirements of specific tasks [1]. The local interactions between these agents result in complex swarm behavior, whose dynamics or functional properties are often not reducible to the behaviors or properties of the individual agents involved.

Key features of swarm systems include their rapid adaptability to environmental changes, the gradual system degradation when components fail, and their scalability, which enables effective load distribution among the agents to address complex, large-scale tasks [2].

Unmanned vehicle swarms are utilized across a broad spectrum of applications, ranging from search and rescue operations to military engagements and beyond [3–9]. Depending on the specific task and environment, the agents may be aerial (Unmanned Aerial Vehicle – UAV), terrestrial (Unmanned Ground Vehicle – UGV), underwater (Unmanned Underwater Vehicle – UUV), or aquatic (Unmanned Surface Vehicle – USV) unmanned vehicles. The integration of artificial intelligence (AI) with these unmanned systems significantly enhances their capabilities, enabling them to exhibit intelligent behavior, adapt to dynamic environments, and perform previously unachievable tasks [2].

While traditional AI technologies are essential for the advancement of unmanned vehicles, they come with challenges. These methods require substantial training data and perform optimally only under specific configurations. They are particularly susceptible to environmental dynamics and uncertainties, which are characteristic challenges for unmanned vehicles [3]. As such, in a swarm context, the coordination of numerous unmanned vehicles in dynamic environments presents significant challenges for traditional AI methods.

The application of AI in swarm systems can greatly enhance various aspects of their operation. Here are some tasks within swarm systems that AI can address:

Swarm Formation and Coordination. AI algorithms can ease the process of forming a swarm [2]. These algorithms enable the drones within a swarm to detect the positions and velocities of their neighbors, adjust their behavior accordingly, and maintain desired formations. The drones can dynamically alter their formation based on environmental conditions, task requirements, or changes in swarm composition.

Task Distribution and Optimization. AI algorithms can analyze factors such as the capabilities of agents, task requirements, energy consumption, and proximity to other agents to optimize task distribution among the drones. Through the use of genetic algorithms and reinforcement learning, these systems can

effectively distribute tasks, balance workloads, enhance overall performance [2].

Navigation and Trajectory Planning. Trajectory planning for swarm agents is a complex optimization task that involves multiple objectives and interdependencies. Its primary aim is to ensure optimal routing for unmanned vehicles in dynamic environments, avoiding obstacles and avoiding collisions [10]. Techniques like artificial potential fields, A-search algorithms, or probabilistic roadmap methods can facilitate collaborative navigation. Drones can share information on obstacles, environmental features, and preferred routes to efficiently plan and execute navigation strategies [2].

Communication and Information exchange. Effective communication and the exchange of information are crucial for the coordination and collaborative decision-making within a swarm. AI-driven communication protocols and algorithms enable swarm agents to share data, coordinate actions, and spread information throughout the swarm [2].

Decision-making and Adaptation. Swarm agents need to make informed decisions to adapt to changing environmental conditions and successfully carry out tasks. AI algorithms can process sensor data, assess various options, and make collective decisions based on pre-defined goals or rules. Techniques such as decentralized decision-making, machine learning-based decision models, or game theory can support intelligent decision-making processes among drones [2].

AI Algorithms. These tasks and others within the context of unmanned vehicle swarms are proposed to be addressed through a variety of artificial intelligence algorithms. Machine learning methods, including Deep Learning (DL) and Reinforced Learning (RL), are crucial to the development of swarm systems. These methods, which utilize extensive datasets, allow drones to learn from experience and incrementally improve their performance. Reinforcement learning algorithms enable drones to discover optimal strategies through interaction with their environment. Deep learning methods, such as convolutional neural networks or recurrent neural networks, are employed for tasks involving perception, object recognition, or anomaly detection, which enhance the drones' situational awareness and decision-making capabilities [2].

Federated Learning (FL) – a method of distributed learning [11, 12], enables a group of UAVs to develop a machine learning model using distributed data sets. During the federated learning process, swarm agents transmit parameters of their local models to a central server without sending raw data, ensuring data confidentiality and reducing the transfer of large data volumes over mobile networks, as well as conserving energy [10], [13–15].

Disadvantages of FL include the substantial load on communication resources when a large number of agents broadcast their local models [16]. Hardware disparities among agents, such as differences in battery life, network settings, and computational power, can lead to inconsistent participation in the learning process and potentially cause some agents to fall behind. It is challenging to ensure timely acceptance of all local models by the server for aggregation due to varying processing speeds and communication capabilities [16]. The data collected by agents are unevenly distributed, leading to potential inconsistencies in the models

[17].

Reinforcement Learning (RL) is a key method in Machine Learning (ML), primarily used for decision-making in dynamic environments through interactions with those environments. Generally, RL involves six elements: agent, environment, policy, action, reward, and value function. The agent acts and receives rewards through its interactions, and the process can be viewed as a game between the agent and its environment, akin to a game between state and action. The policy maps each state to actions, while the value function indicates the quality of a state, representing the total expected future rewards from that state. The objective of RL is to maximize the accumulation of rewards. Notable RL algorithms include Q-learning, Deep Q Network (DQN), and Deep Deterministic Policy Gradient (DDPG) [10].

In scenarios involving multiple agents, the complexities increase, leading to the use of multi-agent reinforcement learning (Multiagent Reinforced Learning – MARL), which is essentially a distributed form of RL that several agents can execute simultaneously [10].

Distributed Inference (DI) is a significant aspect of ML, involving initial training of a model based on available data followed by the application of new data to derive insights (regression or classification). Each agent develops its model based on individual observations to create a local solution. A central server is necessary to consolidate these individual outcomes into a final decision, referred to as distributed inference. This process is categorized into cooperative inference [10], model inference, and decision inference.

Split Learning (SL) is a distributed learning algorithm for a global educational network that operates without sharing raw data [19]. In SL, the ML model is divided into several sub-models, and the training of these sub-models is distributed among several clients and a server. Each client trains a sub-model for a specific layer and sends the segmented data to the server, which then trains the remaining layers. As the client only transmits intermediate output data during forward propagation and the server only sends the gradient during backward propagation, this setup preserves the confidentiality of the raw data [10].

Deep Learning and Neural Networks. Techniques such as Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) are extensively used in swarm systems. CNNs enable drones to perform tasks related to visual perception, including object recognition, localization, and tracking. RNNs, with their ability to remember temporal sequences, assist in decision-making and planning in dynamic settings. The combination of deep learning with reinforcement learning has also facilitated comprehensive training, where drones learn directly from unprocessed sensor data, promoting more efficient and autonomous behavior [2].

Generative Artificial Intelligence (GAI) marks a transformative shift in AI technology, characterized by its capacity to generate novel and significant content such as text, images, audio, and 3D models [3]. Unlike discriminative models, which focus on classification or prediction, GAI models can interpret instructions and generate entirely new outcomes, indicating a substantial advancement in AI

capabilities [20].

With its ability to synthesize absent information and amalgamate diverse data sources, GAI can be employed for an in-depth evaluation of the status of unmanned vehicle swarms.

The capability to perceive and interpret the surrounding environment in real-time is a pivotal technology for achieving autonomous navigation and task fulfillment in unmanned vehicle swarms [3]. This often involves using sensors like LiDARs, cameras, and millimeter-wave radars to interact with the external environment [22]. The field of environmental perception in unmanned vehicles has significantly progressed through various innovative applications of GAI, such as enhancing the quality of blurred or low-resolution images captured by UAVs under adverse weather conditions, among others [3], [23].

Another innovative approach is the Generative Knowledge-Supporter Transformer (GKST), which improves feature representation and search performance by integrating information from various image perspectives [24]. These technologies excel at processing and interpreting complex visual data, offering a level of contextual understanding that closely mirrors human perception [3].

Conclusions. Swarm system technology is undergoing rapid development and faces a host of complex challenges: agent formation and coordination, task and goal distribution among agents, agent trajectory planning and navigation, effective data sharing, decision-making, and adaptation. A significant leap forward in swarm system development is enabled by the explosive growth of artificial intelligence. However, the existing AI algorithms need further refinement and substantial enhancement, as they currently demand considerable computational and energy resources, which complicates their deployment in unmanned vehicle swarms.

[1] Beni, G., & Wang, J. Swarm intelligence in cellular robotic systems. In Robots and biological systems: Towards a new bionics? 1993. (pp. 703-712). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-58069- 7_38.

[2] Semwal A., Shikalgar S., Solanki D. R. The Use of Artificial Intelligence in Swarm Drones. International Journal for Research in Applied Science and Engineering Technology. 2023. Vol. 11, no. 7. P. 1052–1057. URL: https://doi.org/10.22214/ijraset.2023.54799.

[3] Generative AI for unmanned vehicle swarms: Challenges, applications and opportunities / G. Liu et al. ArXiv. Abs/2402.18062. URL: https://api.semanticscholar.org/CorpusID:268041856.

[4] Y. Tan, J. Wang, J. Liu, and Y. Zhang, “Unmanned systems security: Models, challenges, and future directions,” IEEE Network, vol. 34, no. 4, pp. 291–297, 2020.

[5] P. McEnroe, S. Wang, and M. Liyanage, “A survey on the convergence of edge computing and AI for UAVs: Opportunities and challenges,” IEEE Internet of Things Journal, vol. 9, no. 17, pp. 15 435–15 459, 2022.

[6] A. Ahmadzadeh, A. Jadbabaie, V. Kumar, and G. J. Pappas, “Multi- UAV cooperative surveillance with spatio- temporal specifications,” in Proceedings of the 45th IEEE Conference on Decision and Control, 2006, pp. 5293–5298.

[7] N. Nigam, S. Bieniawski, I. Kroo, and J. Vian, “Control of multiple UAVs for persistent surveillance: Algorithm and flight test results,” IEEE Transactions on

Control Systems Technology, vol. 20, no. 5, pp. 1236–1251, 2012.
[8] J. Scherer and B. Rinner, “Multi-UAV surveillance with minimum information idleness and latency constraints,” IEEE Robotics and Automation Letters, vol. 5, no. 3, pp. 4812–4819, 2020.
[9] R.-j. Yan, S. Pang, H.-b. Sun, and Y.-j. Pang, “Development and missions of unmanned surface vehicle,” Journal of Marine Science and Application, vol. 9, pp. 451–457, 2010.
[10] Distributed machine learning for UAV swarms: Computing, sensing, and semantics / Y. Ding et al. arXiv. 2023. ArXiv:2301.00912. URL: http://arxiv.org/abs/2301.00912.
[11] J. Konecˇny, H. B. McMahan, F. X. Yu, P. Richta´rik, A. T. Suresh, and D. Bacon, “Federated learning: Strategies for improving communication efficiency,” arXiv preprint arXiv:1610.05492, 2016.
[12] J. Konecˇny, H. B. McMahan, D. Ramage, and P. Richta´rik, “Federated optimization: Distributed machine learning for on-device intelligence,” arXiv preprint arXiv:1610.02527, 2016.
[13] Q. Yang, Y. Liu, T. Chen, and Y. Tong, “Federated machine learning: Concept and applications,” ACM Transactions on Intelligent Systems and Technology (TIST), vol. 10, no. 2, pp. 1–19, 2019.
[14] S. Niknam, H. S. Dhillon, and J. H. Reed, “Federated learning for wireless communications: Motivation, opportunities, and challenges,” IEEE Communications Magazine, vol. 58, no. 6, pp. 46–51, 2020.
[15] Z. Yang, M. Chen, K.-K. Wong, H. V. Poor, and S. Cui, “Federated learning for 6g: Applications, challenges, and opportunities,” Engineer- ing, 2021.
[16] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, “Federated learning: Challenges, methods, and future directions,” IEEE Signal Processing Magazine, vol. 37, no. 3, pp. 50–60, 2020.
[17] A. Fallah, A. Mokhtari, and A. Ozdaglar, “Personalized federated learn- ing with theoretical guarantees: A model-agnostic meta-learning ap- proach,” Advances in Neural Information Processing Systems, vol. 33, pp. 3557–3568, 2020.
[18] M. Chen, D. Gu¨nduˆz, K. Huang, W. Saad, M. Bennis, A. V. Feljan, and H. V. Poor, “Distributed learning in wireless networks: Recent progress and future challenges,” IEEE Journal on Selected Areas in Communications, 39(12), pp. 3579–3605, 2021
[19] O. Gupta and R. Raskar, “Distributed learning of deep neural network over multiple agents,” Journal of Network and Computer Applications, vol. 116, pp. 1–8, 2018.
[20] M. Byrne, “The disruptive impacts of next generation generative artificial intelligence,” CIN: Computers, Informatics, Nursing, 41(7), pp. 479–481, 2023.
[21] W. Zhang, F. Jiang, C.-F. Yang, Z.-P. Wang, and T.-J. Zhao, “Research on unmanned surface vehicles environment perception based on the fusion of vision and lidar,” IEEE Access, vol. 9, pp. 63 107–63 121, 2021.
[22] Z. Zhang and M. Fu, “Research on unmanned system environment per- ception system methodology,” in International Workshop on Advances in Civil Aviation Systems Development. Springer, 2023, pp. 219–233.
[23] Y. Shi, L. Han, L. Han, S. Chang, T. Hu, and D. Dancey, “A latent encoder coupled generative adversarial network (LE-GAN) for efficient hyperspectral image super-resolution,” IEEE Transactions on Geoscience and Remote Sensing, 60, 1–19, 2022.
[24] J. Zhao, Q. Zhai, P. Zhao, R. Huang, and H. Cheng, “Co-visual pattern-augmented generative transformer learning for automobile geo-localization,” Remote Sensing, vol. 15, no. 9, 2023. [Online]. Available: https://www.mdpi.com/2072-4292/15/9/2221

I.O. Dubovkina, A.O. Myronchuk

UNINTERRUPTED ENERGY SAVING MODE of WATER TREATMENT for GROWING CROPS

Using of energy saving technologies gives the possibilities to reduce the energy and recourses consumption of different production. Innovative technologies have been improved by the application of modern scientific knowledge. Modern agriculture throughout the world is aimed at growing food products. Present production is based on intensive technologies of growing plants.

Growing vegetable products in the open has a number of difficulties associated with complex agricultural technology, the impossibility of growing in difficult climatic conditions, as well as the impossibility of growing tomatoes, cucumbers, salads and spicy herbs in winter and in the off-season. But the market needs this product. Therefore, countries with developed agricultural production use a protected soil environment as the main means of production to meet the population's needs for vegetable products, which opens up wide opportunities for the production of fastidious vegetable crops. The feature of the food products depends of many factors. One of them is a quality characteristic of the raw material, because they are the foundation of finished food products. Thus, greenhouses and greenhouse complexes are gaining a lot of development, especially with climate changes observed in recent years. The list of crops that should be grown in a protected soil environment includes: tomatoes, cucumbers, peppers, radishes, salads, spicy greens, as well as various types of flower products [1]. It should be noted that each crop has its own characteristics of growth and vegetation, and therefore the cultivation technologies of these crops differ among themselves.

Growing plants on hydroponics is the most common technology, which involves the rejection (or partial rejection) of the soil as the main environment where the root mass of the plant develops [2].

Raw materials include: ingredients; processing aids; packaging materials. Fruits, vegetables, corns, herbs, grains, berries are the important components of the food raw materials. The first stage of the foodstuff production begins from the growing crops. That’s why many food industries depend almost entirely on agriculture and growing crops. Aquatic solutions were used for experimentation investigations. Aquatic solutions gave in to processing by physical influence before the technological process of production. Aqua treatment and obtaining process was spent in the condition of the physical influence. The analytical chemistry and chemical methods were used for the researches physical and chemical parameters of the aquatic solutions.There are different types of hydroponic systems. It is passive hydroponic systems without any powered equipment and apparatus and active hydroponic systems, which include automatic controllers, timers, measuring systems, mechanical pumps, engines etc. There are two types of hydroponic systems. It is passive (without any mechanical equipment) and active systems,

which includes pumps, timers and automatic complexes.

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

The effects of analytical computation and mathematical modeling, statistical experiment have given the possibility to calculate basic design data of devices which influence on intensification of carrying out of obtaining processes for aquatic mediums, and also processing for the purpose of change of physical and chemical parameters and structural transformations. The research studies demonstrated the increasing of the pH of the water prepared for the technology on the 15%.

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

The potential of hydrogen can greatly verify the velocity of itinerary of chemical reactions. Throughout processing of aquatic solutions and obtaining process in the conditions of linear speeds of the first rotor is 21,5 m/s and the second rotor is 23,5 m/s. The pressure of shift of a stream for the first rotor is 215 Pa and for the second rotor is 235 Pa. The speeds of shift of a stream for the first rotor is $2{,}0 \times 10^5\ s^{-1}$ and for the second rotor is $2{,}5 \times 10^5\ s^{-1}$. The speed of rotary motion of the rotors is $n = 50\ sec^{-1}$. Through researches the potential of hydrogen of the aquatic solutions prepared on standard technology has raised on 15%. Employment the method of physical influence in technology of receiving of mediums allows receiving the activated aquatic solutions with the certain physical properties and parameters, assured value of a potential of hydrogen.

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

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

[1] Elvira Molin, Michael Martin (2018). Assessing the energy and environmental performance of vertical hydroponic farming, IVL Swedish Environmental Research Institute 2018, №. C 299, p.36

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

Р.І. Драгунцов

ОСОБЛИВОСТІ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ З ЗАЛУЧЕННЯМ ШКІДЛИВОГО ПЗ В УМОВАХ КІБЕРВІЙНИ – АНАЛІЗ ТА РЕАГУВАННЯ

Огляд. В умовах зростаючої глобалізації інформаційних технологій та посилення кібернетичних загроз, в контексті військових конфліктів, атаки у кіберпросторі стають невід'ємним аспектом стратегічних військових дій. Зокрема, шкідливе програмне забезпечення (ШПЗ), використовуване під час російсько-української війни, інструментується для проникнення, закріплення, та просування в інформаційних системах противника. Дані інструменти використовуються, в першу чергу, для проникнення в інформаційну систему.

Для доставки шкідливого ПЗ активно використовуються складені вектори атак. Соціальна інженерія дозволяє атакуючому маніпулювати користувачами для отримання необхідних даних або доступів, тоді як експлуатація вразливостей забезпечує технічне проникнення через існуючі слабкі місця в захисті систем. Це поєднання забезпечує високу ефективність кібератак та ускладнює процес їх виявлення та нейтралізації а також зумовлює ефективність застосування ШПЗ.

Отримує актуальність питання створення та імплементації концепцій для оперативного реагування та завчасного виявлення інцидентів кібербезпеки з використанням таких інструментів. Основними компонентами таких систем є інтеграція технологій для моніторингу, раннього виявлення потенційних загроз, джерел розвідувальної інформації та механізмів швидкої реакції. Акцент робиться саме на предиктивному визначенні потенційного інциденту та застосуванні відповідних практик реагування.

Аналіз застосування шкідливого ПЗ в рамках APT атак

На сучасному ландшафті кіберзагроз можна виокремити три основних типи шкідливого програмного забезпечення (Malware), кампанії яких відіграють помітну роль у глобальному контексті кібербезпеки: Wiper, Ransomware, та RAT (Remote Access Trojan) [1]. У контексті кібервійни між Україною та Росією спостерігається значна кількісна перевага першого і останнього типів цього зловмисного програмного забезпечення над класичним Ransomware.

Wiper-програми, призначені для навмисного знищення даних з інфраструктур ворожих мереж, стали важливим інструментом у стратегії кібервійни, використовуючи тактику "спаленої землі" для максимального деструктивного впливу на інформаційні системи супротивника. Wiper використовуються в якості фінального інструменту більшості атак, спрямованих на винищення інфраструктури та зупинки роботи критичних систем. Одним з найяскравіших випадків застосування вайперів став інцидент в мережі телекомунікаційного провайдера «Київстар» за якого було знищено суттєву частину інформаційної інфраструктури, нанесено прямого

фінансового впливу на десятки мільйонів доларів та викликано перерву в обслуговуванні на більше ніж тиждень часу [2] [3].

В свою чергу, RAT-програми використовуються для довгострокової та непомітної інфільтрації в мережах противника, забезпечуючи можливість інціаційного доступу, збір розвідувальної інформації, що може бути використана для подальших стратегічних дій. RAT дозволяють зловмисникам виконувати дії як з проникнення до інфраструктури, так і просування в ній, а також ексфільтрації даних. Дані характеристики роблять RAT інструментом, що використовується у переважній більшості кіберінцидентів в рамках військового протистояння.

В кібервійні України з росією RAT та Wiper відіграють ключову роль серед інструментів Malware, що використовуються для атак, зокрема на критичну інфраструктуру, оскільки їх застосування відповідає стратегічним цілям атакуючого, де Wiper-програми використовуються для нанесення негайної шкоди, тоді як RAT-– для довгострокової розвідки та контролю, та в першу чергу проникнення в мережу.

В рамках аналізу визначено, що в ході кібервійни, спостерігається зростання загальної частки деструктивних інструментів – а саме Wiper [4]. Дані інструменти часто істотно модифікуються, що робить їх виявлення та блокування складними, а їх застосування відбувається на тому етапі інциденту, коли реагування, як правило, вже є запізнілим або неефективним. Це робить стратегію, орієнтовану виключно на протидію Wiper, програшною, оскільки вона не здатна ефективно запобігти або змінити хід кібератаки.

Водночас, програми типу RAT, які використовуються для отримання ініціаційного доступу до мережевої інфраструктури, представляють собою більш пріоритетний об'єкт для розробки процесів реагування. Розробка методів протидії та прогнозування масового застосування RAT може значно підвищити кіберстійкість, запобігаючи не тільки безпосереднім загрозам, але й ускладнюючи дії агресора на ранніх етапах інциденту.

На основі аналізу джерел CERT.gov.ua [5][6][7] а також інших повідомлень про інциденти з використанням RemcosRAT, стає зрозумілим, що атаки з використанням даного ШПЗ мають хвилеподібний характер, з періодичністю від кількох тижнів до декількох місяців. Ці хвилі характеризуються цілеспрямованими фішинговими кампаніями, які призначені для отримання несанкціанованого доступу до інфраструктур через компрометацію користувацької електронної пошти. Атакуючі суб’єкти неперервно переосмислюють та удосконалюють стратегії та спроможності між хвилями атак.

Особливу увагу слід звернути на методику проведення фішингових кампаній, що передують запуску RemcosRAT. Зловмисники часто використовують легітимно виглядаючі електронні листи та інші види комунікацій, які заманюють жертв до відкриття інфікованих вкладень або переходу за шкідливими посиланнями. Це зумовлює складність своєчасного виявлення та необхідність у впровадженні методів реактивної відповіді на подібні інциденти а також предиктивного прогнозування.

Прогнозування атак та графова модель атаки

Зазвичай алгоритм дій супротивника підчас регулярних атак має наступний вигляд:

— супротивник формує новий екземпляр ШПЗ та спосіб його доставки на ціль;

— супротивник формує перелік цілей;

— супротивник здійснює масовану атаку, найчастіше шляхом фішингу або інших векторів соціальної інженерії.

— супротивник переходить в стан паузи задля:

- формування супротивником нових спроможностей для атаки;
- розвиненням успіху всередині інфрастурктури певної ураженої організації, якщо хоча б одна атака мала успіх.

Настання паузи можна пояснити обмеженими ресурсами супротивника. Модель атаки відносно окремої організації – граф, де електронна пошта співробітника є вхідним вузлом, а Malware RemcosRAT [6], чи аналогічний – гранню. Таким чином у разі наявності успішного даного зв'язку з точки зору зловмисника, можливе подальше просування з використанням скомпрометованого вузла – електронної пошти – як відправної точки в інфраструктурі.

Прогнозування нових масованих атак з використанням ШПЗ конкретного сімейства, що використовуються агентами загрози в рамках кібервійни, зокрема, з наведеним вище RemcosRAT, може здійснюватись статистичним методом шляхом аналізу частоти застосування «хвиль» атак. Виявлення початку нової масованої атаки можливе шляхом використання відповідних технічних засобів захисту та активного обміну розвідувальною інформацією по загрозам.

Підхід до реагування на інцидент

З урахуванням викладеної вище моделі загроз, можна дійти ряду висновків щодо необхідних дій з реагування на подібні інциденти. Оскільки імовірність масованої атаки з залученням великої кількості скомпрометованих цілей та підготовлених засобів зростає з кожним днем після останньої аналогічної масованої атаки, розподіл зусиль з реагування може здійснюватись відповідно. В момент початку нової масованої атаки можливо використання значно більшого обсягу ресурсів – зокрема людських – ніж в звичайний період, компенсуючи витрати періодом між «хвилями». Прогнозування моменту початку масованої атаки дозволить краще спланувати використання ресурсів. В свою чергу, масовість атаки суттєво підвищує імовірність своєчасного виявлення точки входу – атаки на конкретну інфраструктуру, за умови наявності обміну розвідувальною інформацією про загрози в рамках процесів Threat Intelligence. Цим зумовлюється необхідність створення специфічних каналів обміну розвідувальною інформацією між компаніями та установами всередині держави, що дозволить масштабувати спроможності з виявлення інцидентів та спростити виявлення моменту початку інциденту.

Висновки. В моделі вектору проникнення в інформаційну інфраструктуру RAT є гранню графа атаки, спрямованим з однієї з точок входу на початкові системи в IT інфраструктурі. В рамках реагування необхідно розглядати саме цю структуру, як основну, протидію якій необхідно здійснювати. Ефективним способом протидії подібним атакам є предиктивний, з використанням розвідувальних даних по загрозам. Атаки державно-афілейованих груп супротивника мають чітко прослідковуваний хвилеподібний характер, що підвищує імовірність виявлення інциденту за рахунок його масовості – великої кількості атакованих цілей зі схожими атрибутами та інструментами – та за рахунок статистичного передбачення підвищення імовірності атаки з певними інструментами. Випливає необхідність активного обміну розвідувальною інформацією по кіберзагрозам між усіма вагомими ІКС в державі з метою виявлення хоча б одного індикатора початку нової «хвилі» атак для підвищення проактивної готовності інших об’єктів. За відсутності конкретної інформації про початок нової масованої атаки, може застосовуватись статистичний метод для визначення рівня готовності до реагування в залежності від імовірності останньої.

[1] Horowitz, M. (2022). CHECK POINT 2022 SECURITY REPORT. https://go.checkpoint.com/security-report/page-introduction.php

[2] 5 Questions (and Answers) About the Kyivstar Attack. (2023, 15 грудня). Kela blog. https://www.kelacyber.com/5-questions-and-answers-about-the-kyivstar-attack/

[3] Kyivstar Completes Preliminary Assessment of the Financial Impact of the Cyberattack [Прес-реліз]. (2024, 12 січня). https://www.veon.com/newsroom/press-releases/kyivstar-completes-preliminary-assessment-of-the-financial-impact-of-the-cyberattack

[4] 2023 SECURITY REPORT: CYBERATTACKS REACH AN ALL-TIME HIGH IN RESPONSE TO GEO-POLITICAL CONFLICT, AND THE RISE OF ‘DISRUPTION AND DESTRUCTION’ MALWARE. (2024, 8 лютого). CheckPoint Research. https://research.checkpoint.com/2023/2023-security-report-cyberattacks-reach-an-all-time-high-in-response-to-geo-political-conflict-and-the-rise-of-disruption-and-destruction-malware/

[5] Кібератака UAC-0050 з використанням Remcos RAT, замаскована під "запит СБУ" (CERT-UA#8026). (2023). https://cert.gov.ua/article/6276351

[6] "Заборгованість Київстар", "Запит СБУ": нова атака UAC-0050 з використанням RemcosRAT (CERT-UA#8338). (2023). https://cert.gov.ua/article/6276824

[7] "Повістка до суду": чергова цільова атака UAC-0050 з використанням RemcosRAT (CERT-UA#8150). (2023). https://cert.gov.ua/article/6276567

В.М. Губаревич, О.А. Зайченко, Ю.В. Маруня,
О.М. Рижков, Н.С. Зайченко

ДОСЛІДЖЕННЯ РОБОТИ ІНДУКТИВНО-ЄМНІСНОГО ПЕРЕТВОРЮВАЧА ЯК ДЖЕРЕЛА СТРУМУ ДЛЯ ТРАНЗИСТОРНОГО МОСТОВОГО ІНВЕРТОРА З ІНДУКТОРОМ

Промислові мережі електроживлення (*ПМЕ*) обмеженої потужності накладають вимоги до навантажень, що підключені до них [1]. У випадку використання індукційного нагріву у виробних каналах зі спеціальними режимами роботи, коли потрібно забезпечити високу однорідність розподілу температури в обсязі розплавленого скла і вихідна потужність в процесі роботи не регулюється, було розглянуто можливість застосування індуктивно-ємнісних перетворювачів (*ІЄП*) джерела промислової напруги в джерело струму в якості джерела живлення для інвертора струму на транзисторах [2,3].

Мостовий випрямляч, що знаходиться в існуючих перетворювачах для індукційного нагріву, споживає струм несинусоїдної форми і є потужним нелінійним навантаженням для систем обмеженої потужності, погіршуючи параметри якості електроенергії мережі. Якщо нелінійний струм проходить через коло з поздовжніми параметрами, то виникають спотворення напруги у вузлах підключення інших споживачів, що впливає на їх роботу. Це породжує проблеми електромагнітної сумісності. Для забезпечення ефективності функціонування та експлуатації *ПМЕ* обмеженої потужності є дотримання нормованого рівня параметрів якості електричної енергії [4]. І чим «слабкішою» є така система, тобто чим більший відносний опір короткого замикання вона має, тим суворішими мають бути обмеження за показниками якості електроенергії, щоби отримати безпечну та безвідмовну роботу споживачів. Тому електромагнітна сумісність мостових випрямлячів з *ПМЕ* обмеженої потужності є обов'язковою.

В роботах [5,6] проведений порівняльний аналіз цих схем та досліджено електромагнітні процеси в однофазному мостовому випрямлячі з ємнісним фільтром та активним навантаженням при живленні безпосередньо від *ІЄП,* який одночасно виконує функції фільтра та джерела струму. Такий випрямляч з *ІЄП* на вході називають струмопараметричним, що пояснюється формуванням вихідної струмової характеристики за рахунок резонансного налагодження параметрів реактивних елементів перетворювача. Дослідження в [6] показали, що *ІЄП* за схемою *T1-LCL* може використовуватися як джерело струму та фільтр гармонік струму, водночас має високий $\cos\phi$, а також найкращі масогабаритні показники серед розглянутих *ІЄП,* враховуючи параметри якості електроенергії. Розглянемо систему «*ІЄП* – мостовий випрямляч – ємнісний фільтр – мостовий інвертор струму – паралельний резонансний контур» (рис. 1)

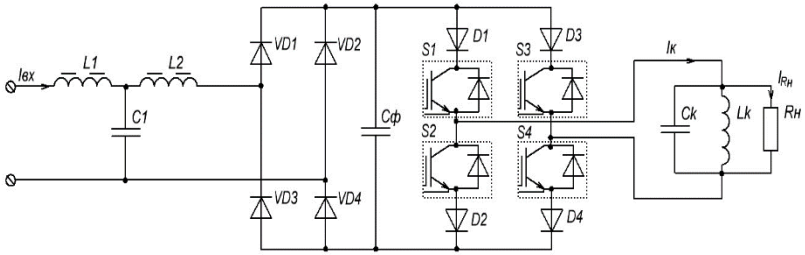


Рисунок 1 – Джерело живлення для індукційного нагріву

Параметри схеми для моделювання були такими: $U_м$=*230 В* [5], частота напруги мережі *50 Гц*, потужність навантаження *10 кВт (Uн*=300±10%В*)*, ємність конденсатора фільтра *Сф*=10мФ. *ІЄП* представлено реакторами з індуктивностями *L1=L2=17,5 мГн* та конденсатором з ємністю *С=579 мкФ,* які налаштовані в резонанс на основній частоті.

Параметри індуктора наступні - *Ск=10 мкФ, Lк=39мГн, Rн=10 Ом.* Частота спрацьовування ключів інвертора – 8 кГц. Ці параметри обрано на основі реальних індуктора та інвертора, а *ІЄП* розрахований теоретично з урахуванням визначених в [5] коефіцієнтів перетворення по струму та напрузі та оптимізації за масогабаритними показниками.

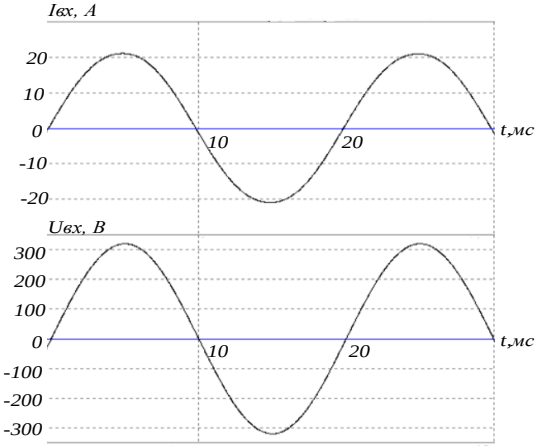


Рисунок 2 – Епюри струму та напруги на вході *ІЄП*

На рис. 2 зображено форми струму та напруги на вході *ІЄП*, при цьому $\cos\phi$=0,99; THD_I <1%. На рис. 3 зображено форми струму та напруги на вході індуктора, на рис. 4 зображено форми струму та напруги на активному навантаженні.

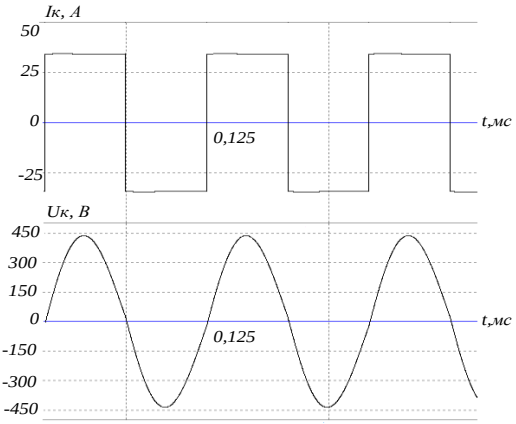


Рисунок 3 – Епюри струму та напруги на вході резонансного контуру

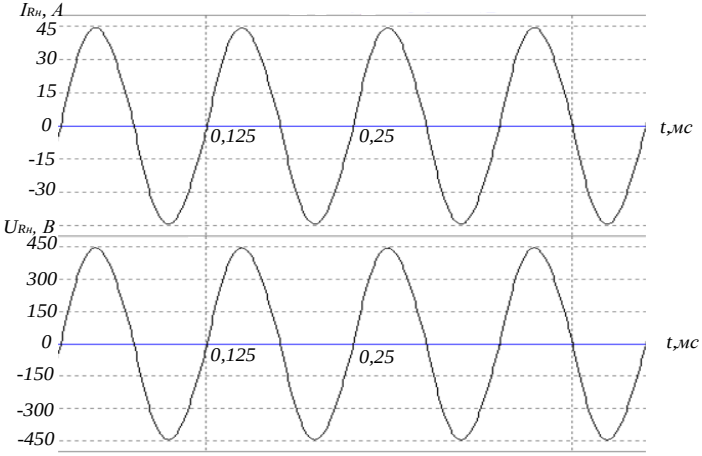


Рисунок 4 – Епюри струму та напруги на *Rн* резонансного контуру

На рис. 5 наведено навантажувальні характеристики *ІЄП* за схемою *T1-LC* при роботі на чисто активне навантаження (верхня крива) і при роботі на інвертор з резонансним контуром (нижня крива), з яких видно, що «жорсткість» характеристики *ІЄП* (нижня крива) зберігається: джерело струму працює надійно, стабілізація струму навантаження є достатньою.

Проведені дослідження демонструють доцільність використання *ІЄП* за схемою *T1-LC* в якості джерела струму в установках індукційного нагріву виробних каналів скловареної печі, оскільки схема є не тільки перетворювачем, але і має високі фільтруючі властивості: коефіцієнт

потужності $\cos\phi = 0{,}99$, а коефіцієнт гармонік струму THD_I <1%.

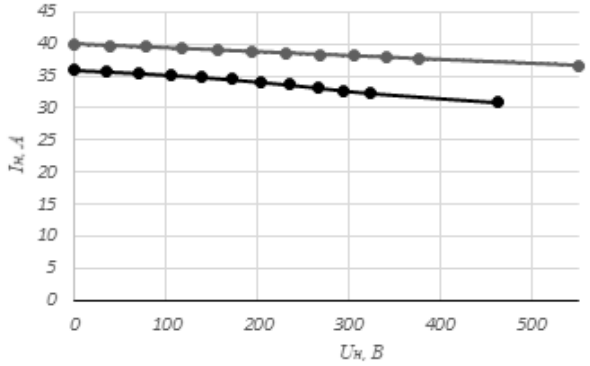


Рисунок 5 – Навантажувальні характеристики ІЄП

[1] Волков И.В., Акинин К.П., Исаков Г.В. Сравнительный анализ способов фильтрации токов, потребляемых выпрямительными установками. Технічна електродинаміка. 1999. No 6. С. 23–27.

[2] Волков И.В., Подольцев А.Д., Кучерявая И.Н. Электромагнитные, тепловые и гидродинамические процессы при индукционном нагреве выходного канала стекловаренной печи. Праці Ін-ту електродинаміки НАН України. 2018. Вип. 51. С. 113-120.

[3] Кондратенко И. П. Энергетические параметры трехфазных цилиндрических индукторов. Технічна електродинаміка. 1996. № 6. С. 55–58.

[4] EN 61000-3-12:2017. Electromagnetic compatibility. Part 3-2: Limits. Limits for harmonic currents produced by equipment connected to public low-voltage systems with input current >16A and ≤ 75A per phase.

[5] Спірін В.М., Губаревич В.М., Маруня Ю.В., Салко С.В., Гребенюк В.Г. Визначення коефіцієнтів перетворення мостового однофазного випрямляча з живленням від індуктивно-ємнісного перетворювача та паралельним активно-ємнісним навантаженням. Технічна електродинаміка. 2019. Вип. 5. С. 43-48.

[6] Спірін В.М., Губаревич В.М., Маруня Ю.В., Салко С.В., Гребенюк В.Г. Оптимізація індуктивно-ємнісного перетворювача з мостовим однофазним випрямлячем, ємнісним фільтром та активним навантаженням за питомими потужностями електромагнітних елементів. Технічна електродинаміка. 2019. Вип. 6. С. 25-29.

І.Е. Фуртат, Ю.О. Фуртат

KINETICS OF ADSORPTION DURING THE DYEING PROCESS

To describe the process of dyeing textile materials, in the general case, it is not enough to consider the kinetics of dye adsorption by a single fiber. This assumption is valid in the case of low intensity low temperature processes, when the diffusion coefficient of the dye to the fiber is several orders of magnitude smaller than the diffusion coefficient in the space between the fibers. In this case, the mass transfer process is determined by the transfer in the fiber. As the temperature rises or with other methods of intensifying the process, there is a sharp increase in the diffusion coefficient in the fiber, while the diffusion coefficient in the liquid phase outside the fiber changes to an incomparably lesser extent, i.e. the difference in the values of the diffusion coefficients in the fiber and outside the fiber decreases sharply. If we take into account the significant difference in the linear dimensions of the fiber and thread, it becomes obvious that there comes a moment when the relaxation time of the diffusion in the fiber, defined as $\tau_f = \frac{r_f^2}{D_f^2}$, becomes less than the relaxation time in the thread, defined as $\tau_t = \frac{r_t^2}{D_t^2}$. Given these conditions for the comparability of the relaxation times of diffusion along the fiber and thread, it is completely incorrect to describe the process of dyeing a textile material by considering the kinetics of the process in a separate fiber.

The following scheme of the process is more rigorous: transfer of the dye to the surface of the thread, diffusion in the space between the fibers, adsorption by the inner surface of the fiber, and chemical interaction, if any.

Such a formulation of the problem has much in common with the problems of diffusion in granular porous media that have attracted attention, especially recently [1], which are of great importance for the quantitative description of the dynamics of sorption both in general theoretical terms and for describing various technological processes: filtration through a layer grains of various shapes, diffusion extraction of substances from porous media, etc.

The most general approach to solving problems of diffusion in porous systems containing microporous inclusions was developed by Zolotarev and Radushkevich [2]. The equations they obtained describe diffusion processes without restrictions on the shape of the microporous inclusion and, in general, on the geometry of the system. Naturally, the solution of these equations requires a certain specification both in relation to the shape of the microporous inclusion and in relation to the nature of diffusion.

When considering such processes, it is necessary to proceed from the solution of the problem of diffusion into a microporous inclusion. The process of mass transfer in a fiber is considered as a diffusion process with an apparent diffusion coefficient . In the general case, this statement of the problem should be

supplemented by taking into account the interaction of double electrical layers of the dye particle and fibers, which slows down (for the same surface charges) the process of dye transfer

In the meantime, in order to simplify the problem, the following model of the process is proposed: we consider molecular diffusion into an infinitely long end-impermeable cylinder (thread) with many infinitely long microporous cylindrical inclusions (fibers) uniformly distributed over its cross section. In this case, a problem is considered that is symmetrical in the section.

The kinetic problem is solved for four cases corresponding to the following process conditions:

1. Isothermal mode, constant concentration of dye on the surface of the thread. This task corresponds to dyeing from baths of constant concentration.

2. Isothermal mode, variable concentration on the surface. Corresponds to dyeing from baths of variable concentration, fixing from a film in an environment of saturated steam or in an environment of superheated steam, or heated air at relatively low temperatures (when the heating time of the material is much less than the fixation time).

3. Non-isothermal mode, constant concentration on the surface. Corresponds to dyeing from an aerosol medium.

4. Non-isothermal mode, variable surface concentration. This most complex case corresponds to high-intensity, high-temperature methods of fixing at temperatures of the material at the end of the process, close to the temperature of its softening or destruction.

[1] Ruchenstein, E., Vaidynathan, A.S., & Youngquist, G.R. (1971). Sorption by Solids with bidisperse pore structures. Journal of Chemical Engineering Science, vol. 26 (№ 9), 1305-1318.

[2] Золотарев, П.П., & Радушкевич, Л.В. (1970). О динамике и кинетике неизотермической адсорбции. Журнал физической химии, том 44 (№ 4), 889-899.

В.В. Кучанський, О.М. Коваленко

ЕКОЛОГІЧНІ АСПЕКТИ ДІАГНОСТУВАННЯ ПОВІТРЯНИХ ЛІНІЙ ЕЛЕКТРОПЕРЕДАВАННЯ БЕЗПІЛОТНИМИ ТЕХНІЧНИМИ ЗАСОБАМИ

За характером впливу на довкілля вплив повітряних ліній (ПЛ) можна розділити на механічне та електромагнітне, а також необхідно враховувати хімічне забруднення повітря продуктами, що виникають при коронних розрядах [1-3], радіо та телевізійні завади, акустичний шум. Просіки, під'їзні шляхи, опори ПЛ впливають на функціонування елементів екологічних систем, змінюючи ландшафтні, мікрокліматичні умови.

Просіка шириною понад 200 м нерідко стає непереборною перешкодою для переміщення тварин. У період міграції на просіках годуються та відпочивають великі скупчення птахів, але у місцях масового перельоту повітряні лінії можуть служити механічною перешкодою. Спорудження ліній електропередавання пов'язані з відчуженням земель, що позначається на сільському господарстві. Невпорядковане розташування ПЛ порушує цілісність полів та кормових угідь. Створюються перешкоди обробки полів з повітря, обмежується застосування агротехніки. Повітряні лінії проходять також і через лісові масиви, цінність яких визначається запасами деревини, лікарських рослин, мисливських тварин, ягід, грибів. Основним специфічним чинником впливу ПЛ на довкілля є електромагнітне поле (ЕМП) [4-7].

Вплив ЕМП на ґрунт залежить від концентрації сполук заліза та гумусу у самому ґрунті. Електричне поле викликає поляризацію та структурну перебудову елементів ґрунту, впливає на процес ґрунтоутворення. ЕМП може надавати стимулюючу дію на інтенсивність росту зелених рослин на початковій стадії розвитку, потім дія ЕМП стає гнітючим.

При тривалому перебування людини в ЕМП (10 кВ/м) можуть виникнути несприятливі фізіологічні зміни, пов'язані з впливом на нервову та серцево-судинну систему (зміни тиску, пульсу, аритмія тощо). Ці явища зникають через деякий час після припинення дії ЕМП. Розроблені норми, що обмежують напруженість електричне поле під повітряними лініями.

Аеросканування є незамінним при проектуванні та реконструкції або капітальному ремонті, а також при створенні електронних паспортів ПЛ. Комбіновані способи аеродіагностики успішно доповнюють інформацію аеросканування. Відпрацьовано основні методичні прийоми аеродіагностики. Сформовано попередні критерії дефектоскопії ПЛ за характеристиками електромагнітного випромінювання розрядних процесів. На основі отриманого досвіду сформовано загальні вимоги до завдань аеродіагностики та основні технічні вимоги до апаратури.

На сьогодні існує необхідність, розроблення стандарту із застосування безпілотних літальних апаратів для обстеження повітряних ліній електропередавання та енергетичних об'єктів міг урегулювати практичні

аспекти застосування екодронів в енергетиці [11-14]. Такий документ регламентував би проведення щорічних періодичних оглядів стану трас ПЛ, з метою виявлення низки порушень, у тому числі: 1) наявність на краю просіки окремих дерев, що загрожують падінням або розростанням бік ПЛ на неприпустимі відстані; 2) недостатня ширина просіки по трасі ПЛ; 3) наявність під проводами дерев та чагарників заввишки 4 м і більше; 4) наявність рослинності землі, відведеної під опору; 5) виконання на трасі в охоронних зонах неузгоджених робіт; 6) підтоплення в охоронній зоні по трасі ПЛ; 7) крім планового щорічного огляду, організовується додатковий моніторинг пожежонебезпечний період, грозовий період та в період льодоутворення.

Усього документ має містити обов'язкові пункти для технічного завдання «екодронам», а також рекомендації щодо збору та синтезу картографічного масиву даних його аналізу, зберігання та експорту в геоінформаційну систему, тобто вся зібрана інформація обробляється, зберігається і може бути затребувана будь-якої миті. Документ також містив би обґрунтовані вимоги до використовуваної апаратури та програмного забезпечення. Слід зазначити, що останнє може бути з успіхом використане для вирішення багатьох екологічних завдань.

[1] Blinov, I., Zaitsev, I.O., Kuchanskyy, V.V.: Problems, methods and means of monitoring power losses in overhead transmission lines. In: Babak, V.P., Isaenko, V.M., Zaporozhets, A.O. (eds.) Systems, Decision and Control in Energy I. Studies in Systems, Decision and Control, pp. 123–136. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-48583-2_8

[2] Kuchanskyy, V.V., Malakhatka, D.O., Blinov, I.: Efficiency increase of open phase modes in bulk electrical networks. In: Zaporozhets, A., Artemchuk, V. (eds.) Systems, Decision and Control in Energy II. Studies in Systems, Decision and Control, pp. 31–48. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-69189-9_2

[3] Zaitsev, I.O. & Kuchanskyy, V.V. (2021). Corona discharge problem in extra high voltage transmission line. In: Systems, Decision and Control in Energy II, Studies in Systems, Decision and Control (edited by A. Zaporozhets & V. Artemchuk). Pp. 3–30. Cham: Springer International Publishing. DOI: 10.1007/978-3-030-69189-9_1

[4] Morgan J. L., Gergel S. E., Coops N. C. Aerial photography: A rapidly evolving tool for ecological management. BioScience 60. 2010. P. 47-59.

[5] Seasonal variation in spectral signatures of five genera of rainforest trees / M. Papes, R. Tupayachi, P. Martfnez, A. T. Peterson, G. P. Asner, G. V. N. Powell // IEEE J. of Selected Topics in Applied Earth Observations and Remote Sensing 6 . 2013. P. 339-350

[6] Villa, P., Bertazzi, A., Leva, M. (2002). Compact transmission line with inverted delta configuration. Cigre 2002 conference, No. 22.103, pp.1-4.

[7] Melo, M. O. B. C., Fonseca, L. C. A., Fontana, E., Naidu, S. R. (1997). Lightning Performance of Compact Transmission Lines. International Conference on Power Systems Transients (IPST'97), pp. 319-324.

В.В. Кучанський, Ю.Г. Лиховид

АНАЛІЗ ГРАНИЧНИХ РЕЖИМІВ РОБОТИ ЕЛЕКТРОЕНЕРГЕТИЧНИХ СИСТЕМ ЗА НЕПОВНОФАЗНИХ РЕЖИМІВ

Фізична необхідність забезпечення балансу потужності в кожний момент часу у всіх елементах виробництва, перетворення, передавання та розподілу електричної енергії, що розміщені на великій території, відсутність можливостей запасати електроенергію в необхідних обсягах та висока вартість електроенергії визначили особливу важливість надійності електропостачання споживачів. Синхронне обертання роторів всіх генераторів є основою основ роботи електричних систем (ЕС), що зумовило вирішення проблем, пов'язаних із забезпеченням статичної стійкості. Майже всі регламентні документи, зрештою, спрямовані на підтримку стійкості ЕС.

Робота присвячена дослідженню математичної моделі потокорозподілу ЕС та її особливостей, що впливають на розрахункові граничні режими (ГР) та області існування режимів (ОІР). Запропоновано та досліджено геометричну інтерпретацію рівнянь усталених рівнянь режимів як гіперповерхні у просторі потужностей вузлів, а ОІР – як проекцію цієї гіперповерхні вздовж осі активної потужності балансувального вузла. Запропоновано розрахункову модель ГР, що забезпечує адекватну оцінку коефіцієнтів запасу статичної стійкості.

Лінія електропередавання зазвичай проектується, виходячи з принципів певного встановленого економічним аналізом перетоком потужності. При цьому перевіряється можливість перевантаження лінії електропередавання. Крім цього визначаються умови роботи лінії електропередавання в післяаварійному режимі, коли в результаті аварії можуть бути від’єднані: одна з фаз лінії електропередавання, груп однофазних автотрансформаторів та шунтувальних реакторів або одна з груп паралельно працюючих автотрансформаторів.

По тривалим нормальним та післяаварійним режимам визначаються основні показники роботи лінії електропередавання, розраховуються її статична стійкість, визначаються втрати потужності. Однак, крім тривало-існуючих нормальних усталених режимів, в лінії електропередавання можуть існувати нетривалі анормальні режими. Такі режими не можуть вважатися аварійними, так як на непошкодженій лінії, за умов роботи в нормальному стані обладнання. Але в той же час не є нормальними, тому правильніше їх називати анормальними режимами. Можливість існування тривалих неповнореакторних режимів електропередавання надвисокої напруги зазначається у роботах [1-5].

Для вирішення цих питань розрахунки стаціонарних режимів необхідно виконувати, розглядаючи мережу як трифазну, з несиметричними елементами, проте розроблення трифазних моделей (у фазних координатах)

значно трудомісткіша, тому такі моделі, якщо й розробляються, то лише як вузько спеціалізовані [6-8] для окремих завдань (розрахунок неповнофазного режиму електропередавання, наведених напруг тощо). Відсутність моделей у фазних координатах вже стає фактором, що стримує вирішення цілого ряду завдань. Як підтвердження цього можна розглядати появу цілого ряду робіт [9-12], спрямованих на те, щоб представити трифазні схеми заміщення мереж з несиметрією, як однофазні схеми заміщення в симетричних режимах набором резистивних, індуктивних та ємнісних елементів.

Неповнофазний режим роботи групи однофазних ШР виглядає наступним чином у випадку відключення фази В однієї з ШР наведено на рис.1 а) та його заступна схема у з узагальненим вектором.

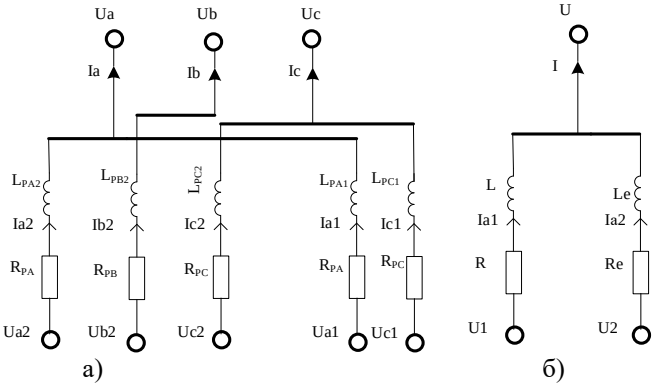


Рис.1

Модель автотрансформатора наведена на рис. 2.

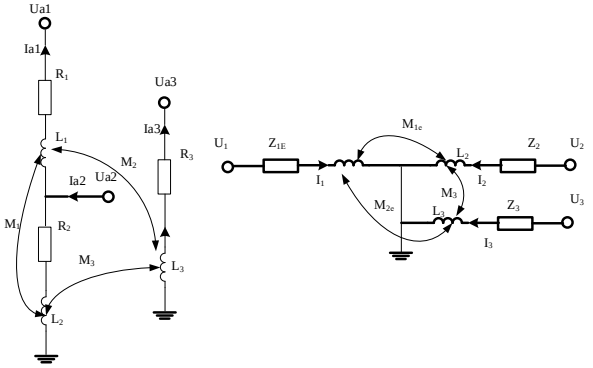


Рис. 2. Модель автотрансформатора

Напруги фаз з відключеними реакторами підвищуються, тому необхідно або знижувати рівень напруги в мережі (що призводить до збільшення втрат і зниження меж потужності, що передається), або допускати тривалі режими з підвищеними напругами окремих фаз, або, нарешті, обмежувати тривалість

неповнореакторних режимів. Для вирішення цих питань необхідні додаткові дослідження.

[1] Кириленко О.В., Буткевич О.Ф., Черненко П.О., Блінов І.В. Моделі, засоби та заходи забезпечення надійного та ефективного функціонування енергопостачальних компаній, балансування та розподілу електроенергії в ОЕС України. Праці Інституту електродинаміки НАН України. Зб. наук. праць. 2019. Вип. 53. С. 5-14. DOI: https://doi.org/10.15407/publishing2019.53.005

[2] Kuchanskyy, V., Butkevych, O. (2024). On Effective Use's Ensuring of High-Voltage Electrical Networks Under Non-full Phase Operational Conditions. In: Kyrylenko, O., Denysiuk, S., Strzelecki, R., Blinov, I., Zaitsev, I., Zaporozhets, A. (eds) Power Systems Research and Operation. Studies in Systems, Decision and Control, vol 512. Springer, Cham. https://doi.org/10.1007/978-3-031-44772-3_2

[3] Буткевич О.Ф., Кучанський В.В. Забезпечення ефективного функціонування енергосистеми в неповнофазних режимах. Electrical and Power Engineering and Electromechanics (EPEE 2023). Odesa, Ukraine, June 15, 2023: proceedings. Odesa Military Academy, 2023. 26-28p.

[4] Kundur P. Power system stability and control, McGraw-Hill, Inc., USA, 1993, 1196 p.

[5] Anderson P.M., Fouad A.A. Power system control and stability, Second edition, Willeyinterscience, USA, 2003, 672 p.

[6] Kuchanskyy V. (2016) Criteria of resonance overvoltages occurrence in abnormal conditions of extra high voltage transmission lines. Scientific works of Vinnitsa National Technical University. (4). 51–54.

[7] Kuchanskyy, V.; Satyam, P.; Rubanenko, O.; Hunko, I. Measures and technical means for increasing efficiency and reliability of extra high voltage transmission lines. Prz. Elektrotech. 2020, 11, 135–141.

[8] Kuznetsov, Y. Tugay and V. Kuchanskyy (2012) Abnormal overvoltages in the modes of transmission lines EHV. Tekhnichna Elektrodynamika, 2012(2), pp 40-41.

[9] Тугай Ю.І., Кучанський В.В., Тугай І.Ю. Застосування керованих пристроїв компенсації зарядної потужності ЛЕП НВН в електричних мережах. Технічна електродинаміка. 2021. No 1. С. 53−56. DOI: https://doi.org/10.15407/techned2021.01.053

[10] O. Hunko, V. V. Kuchanskyy, A. B. Nesterko, Engineering sciences: development prospects in countries of Europe at the beginning of the third millennium: Collective monograph. vol. 2, Riga, Izdevniecība "Baltija Publishing", 2018.

[11] Кучанський, В., & Малахатка, Д. (2021). Заходи та технічні засоби підвищення ефективності режимів роботи магістральних електричних мереж. Publishing House «European Scientific Platform». https://doi.org/10.36074/ztzperrmrm-monograph.2021

[12] Зайцев Є. О. Підвищення експлуатаційної надійності та ефективності роботи електричних мереж та електроустаткування : монографія / Є. О. Зайцев, В. В. Кучанський, І. О. Гунько. - Вінниця : ГО «Європейська наукова платформа», 2021. - 156 с.

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

ЗАСТОСУВАННЯ ШВИДКОГО ПЕРЕТВОРЕННЯ ФУР'Є У КОРЕЛЯЦІЙНОМУ ПАРАМЕТРИЧНОМУ ТЕЧЕШУКАЧІ

На рис.1. представлено узагальнений алгоритм роботи течешукача, ефективність якого обумовлюється застосуванням швидкого перетворення Фур'є (ШПФ) майже на всіх рівнях обробки даних.

Алгоритм починається з встановлення пари датчиків на кінцях пошкодженої ділянки трубопроводу у перше положення. Положення датчиків у місцях технологічного доступу до трубопроводу суттєво впливає на чутливість кореляційних течешукачей (КТ) до інформативного типу акустичних хвиль, що генеруються витоками. Це положення вибирається ітераційним шляхом, виходячи з аналізу параметрів взаємної кореляційної функції акустичних сигналів (ВКФ) [1,2]. Оцифровані сигнали підлягають спектральному аналізу, виходячи з якого визначаються параметри вхідних цифрових фільтрів [3]. Вхідні фільтри призначені для попередньої фільтрації сигналів у виносних блоках КТ перед їхньою передачею по радіоканалах у системний, центральний блок для подальшої кореляційної обробки. Важливість попередньої фільтрації викликана обмеженим динамічним діапазоном радіоканалу, який часто не перевищує 40 дБ. За прийнятими у системний блок сигналами обчислюється оцінка їхньої ВКФ, яка потім розкладається на вузькосмугові складові. Для кожної складової визначаються параметри ВКФ відповідно до [2,3]. Як правило, параметрів розкладання, прийнятих за умовчанням для визначеного типу трубопроводів, буває достатньо. Однак, при малому відношенні сигнал-перешкода, координати витоку можуть не виявитися. Тоді параметри розкладання коригуються та операції розкладання та аналізу отриманих параметрів ВКФ повторюються. Потім один із датчиків зміщують на 0,5 - 3м. на трубопроводі та наведені вище операції повторюють. Як правило, достатньо 2-3 повторень за різних положень датчиків. Таким чином, проводиться описане у [2,3] узгоджене частотно-просторове налаштування КТ на сигнали витоку. З аналізу сукупності отриманих частотно-просторових параметрів ВКФ визначається найбільш ймовірна координата витоку. Наведемо далі приклад застосування ШПФ у частині обробки приладової оцінки ВКФ. Операції прямого та зворотного ШПФ будемо позначати відповідно як F та F^{-1}.

Обробка кореляційних функцій. Параметрами розкладання ВКФ є: $f_н$ і $f_в$ - нижня та верхня частоти, у межах яких виконується параметричний аналіз ВКФ шляхом її сканування смуговими фільтрами (СФ); Δf - крок перестроювання за частотою СФ; B – ширина смуги пропускання СФ; m – номер позиції пари датчиків КТ за порядком на трубопроводі, при якому обчислена оцінка ВКФ; N_c - число налаштувань СФ з кроком Δf у межах

Рис.1 Обробка даних у кореляційному параметричному течешукачі.

$f_н$ і $f_в$. Позначимо отриману для позиції m датчиків на трубопроводі

оцінку ВКФ як $\hat{R}_{ab}(m,k)$, де m позначає просторову залежність оцінки ВКФ. Нижче надано опис алгоритму її обробки.

1. Формують вихідні дані для ШПФ оцінки ВКФ:

$$\mathrm{Re}\left(\dot{\gamma}(m,k)\right)=\begin{cases}\hat{R}_{ab}(m,k)\ ,\ \text{при}\ k\in\left[-(k_{\max}/2)...(k_{\max}/2)\right],\\ 0\ \text{при}\ k\in\left[(k_{\max}/2)+1...L-1\right]\end{cases}$$

$$\mathrm{Im}\left(\dot{\gamma}(m,k)\right)=0 \text{ при } k\in\left[0...L-1\right],\ \text{де}\ L=2^m \text{ - число точок ШПФ.}$$

2. Обчислюють частотний образ оцінки ВКФ: $\left\{\dot{P}(m,q)\right\}=\mathrm{F}\left\{\dot{\gamma}(m,k)\right\}$.

3. Ініціюють початкове значення лічильника сканування (фільтрації) оцінки ВКФ i=1;

4. Формують резонансні частоти для двох смугових фільтрів:

$$f_i = f_н + \frac{\Delta f}{2} + \Delta f\cdot(i-1);\quad f_{i+1} = f_i + \Delta f;$$

5. Формують дві імпульсні характеристики (ІХ) скануючого фільтра оцінки ВКФ:

$$h(B,\, f_i, n) = 2\cdot h_{нч}(B,n)\cdot\cos(2\pi f_i T(n-\frac{N_h-1}{2})),\ \forall n\in\left[0..N_h\right],$$

$$h(B,\, f_{i+1}, n) = 2\cdot h_{нч}(B,n)\cdot\cos(2\pi f_{i+1} T(n-\frac{N_h-1}{2})),\ \forall n\in\left[0..N_h\right]$$

де $h_{нч}(B,n)$ - ІХ оптимального у сенсі узагальненої теореми Чебишева фільтр нижніх частот з симетричною імпульсною характеристикою і з лінійною фазочастотною характеристикою [4]; T – інтервал дискретизації сигналів за часом, N_h - непарна кількість відліків $h_{нч}(B,n)$.

6. Обчислюють частотні образи ІХ:

- Формують комплексний масив $\left\{\dot{h}(n)\right\}$

$$\mathrm{Re}\left(\dot{h}(n)\right)=\begin{cases}h\left(B,\, f_i, n\right),\ \text{при}\ n\in\left[0..(N_h-1)\right],\\ 0,\ \text{при}\ n\in\left[N_h..(L-1)\right],\end{cases}$$

$$\mathrm{Im}\left(\dot{h}(n)\right)=\begin{cases}h\left(B,\, f_{i+1}, n\right),\ \text{при}\ n\in\left[0..(N_h-1)\right],\\ 0,\ \text{при}\ n\in\left[N_h..(L-1)\right],\end{cases}$$

де $L=2^m$ - кількість точок ШПФ.

- Обчислюють $\left\{\dot{H}(q)\right\}=\mathrm{F}\left\{\dot{h}(n)\right\}$;
- $\left\{\dot{H}(q)\right\}$ поділяють на $\left\{\dot{H}(B,\, f_i, q)\right\}$ і $\left\{\dot{H}(B,\, f_{i+1}, q)\right\}$, які відповідають $\mathrm{F}\left\{\mathrm{Re}\left(\dot{h}(n)\right)\right\}$ і $\mathrm{F}\left\{\mathrm{Im}\left(\dot{h}(n)\right)\right\}$:

$$\dot{H}\left(B,\, f_i, q\right) = \frac{\dot{H}\left(q\right) + \dot{H}^{*}\left(L-q\right)}{2},\ \dot{H}\left(B,\, f_{i+1}, q\right) = \frac{\dot{H}\left(q\right) - \dot{H}^{*}\left(L-q\right)}{2j}$$

$\forall k \in \left[0...L-1\right]$.

7. Формують результат сканування оцінки ВКФ:

Обчислюють $\left\{\phi\left(m, B,\, f_i, n\right)\right\} = \mathrm{F}^{-1}\left(\left\{\dot{P}\left(m,q\right)\cdot\dot{H}^{*}\left(B,\, f_i, q\right)\right\}\cdot L^{-1}\right)$,

$$\left\{\phi\left(m, B,\, f_{i+1}, n\right)\right\} = \mathrm{F}^{-1}\left(\left\{\dot{P}\left(m,q\right)\cdot\dot{H}^{*}\left(B,\, f_{i+1}, q\right)\right\}\cdot L^{-1}\right).$$

8. Формують параметри ВКФ за $\left\{\phi\left(m, B,\, f_i, n\right)\right\}$ і $\left\{\phi\left(m, B,\, f_{i+1}, n\right)\right\}$

Відповідно до [2,3]. Значення лічильника частотного сканування оцінки ВКФ збільшують на 2.

9. Якщо значення лічильника перебільшило заплановане значення N_c, то виконують відображення всіх отриманих параметрів ВКФ відповідно до [2,3]. В іншому випадку виконання алгоритму повторюють з п.4.

Обробка даних на основі швидкого перетворення Фур'є є ефективним обчислювальним алгоритмом у сучасних кореляційних шукачах. Особливу гнучкість, можливість оптимізації обчислень, застосуванню ШПФ надає операція поєднання двох дійсних процесів в один комплексний [5]. Застосування ШПФ забезпечує добре узгодження режимів роботи течешукача з його апаратними можливостями, вимоги до яких не є занадто високими. Саме завдяки ШПФ, для організації кореляційної та подальшої обробки даних достатньо застосування звичайного мобільного ПК типу notebook, планшета і навіть смартфона.

[1] Патент на корисну модель № 144444. Параметричний кореляційний спосіб визначення координат витоків трубопроводів. Публікація відомостей 25.09.2020, Бюл. №18. Владимирський О.А., Владимирський І.А.

[2] Владимирський О.А., Владимирський І.А. Кореляційні параметричні методи визначення координат витоків підземних трубопроводів. Електронне моделювання. 2021. 43 (3). С.3-16.

[3] Владимирский А. А., Владимирский И. А. Обработка данных на основе БПФ при поиске утечек. Збірник наукових праць ІПМЕ ім. Г. Є. Пухова НАН України. 1998. Вип. 6. С. 39-49.

[4] Рабинер Л., Гоулд Б..Теория и применение цифровой обработки сигналов. Пер.с англ. М.: Мир., 1978. 848с.

[5] Дж.Бендат, А.Пирсол. Прикладной анализ случайных данных. Пер.с англ. М.: Мир. 1989. 540с.

О.А. Владимирський, І.А. Владимирський,
І.П. Криворучко, Г.В. Анфімова

РОЗРОБКА СИЛОВИМІРЮВАЛЬНОЇ СИСТЕМИ МАНЕКЕН 1.03

Групою "Технічна діагностика" ІПМЕ ім. Г.Є. Пухова НАН України спільно з ТОВ “ТЕСКО” (м. Київ) розроблено та випробувано силовимірювальну систему “МАНЕКЕН 1.03”, призначену для проведення статичних та динамічних випробувань засобів індивідуального захисту від падіння та при падінні з висоти, в т.ч. систем утримання, ременів безпеки, поясів запобіжних, стропів, пристроїв для зупинки падіння, поглиначів енергії, систем зупинки падіння та ін. відповідно до нормативних вимог [1].

До складу силовимірювальної системи "МАНЕКЕН 1.03" входять S-подібний тензодатчик Zemic H3-C3-3,0t-6B з вушами (робоче навантаження до 3000 кг), оригінальний вимірювальний блок з фільтрами, АЦП (16 розрядів, частота дискретизації – 2000 кГц) та інтерфейсом USB (Рис.1.) та ноутбук зі спеціальним програмним забезпеченням.

Рис.1. Тензодатчик та інтерфейсний блок силовимірювальної системи "МАНЕКЕН 1.03"

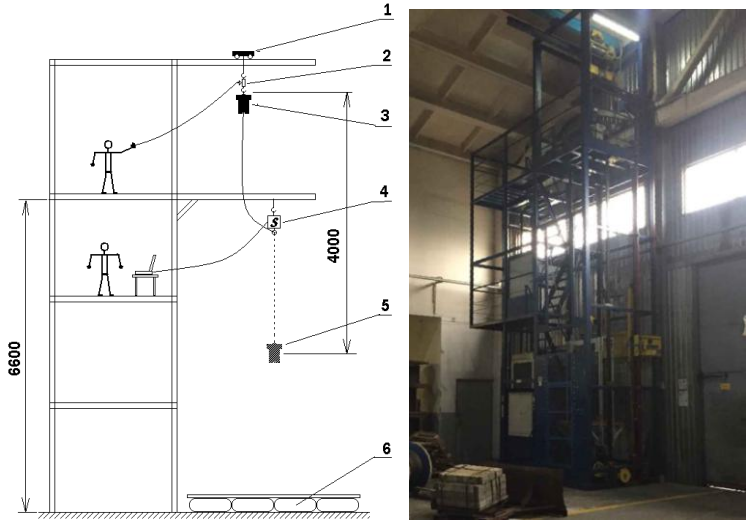
Випробування проводять у складі спеціального стенду (рис.2.). Параметрами, що характеризують технічні можливості стенду, є: висота вільного падіння манекена, маса манекена, кінетична енергія падаючого манекена, накопичена на початок гальмування.

Маса манекена – (100 ± 1,0) кг; Діапазон вимірювання зусилля ривка – від 200 до 1600 кг;

Основа стенду – сталевий каркас із вертикальних стійок та горизонтальних балок (див. рис.2а). Перед випробуванням підйом манекена 3 здійснюється за допомогою лебідки на візку 1. Скидання манекена здійснюється за допомогою скидаючого механізму 2. Страхувальний трос кріпиться до консольної балки через вимірювальний тензодатчик 4, який входить до складу силовимірювальної системи "МАНЕКЕН 1.03". Дистанція вільного падіння манекена – до 4 М. Початкове та кінцеве положення манекена при випробуваннях представлено у позиціях 3 та 5 відповідно. Для унеможливлення пошкодження обладнання при обриві страхувального троса

та систем утримання передбачена установка буферної подушки 6.

На рис.3 представлений манекен із системою утримання.



а) б)

Рис.2. Стенд для проведення випробувань: а) схема стенду; б) фотографія стенду на заводі “Каратліфткомплект”, м. Вишгород.

а) б)

Рис.3. Манекен з комплектом індивідуального захисту від падіння з висоти на випробувальному манекені: а) перед випробуваннями; б) після випробування – захисний комплект пошкоджений, ремені надірвані, але манекен не випав.

Приклади зареєстрованих випробувань засобів індивідуального захисту від падіння з висоти на стенді “Каратліфткомплект” 02.02.2024 р. представлені на рис.4 - рис.6.

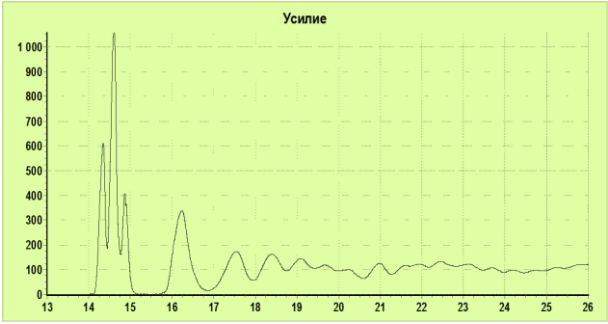


Рис.4. Скидання манекена догори ногами, довжина троса 2 М. Дистанція вільного падіння манекена – 4 М. Максимальне зусилля – 1057,2 кг. Трос подовжився на 12 см, але не порвався. Манекен із страховки не випав.

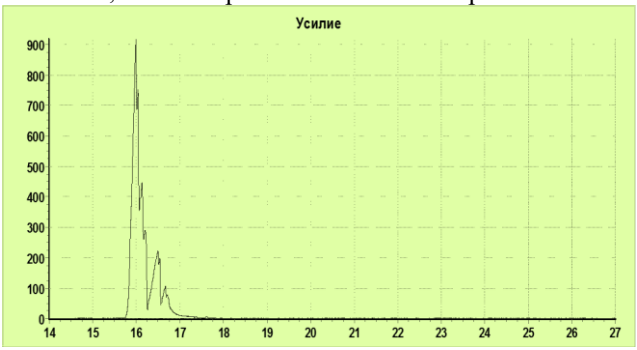


Рис.5. Скидання манекена головою вгору, довжина троса 2 М. Дистанція вільного падіння манекена – 4 М. Трос порвався.

Максимальне зусилля – 917,5 кг.

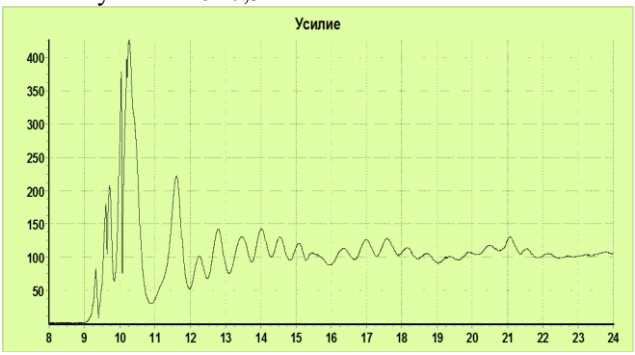


Рис.6. Скидання манекена догори ногами. Довжина троса 1 М. Точка скидання на рівні датчика. Дистанція вільного падіння манекена – 1 М. Кріплення троса на боці манекена. Страховка надірвалася - порвалися деякі шви, але манекен залишився висіти на страховці (див. рис. 3б). Гальмування розтягнуте за часом (на фронті основного сплеску кілька ривків), це пом'якшило удар. Максимальне зусилля – 425 кг.

КАЛІБРУВАЛЬНА СЛУЖБА ДП «УКРМЕТРТЕСТСТАНДАРТ»
CALIBRATION SERVICE OF THE SE «UKRMETRTESTSTANDART»

ДЕРЖАВНЕ ПІДПРИЄМСТВО
"ВСЕУКРАЇНСЬКИЙ ДЕРЖАВНИЙ НАУКОВО-ВИРОБНИЧИЙ ЦЕНТР СТАНДАРТИЗАЦІЇ, МЕТРОЛОГІЇ, СЕРТИФІКАЦІЇ ТА ЗАХИСТУ ПРАВ СПОЖИВАЧІВ"
(ДП "УКРМЕТРТЕСТСТАНДАРТ")
STATE ENTERPRISE "ALL-UKRAINIAN STATE RESEARCH AND PRODUCTION CENTER FOR STANDARDIZATION, METROLOGY, CERTIFICATION AND CONSUMERS' RIGHTS PROTECTION"
(SE "UKRMETRTESTSTANDART")

40004
Калібрування

СЕРТИФІКАТ КАЛІБРУВАННЯ
Calibration Certificate

Реєстраційний №: *UA/34/240207/000376*
Certificate number:

Дата калібрування: *07.02.2024 р.*
Date of calibration:

Об'єкт калібрування: *Система силовимірювальна*
Calibration object:

Виробник: *Інститут проблем моделювання в енергетиці ім. Г.Є.Пухова НАН України*
Manufacturer:

Тип: *Манекен 1.03*
Type:

Заводський/серійний номер: *01-2024*
Serial number:

Назва та адреса замовника: *ТОВ "ТЕСКО"*
The name and address of the customer: *03142, м. Київ, вул. В. Стуса, 35-37, Бізнес центр "Палладінський", оф. № 205*

Місце калібрування: *ДП «УКРМЕТРТЕСТСТАНДАРТ»*
Place of calibration:

Кількість сторінок сертифіката: *3*
Number of pages of the certificate:

В.о. начальника відділу №34 _____ **В.К. Коваль**
Acting Head of department №34 підпис/signature Ініціали, прізвище/name

М.П. **Дата** *07.02.2024 р.*
Official stamp *Date*

Б05-3.5ПР-1-U-6

Наведені в цьому сертифікаті результати вимірювань метрологічно простежуються до національних або міжнародних еталонів, які реалізують визначення одиниці вимірювань Міжнародної Системи Одиниць (SI). Калібрувальні та вимірювальні можливості, надані національними метрологічними інститутами чи призначеними інститутами, які були піддані процедурам взаємного аналізу в рамках угоди CIPM MRA, або калібрувальними лабораторіями, акредитованими органом з акредитації, що є підписантом угоди про взаємне визнання ILAC (ILAC MRA) або регіональних угод, визнаних ILAC.
Цей сертифікат видано Калібрувальною службою ДП «УКРМЕТРТЕСТСТАНДАРТ» відповідно до умов акредитації, наданих НААУ, які базуються на ISO/IEC 17025. НААУ є підписантом угоди з Європейською кооперацією з акредитації (EA) та угоди про взаємне визнання (ILAC MRA) з Міжнародною кооперацією з акредитації лабораторій (ILAC) за напрямком акредитації калібрувальних лабораторій.
Цей сертифікат калібрування може бути відтворене лише в повному обсязі, за винятком попереднього письмового дозволу Калібрувальної служби. Свідоцтво про калібрування без підписів і печатки не дійсне. Результати стосуються зразків, що були відкалібровані.

Given in this certificate measurement results are metrologically traceable to national or international standards, which realize the definition of measurement units of the International System of Units (SI). Calibration and measurement capabilities provided either by national metrology institutes and designated institutes that have been subject to peer-review processes under the CIPM MRA arrangement or by calibration laboratories that have been accredited by an accreditation body subject to the ILAC Mutual Recognition Agreement (ILAC MRA).
This certificate is issued by the Calibration Service of the SE "UKRMETRTESTSTANDART" in accordance with the accreditation conditions provided by NAAU based on ISO/IEC 17025. NAAU is a signatory to the agreement with the European co-operation for Accreditation (EA) and the agreement with the International Laboratory Accreditation Cooperation (ILAC) in the direction of accreditation of calibration laboratories.
This certificate may not be reproduced other than in full, except with the prior written approval of the issuing Calibration service.Calibration certificates without signature and stamp are not valid. The results relate only to the items calibrated.

Адреса: вул. Метрологічна, 4, м. Київ, 03143, Україна
Address: 4 Metrologichna str, 03143, Kyiv, Ukraine
Телефон/Phone: +38 (044) 526-52-29, факс/fax: +38 (044) 526-42-60, електронна адреса/e-mail: ukrcsm@ukrcsm.kiev.ua, сайт/website: www.ukrcsm.kiev.ua

[1] ДСТУ EN 355:2017 (EN 355:2002, IDT). Індіндивідуальне спорядження для захисту від падіння з висоти. – На заміну ДСТУ EN 355-2001. https://online.budstandart.com/ua/catalog/doc-page.

С.Я. Гільгурт, А.В. Ковилін

ЗАСТОСУВАННЯ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ В ЕНЕРГЕТИЧНИХ СИСТЕМАХ

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

Виявлення кіберзагроз та вчасне реагування на них – важлива функція кібербезпеки, метою якої є своєчасна ідентифікація потенційних загроз, що надає можливість реагувати на них до завдання шкоди інформаційним системам [1]. Традиційно системи кібербезпеки, засновані на сигнатурному методі, забезпечують більш чітке виявлення вторгнень та меншій відсоток хибних тривог (false positive) порівняно з конкуруючими рішеннями. Але у випадку захисту об'єктів критичної інфраструктури підвищений рівень відповідальності таких систем вимагає здатності виявляти нові загрози, швидко адаптуватися до змін в оперативному оточені та до появи нових підходів щодо здійснення кібератак [2]. З метою підвищення адаптивності та пришвидшення процесу виявлення потенційних загроз спеціалісти з безпеки комп'ютерних систем, дата-аналітики та дослідники звертаються до методів штучного інтелекту й машинного навчання, яки на сьогодні вважаються найбільш перспективними для вирішення даної задачі.

Використання алгоритмів машинного навчання (англ. Machine Learning – ML) для розробки систем виявлення вторгнень значно підвищило ефективність розпізнавання та ідентифікації потенційних загроз. Покращення моделей ML в сенсі підвищення точності розпізнавання та мінімізації хибних тривог є важливими викликами, які потрібно подолати під час розробки та використання систем виявлення кіберзагроз [3].

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

До поширених засобів виявлення кіберзагроз, що базуються на використанні ML, також відносяться методи контрольованого та неконтрольованого навчання (табл. 1). Вони передбачають навчання ML-моделей з використанням даних, попередньо підготовлених дата-аналітиком з використанням відповідного програмного забезпечення. Такі підходи також

можуть бути використані для виявлення закономірностей в поведінці інформаційних систем, логах мережевого трафіку та системних журналах [4].

Таблиця 1 – Переваги та виклики технік виявлення вторгнень на базі алгоритмів машинного навчання (ML)

Техніки виявлення підозрілої активності	Переваги	Виклики
Виявлення аномалій	Ефективно для ідентифікації невідомих загроз	Важко розрізнити позитивні та зловмисні аномалії
Контрольоване навчання	Висока точність у виявленні відомих загроз	Вимагає попередньо опрацьованих тренувальних даних
Неконтрольоване навчання	Ідентифікація невідомих загроз	Обмежена інтерпретація та пояснювальність

Для кожного підходу існують різні алгоритми ML виявлення підозрілої активності.

Виявлення аномалій:

– ***Isolation Forest***. Ефективний для ідентифікації аномалій, особливо в великих наборах даних;

– ***Autoencoders***. Використовуються у глибокому навчанні для виявлення аномалій шляхом реконструкції вхідних даних;

– ***DBSCAN***. Застосовується для кластеризації даних і виявлення точок даних, що вибиваються із загальних патернів.

Контрольоване навчання:

– ***Random Forest.*** Добре підходить для класифікації та виявлення відомих патернів вторгнення;

– ***Support Vector Machines (SVM).*** Ефективний для класифікації на наборах даних з чітко визначеними границями між класами;

– ***Logistic regression.*** Корисний для проблем бінарної класифікації.

Неконтрольоване навчання:

– ***K-means Clustering.*** Використовується для групування даних і виявлення аномальних кластерів;

– ***Principal Component Analysis (PCA).*** Дозволяє зменшити вимірність даних і виявлення нестандартних патернів;

– ***Gaussian Mixture Models (GMM).*** Базуються на щільності та використовуються для виявлення аномалій та незвичайних відхилень у розподілі даних.

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

В якості джерела даних було використано Windows Event Log. За

допомогою системи Sigma форматувалася та відфільтровувалася найбільш значуща інформація. Отриманий набір даних подавався в якості вихідних даних для аналізу моделлю. На виході було отримано наступні результати:

Anomalous Login Attempts


```
[
  {
    "timestamp": "2023-10-07 11:10",
    "EventID": "4625",
    "targetUserName": "User1",
    "status": "0xc000006d"
  },
  {
    "timestamp": "2023-10-07 11:11",
    "EventID": "4625",
    "targetUserName": "User1",
    "status": "0xc000006d"
  },
  {
    "timestamp": "2023-10-07 11:12",
    "EventID": "4625",
    "targetUserName": "User1",
    "status": "0xc000006d"
  },
  {
    "timestamp": "2023-10-07 11:13",
    "EventID": "4625",
    "targetUserName": "User1",
    "status": "0xc000006d"
  },
  {
    "timestamp": "2023-10-07 11:14",
    "EventID": "4625",
    "targetUserName": "User1",
    "status": "0xc000006d"
  },
  {
    "timestamp": "2023-10-07 11:15",
    "EventID": "4625",
    "targetUserName": "User2'",
    "status": " OR '1'='1",
    "__parsed_extra": [
      "0xc000006d"
    ]
  },
```


Detected SQL Injections


```
[
  {
    "timestamp": "2023-10-07 11:35",
    "EventID": "4625",
    "targetUserName": "Admin'",
    "status": " DROP TABLE users;--",
    "__parsed_extra": [
      "0xc000006d"
    ]
  }
]
```


Detected Phishing Attempts


```
[
  {
    "timestamp": "2023-10-07 11:50",
    "EventID": "4624",
    "targetUserName": "http://phishing.com",
    "status": "0x00000000"
  }
]
```


Normal Behaviour


```
[
  {
    "timestamp": "2023-10-07 11:00",
    "EventID": "4624",
    "targetUserName": "Administrator",
    "status": "0x00000000"
  },
  {
    "timestamp": "2023-10-07 11:05",
    "EventID": "4624",
    "targetUserName": "User1",
    "status": "0x00000000"
  },
  {
    "timestamp": "2023-10-07 11:25",
    "EventID": "4624",
    "targetUserName": "User2",
    "status": "0x00000000"
  },
  {
    "timestamp": "2023-10-07 11:40",
    "EventID": "4624",
    "targetUserName": "User3",
    "status": "0x00000000"
  }
]
```


Як можна побачити (рис. 1), дана модель відфільтрувала дані таким чином, що було виявлено наступну підозрілу активність: спроба користувачів отримати доступ до системи використовуючи логін, потенційну загрозу типу "Phishing", а також активність "SQL injection". Дуже важливо, що модель швидко адаптувалась та навчилась виявляти аномалії після отримання відносно невеликого набору даних порівняно з моделями контрольованого та неконтрольованого навчання [5].

Висновок. Використання систем виявлення потенційних кібератак має важливе значення та допомагає в забезпеченні безперебійної роботи об’єктів критичної інфраструктури. Результати проведеного дослідження свідчать, що моделі машинного навчання розширюють можливості дата-аналітиків та спеціалістів з безпеки комп'ютерних систем щодо виявлення підозрілої активності і вживання заходів з підвищення рівня захисту. З метою підвищення ефективності, швидкості та точності рекомендується своєчасно проводити збір даних щодо активності інформаційних систем (в т. ч. поведінки користувачів) і проводити навчання ML моделей.

Використання ML-підходів для протидії кібератакам є перспективним напрямом в найближчому майбутньому розвитку систем захисту інформації. Розвиток даного напряму надасть можливість підняти рівень захисту та

резильєнтності промислових систем, включаючи об’єкти критичної інфраструктури енергетичної галузі.

Рисунок 1 – Результати виявлення аномальної активності в системі

[1] Thakkar, A., & Lohiya, R. (2022). A survey on intrusion detection system: Feature selection, model, perfor-mance measures, application perspective, chal-lenges, and future research directions. Artificial Intelligence Review, 55(1), 453–563. https://doi.org/10.1007/s10462-021-10037-9

[2] Гільгурт С.Я. HPC та реконфігуровні засоби підвищення резильєнтності кіберфізичних систем // Живучість та резильєнтність критичної інфраструктури – 2023: Матеріали міжнародної науково-практичної конференції, м. Київ, 19 жовтня 2023. – К. : ІПМЕ ім. Г.Є. Пухова НАН України, 2023. – С. 11-14. https://ipme.kiev.ua/wp-content/uploads/2023/11/Матеріали_конференції_Survivability_ and_Resilience-2023-4.pdf

[3] Abiodun, O. I., Jantan, A., Omolara, A. E., Dada, K. V., Mohamed, N. A., & Arshad, H. (2018). State-of-the-art in artificial neural network applications: A survey. Heliyon, 4(11), e00938. https://doi.org/10.1016/j.heliyon.2018.e00938

[4] Afrifa, S., Varadarajan, V., Appiahene, P., Zhang, T., & Domfeh, E. A. (2023). Ensemble machine learning techniques for accurate and efficient detection of botnet attacks in connected computers. Eng, 4(1), 650-664; https://doi.org/10.3390/eng4010039

[5] Ковилін А.В. Використання моделей машинного навчання при аналізі логів Sigma для забезпечення резильєнтності об’єктів критичної інфраструктури., Безпека енергетики в епоху цифрової трансформації, V науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України : матеріали (Київ, 22 листопада 2023 р.). К. : ІПМЕ ім. Г.Є.Пухова НАН України, 2023. 152 с., https://doi.org/10.5281/zenodo.10531706

А.В. Давидюк

АКТИВНИЙ КІБЕРЗАХИСТ ДАТАЦЕНТРІВ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Датацентри є об'єктами критичної інфраструктури. Від роботи датацентрів залежить безперервність процесів клієнтів датацентру. Клієнтами датацентрів можуть бути державні організації, приватний бізнес, об'єкти критичної інфраструктури незалежно від форми власності. Порушення роботи датацентрів може призвести до значних матеріальних та нематеріальних збитків. Під час воєнного стану [1] датацентри України стали бажаними цілями для кібератак з боку противника.

Противник атакує як окремі ресурси ряду організацій, розміщених в датацентрах, так і саму інфраструктуру датацентру [2]. Одним з таких прикладів є кібератака на Датацентр «Парковий» в різний період часу.

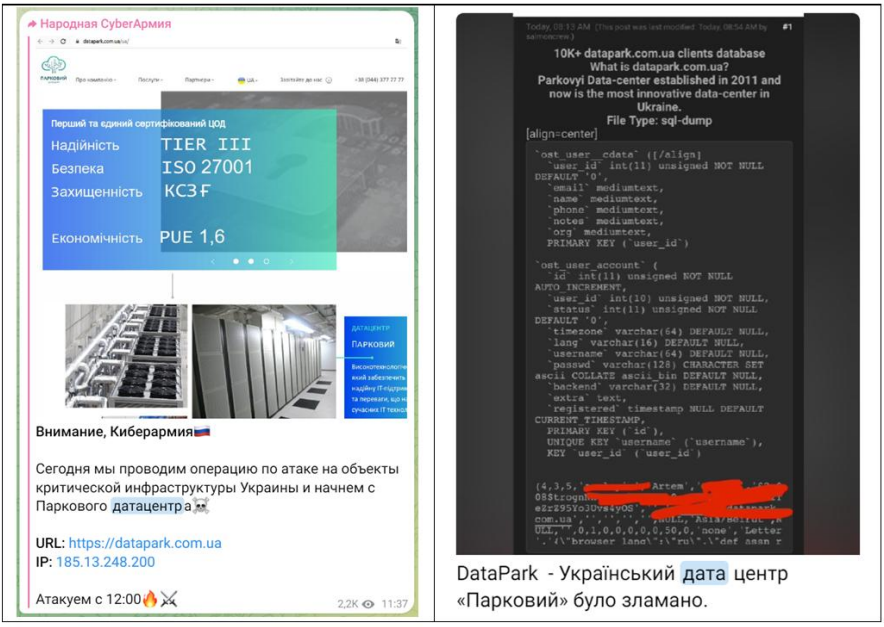


Рисунок 1 – Повідомлення про кібератаку на український датацентр «Парковий» [3, 4]

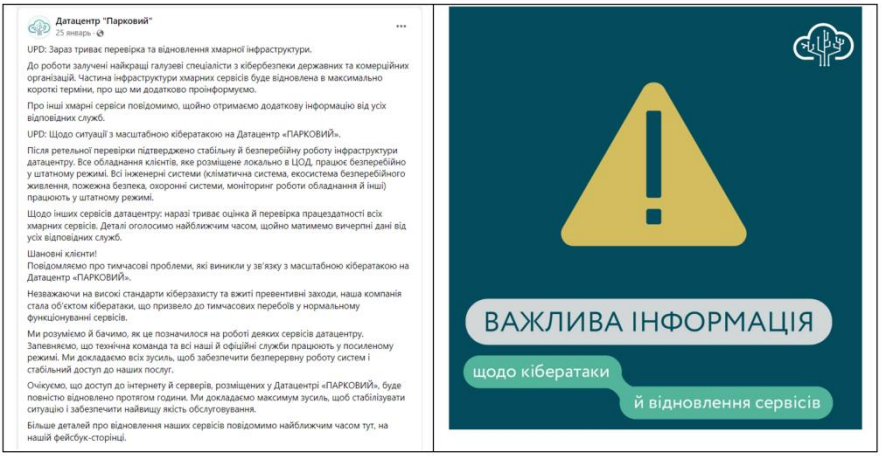


Рисунок 2 – Повідомлення про кібератаку на український датацентр «Парковий» [5]

Іншим прикладом атаки на ресурси клієнтів датацентрів є кібератака на ресурси ДСБТ Укртрансбезпеки, які забезпечують роботу прикордонної служби. Зокрема 28 червня, після 10 години за київським часом, були атаковані адреси: dsbt.gov.ua, сервер Системи «ШЛЯХ» - shlyah.dsbt.gov.ua, та eis.dsbt.gov.ua, сервер електронної пошти та документообігу ДСБТ. На початку атаки навантаження на ресурси датацентру зросло з 50 запитів/сек до 12 тис запитів/сек, а в пікові моменти доходило до 30 тис запитів/сек. Для захисту даних від несанкціонованого втручання та їх витоку було закрито доступ до Системи «ШЛЯХ», бази даних заявок на перетин кордону водіями «18 - 60», реєстрів Ліцензіатів та ТЗ, реєстру дозволів на міжнародні перевезення та реєстру поїздок ЄКМТ. Оскільки пропуск через державний кордон здійснюється з використанням Системи «ШЛЯХ», рух автотранспорту на міжнародних пунктах пропуску було ускладнено упродовж 6 годин [6].

Такі кібератаки здійснюються не тільки на датацентри в Україні, а й в світі. Зокрема був атакований датацентр «BALT NET». Таким чином загроза кібератак для датацентрів має глобальних характер.

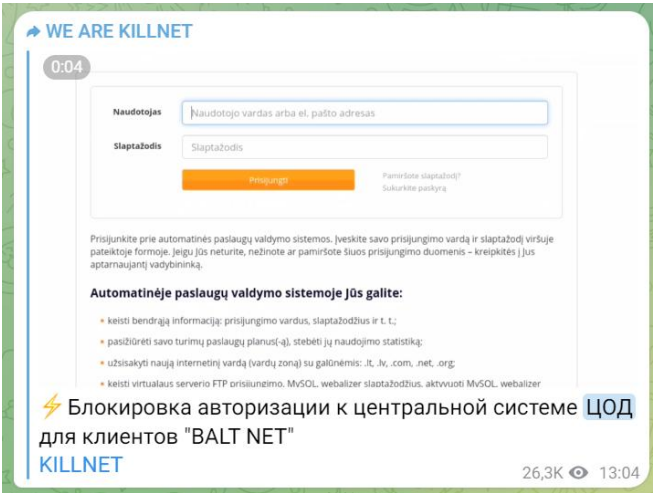


Рисунок 2 – Повідомлення про кібератаку на український датацентр «BALT NET» [7]

Водночас ресурси датацентрів використовуються противником для здійснення власних кібератак. Наявність ресурсів для кібератак всередині країни значно полегшує їх здійснення, так як блокування в рамках локального для країни сегменту мережі на багато складніше, ніж блокування трафіку з автономних систем іншої країни. Таким чином датацентри є середовищем для підготовки та здійснення кібератак.

Отже для датацентрів крім вирішення загальних проблем стійкості [8], важливим є забезпечення кібербезпеки інфраструктури датацентру, ресурсів клієнтів і недопущення використання датацентру для кібератак. Для захисту ресурсів клієнтів 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) [9]. Для забезпечення власної безпеки в датацентрах впроваджуються комплексні системи захисту інформації та системи управління інформаційною безпекою. Однак не зважаючи на досить високі вимоги до кібербезпеки датацентрів, високовартісне програмне та апаратне забезпечення, зловмисники знаходять способи для здійснення кібератак.

З розвитком технологій штучного інтелекту виникає можливість створення нових концепцій та технологій кіберзахисту [10]. Найбільш популярним є застосування штучного інтелекту для моніторингу кіберінцидентів, аналізу поведінки та сигнатур шкідливого програмного забезпечення [11]. Однак технічно є можливим використання штучного інтелекту для здійснення кібератак [12]. Кібератаки крім використання у зловмисних цілях можуть бути превентивними заходами з метою зниження спроможностей протиника для кібератак. Таким чином виникає питання

використання штучного інтелекту, що здатен атакувати противника у відповідь, використовуючи значні ресурси датацентру, що імовірно значно переважатимуть можливості противника. Законодавчі аспекти даного варіанту використання не розглядатимуться в даній публікації, так як є предметом окремої дискусії і буде розглянуто в наступних публікаціях. Водночас таке використання штучного інтелекту значно вплине на аналіз ризиків та безпеку датацентру. Зокрема противник атакуючи датацентр, не може передбачити завчасно, якої потужності кібератака і на який ресурс буде здійснена під управлінням штучного інтелекту, зокрема і які наслідки вона матиме для його країни і нього особисто. Наявність такої технології може значно змінити підходи до кіберзахисту від концепції захисту до концепції превентивної постійної загрози. Подібний вплив на середовище кіберпростору може значно вплинути на кіберзахист критичної інфраструктури і державних інформаційних ресурсів в тому числі. Звісно, в такому підході існує ризик хибного спрацювання або емуляції противником, але це питання якості навчання нейромереж і критерії прийняття рішень.

З огляду на зазначене, впровадження процесів активного кіберзахисту на основі штучного інтелекту для захисту датацентрів може стати виправданим заходом з урахування важливості стійкості [8] та безпеки датацентрів в умовах підвищених загроз воєнного стану [13].

[1] Про затвердження Указу Президента України "Про продовження строку дії воєнного стану в Україні", Закон України № 3564-IX (2024) (Україна). https://zakon.rada.gov.ua/laws/show/3564-20#Text

[2] Тарасовський, Ю. (2024, 26 січня). Кібератака на дата-центр «Парковий». компанія обіцяє відновити повний доступ до даних протягом 48 годин — forbes.ua. Forbes.ua | Бізнес, мільярдери, новини, фінанси, інвестиції, компанії. https://forbes.ua/news/kiberataka-na-data-tsentr-parkoviy-kompaniya-obitsyae-vidnoviti-povniy-dostup-do-danikh-protyagom-48-godin-26012024-18812

[3] @CyberArmyofRussia_Reborn. (2022, 17 жовтня). Внимание, Киберармия□□ Сегодня мы проводим операцию по атаке на объекты критической инфраструктуры Украины и начнем с Паркового датацентра [Долучено зображення] [Допис]. https://t.me/c/1552656714/4867

[4] @salmoncrew. (2024, 25 січня). datapark.com.ua datacenter database & more than 15Tb data [Долучено зображення] [Допис]. https://breachforums.cx/Thread-datapark-com-ua-datacenter-database-more-than-15Tb-data?highlight=Parkovyi

[5] UPD: Зараз триває перевірка та відновлення хмарної інфраструктури [Оновлення статусу]. (2024, 25 січня). https://www.facebook.com/ParkovyiDC/posts/837530208174316/?paipv=0&eav=AfYe06AMHnI_wBNYg8CaJvprF5kRdBT5JRDpelpmPUiKpbvRsDckm_4TmiYkMs_XJWA&_rdr

[6] Interfax-Ukraine. (2022, 29 червня). "Укртрансбезпека" заявляє про атаку російських хакерів і плани відновити роботу найближчим часом. Інтерфакс-Україна. https://interfax.com.ua/news/general/842355.html

[7] @WE ARE KILLNET. (2022, 28 червня). Блокировка авторизации к центральной системе ЦОД для клиентов "BALT NET" [Post_verbose]. https://t.me/c/1552656714/2048

[8] Davydiuk, A. (2023). The assessment of data center resilience. У Інформаційні технології та безпека (с. 112–117).
[9] Про хмарні послуги, Закон України № 2075-IX (2023) (Україна). https://zakon.rada.gov.ua/laws/show/2075-20#Text
[10] Dulloo, R., Suryawanshi, V., Kailas Mokal, D., & Rajendra Hagare, S. (2023). AI in cyber security: Decision support and smart methods. Journal of the Asiatic Society of Mumbai, Vol. 97(No.01 (I) 2023), 118–128. https://www.researchgate.net/publication/379053485_AI_IN_CYBER_SECURITY_DECISION_SUPPORT_AND_SMART_METHODS
[11] Beg, O., Khan, A., Rehman, W., & Hassan, A. (2023). A review of ai-based cyber-attack detection and mitigation in microgrids. Energies, 16(22), 7644. https://doi.org/10.3390/en16227644
[12] Truong, T. C., Diep, Q. B., & Zelinka, I. (2020). Artificial intelligence in the cyber domain: Offense and defense. Symmetry, 12(3), 410. https://doi.org/10.3390/sym12030410
[13] Давидюк, А. В. (2023). Забезпечення безпеки даних датацентрів в умовах воєнного стану. У Збірник матеріалів XLI науково-технічної конференції молодих вчених та спеціалістів інституту проблем моделювання в енергетиці ім. Г.Є. пухова НАН україни (с. 139–140).

Н.В. Заїка, М.Ю. Комаров, Д.В. Ковалик

ВИКОРИСТАННЯ БПЛА ЯК ЕЛЕМЕНТ ТЕХНІЧНОГО ЗАХИСТУ НА ПІДПРИЄМСТВАХ ТА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Захист критичної інфраструктури стає одним із важливих завдань держави, оскільки постійно присутній вплив різних загроз, що можуть призвести до порушення її роботи, втрати ресурсів, та завдати збитків громадянам і державі в цілому [1]. Ефективний захист критичної інфраструктури передбачає комплексний підхід, який враховує різноманітні сценарії і використовує інноваційні технології. Сучасні заходи кібербезпеки включають технічні засоби моніторингу та аналізу стану об'єктів за допомогою безпілотних літальних апаратів [2].

Традиційні системи безпеки можуть бути ефективними в деяких випадках, проте вони також супроводжуються низкою проблем, які можуть знизити їх ефективність і ускладнити процес обслуговування. Традиційні системи безпеки часто схильні до помилкових тривог, що можуть виникати з різних причин, таких як зовнішні умови або людські помилки. Розслідування помилкових тривог може бути дорогим і трудомістким, а також може призвести до втрати довіри до системи безпеки. Крім того, традиційні системи безпеки можуть бути недостатньо гнучкими, щоб адаптуватися до змінних вимог безпеки або змін у середовищі. Наприклад, системи відеоспостереження можуть бути неефективними при поганих умовах освітлення або в екстремальних погодних умовах, або вони можуть не мати достатньої роздільної здатності, тоді як охоронці можуть бути погано підготовлені або не мати необхідного обладнання для реагування на конкретні загрози [3].

Додатково, у порівнянні зі статичними датчиками спостереження, які можуть бути ідентифіковані та обійдені зловмисниками через проведення кібератак через канали підключення до камер та датчиків або передачу фальшивої інформації, безпілотні літальні апарати (БПЛА) отримують перевагу від свого унікального розташування та мобільності.

Автоматизовані системи контролю периметра та віддаленого відеоспостереження зменшують потребу у людських ресурсах на місці і пов'язані з цими витратами. Критична інфраструктура, така як очисні споруди води, комунікаційні мережі та електромережі, потребує захисту периметру для запобігання саботажу та кібератак.

Станція базування БПЛА може змінювати сектори спостереження, захисту та безпеки. Традиційні методи безпеки виникають із проблемами, такими як обмежена обізнаність про ситуацію, потреба у працівниках та обмежені можливості реагування. Використання БПЛА для мобільного відеоспостереження дозволяє швидко охоплювати великі території, збільшує тактичну перевагу та може бути розгорнуто за потребою. Передача даних в

режимі реального часу з БПЛА сприяє прийняттю обґрунтованих рішень для покращення реакції на інциденти та забезпечення безпеки екіпажу.

Використання інноваційних технологій у промислових та енергетичних об'єктах критичної інфраструктури [4] з метою забезпечення безпеки охоплює ряд заходів, включаючи розширений робочий діапазон, дистанційне та автоматизоване обслуговування техніки, зарядку акумуляторів та додаткове налаштування автопілоту для автономної роботи, а також модернізацію обладнання за допомогою різноманітних датчиків (включаючи широкий, зум, лазерний далекомір та теплові) для збору різноманітних даних. Збір даних у реальному часі з живими трансляціями, які можуть бути переглянуті віддалено або персоналом на землі, також є важливою складовою.

Використання додаткового лазерного далекоміра для отримання точних координат місця або об'єкта, а також термодатчика для пошуку людей або об'єктів, відкриває нові можливості для забезпечення безпеки. Сучасне програмне забезпечення може додатково розширити функціональні можливості безпеки для обраного об'єкту, зокрема, налаштовувати автопілот на запрограмовані маршрути патрулювання [5]. Незалежно від того, чи ставиться завдання реагування на надзвичайні ситуації або проведення планових патрулів, безпека на великих об'єктах може бути викликом, який часто потребує значних людських та фінансових ресурсів для забезпечення ефективного покриття.

Проблеми традиційних систем безпеки, такі як обмежена обізнаність про ситуацію, вразливість до втручання та обмежені можливості реагування, можуть бути розв'язані за допомогою вищезазначених інноваційних рішень. Використання безпілотників дозволяє отримувати доступ до важкодоступних або небезпечних місць без ризику для життя людей. Такі дії сприяють підвищенню обізнаності про ситуацію та забезпеченню швидкого та адекватного реагування на будь-які загрози або події.

Це може допомогти групам безпеки залишатися в курсі будь-яких потенційних загроз або інцидентів, дозволяючи їм швидко та належним чином реагувати. Безпілотники можуть отримати доступ до важкодоступних місць або місць з високим ризиком, не наражаючи на життя людей. Поточні операції безпілотників стикаються з низкою проблем, серед яких: Вартість праці пілотних команд та Потреба у високих навичках експлуатації бпла.

Разом з питаннями забезпечення технічного захисту інформації на об’єктах інформаційної діяльності, безпеки інформаційних і комунікаційних систем критичної інфраструктури – кібербезпека потребує постійного удосконалення методів, механізмів та складових її забезпечення [6], включаючи інноваційні технології та підвищення кваліфікації працівників у використанні та обслуговуванні БПЛА.

Усі ці можливості допомагають персоналу служб безпеки приймати обґрунтовані рішення на основі наявних даних, що сприяє збереженню безпеки та цілісності активів та персоналу.

[1] Державна система захисту критичної інфраструктури в системі забезпечення національної безпеки: аналіт. доп. / за ред. О. М. Суходолі. Київ: НІСД, 2020. 28 с.

[2] Євсєєв В. О. Можливі шляхи удосконалення захисту критичної інфраструктури України з урахуванням світового досвіду. Збірник наукових праць ХНУПС. 2016. № 4. С. 168-172.

[3] Автономний охоронний дрон. URL: https://www.heliguy.com/blogs/posts/drone-in-a-box-for-security (дата звернення: 10.05.2024).

[4] Захист критичної інфраструктури в умовах надзвичайних ситуацій / за заг. ред. П. Б. Волянського. Київ : НІСД, 2021. 375 с.

[5] Автономний охоронний дрон. URL: https:// sunflower-labs.com (дата звернення: 06.04.2024).

[6] Грищук Р., Охрімчук В. Постановка наукового завдання з розроблення шаблонів потенційно небезпечних кібератак // Безпека інформації. 2015, Т. 21. №3. С. 301-308.

Д.А. Коваль

МАТЕМАТИЧНА МОДЕЛЬ ДЛЯ ЧИСЛОВИХ РОЗРАХУНКІВ ЕЛЕКТРОМАГНІТНИХ ТА ЕЛЕКТРОМЕХАНІЧНИХ ПЕРЕХІДНИХ ПРОЦЕСІВ В СХЕМІ ГЕНЕРАЦІЇ ТА ВИДАЧІ ПОТУЖНОСТІ АЕС

Для забезпечення оперативного обчислення параметрів перехідних процесів з аналізом поведінки пристроїв РЗА розроблено повну (у трифазному виконанні) математичну модель схеми генерації та видачі потужності АЕС з врахуванням роботи АРЗ синхронних генераторів та регуляторів парових турбін, також враховано насичення сталі синхронних генераторів та силових трансформаторів (при моделюванні процесів поштовхів струмів намагнічування).

Метатична модель виконана шляхом реалізації числового методу розв'язування систем диференційних рівнянь (в даному випадку – метод Гіра), що дає змогу отримувати числові ряди значень необхідних величин перехідного процесу, зберігати їх у форматі COMTRADE з можливістю перевірки і порівняння з осцилограмами реальних перехідних процесів. Такий функціонал дозволяє моделювати задані перехідні процеси для генерування завдань перевірочними пристроями типу РЗА-Тестер, OMICRON та інші. Виконання моделі як повної трифазної дозволяє змоделювати складні перехідні процеси, на кшталт увімкнення блокових трансформаторів на шини ВРУ, на які працює один синхронний генератор в режимі живлення власних потреб. Це дозволяє оцінити вплив пускових струмів силового трансформатора і можливу поведінку пристроїв РЗА (зміна величини напруги, хитання генератора, дія АРЗ).

Для даної математичної моделі виконано ряд верифікаційних дослідів:

1. Моделювання стану синхронних генераторів АЕС і порівняння з виміряними даними записаними аварійними осцилографами внаслідок близького до шин ВРУ-330 однофазного короткого замикання ф. А на землю. В даному верифікаційному досліді продемонстровано врахування фазового зміщення напруг вузлом поперечного регулювання АТ-330/750 кВ та трансформатора поперечного регулювання (рис. 1);

2. Моделювання стану синхронних генераторів енергоблоку з реакторною установкою ВВЕР-440 при відключенні енергоблоку від шин ВРУ-330 кВ з перходом на живлення власних потреб і порівняння з виміряними даними записаними аварійними осцилографами при виконанні відповідних дослідів. В даному верифікаційному досліді продемонстровано деталізацію моделювання АРЗ синхронних генераторів (рис. 2);

3. Моделювання стану синхронного генератора типу ТВВ-1000 при асинхронному ході обумовленому втратою збудження (рис. 3 та 4).

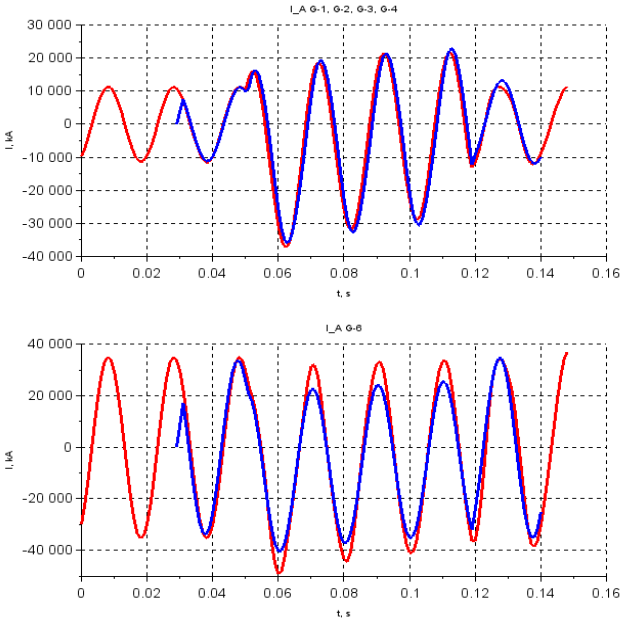


Рисунок 1 – Струми синхронних генераторів ТВВ-220 (увімкнені на шини ВРУ-330 кВ) та ТВВ-1000 (увімкнений на шини ВРУ-750 кВ).

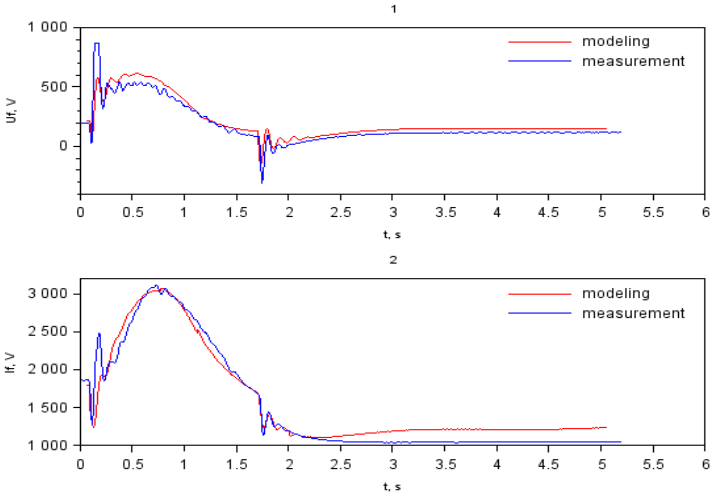


Рисунок 2 – Напруга (1) та струм (2) ротора одного з синхронних генераторів енергоблоку ВВЕР-440 при виконанні досліду вимкнення блоку на стороні 330 кВ

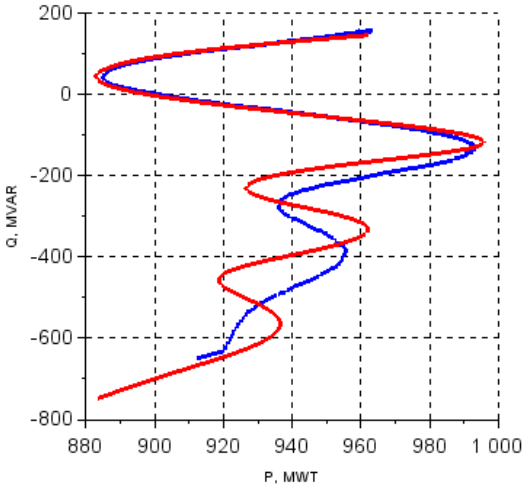


Рисунок 3 – Діаграма потужності синхронного генератора типу ТВВ-1000 при асинхронному ході (червона лінія – модельоване значення, синя – записи осцилографа)

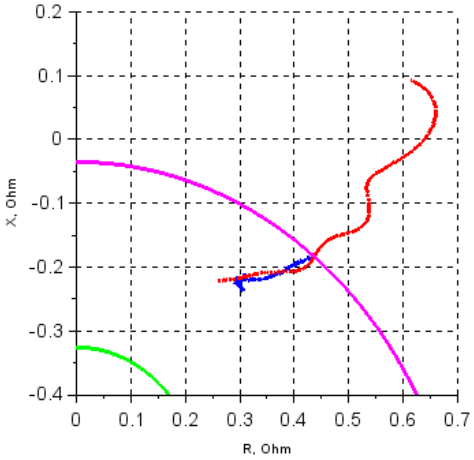


Рисунок 4 – Рух годографа опору ф. А при асинхронному ході синхронного генератора типу ТВВ-1000 (червона лінія – модельоване значення, синя – записи осцилографа)

Дана математична модель використовується на підприємстів як тренажерна система, яка дозволяє персоналу оцінити вплив уставок пристроїв РЗА та АРЗ на роботу електротехнічного обладнання. Також дана модель дозволяє аналізувати перехідні процеси та виконувати імітаційне моделювання з ціллю отримання інформації про стан обладнання при ліквідації аварійних ситауцій (на кшталт повного знеструмлення шин ВРУ

АЕС).

Як приклад імітаційного моделювання було виконано розрахунок стану синхронного генератора типу ТВВ-1000 при виконанні операції подавання напруги на вузол АТ-330/750 кВ з шин генератора при умові повного знеструмлення шин ВРУ-750 кВ і 330 кВ (рис. 5).

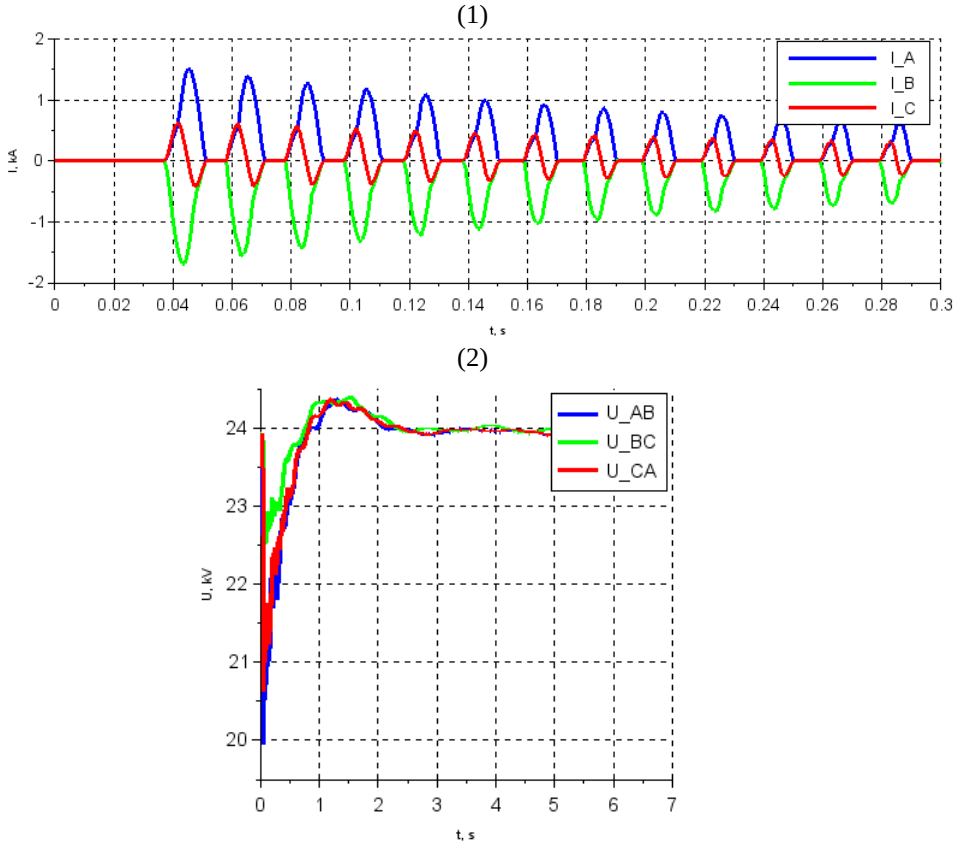


Рисунок 5 – Струми намагнічування АТ-750/330 кВ (1) та графік зміни напруг на шинах генератора (2) при виконанні операції подавання напруги на АТ.

О.О. Огір

ЕВОЛЮЦІЯ МЕТОДІВ ФОРМУВАННЯ АКУСТИЧНИХ ЗОБРАЖЕНЬ ДЕФЕКТІВ У СКАНОВАНИХ СЕРЕДОВИЩАХ: АНАЛІЗ ТА ПЕРСПЕКТИВИ ВИКОРИСТАННЯ СУЧАСНИХ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ

Ефективна стратегія застосування нейронно-мережевого підходу: Однією з ключових задач є розробка ефективної стратегії використання нейронно-мережевого підходу. Нейронні мережі можуть бути застосовані для аналізу акустичних зображень та виявлення дефектів у сканованих середовищах. Наприклад, з використанням згорткових нейронних мереж можна здійснювати аналіз зображень у реальному часі, що є важливим для діагностики. Тип та метод навчання штучної нейронної мережі: Для досягнення оптимальних результатів необхідно обрати відповідний тип та метод навчання штучної нейронної мережі. Наприклад, для аналізу акустичних зображень можуть бути використані різні архітектури нейронних мереж, такі як згорткові нейронні мережі (CNN) або рекурентні нейронні мережі (RNN), залежно від специфіки задачі та об'єму доступних даних. Метод навчання нейронних мереж для використання в задачах обробки оперативної інформації: Оскільки в деяких випадках може бути необхідно обробляти інформацію в реальному часі, важливо розробити методи навчання нейронних мереж, які дозволяють працювати з оперативною інформацією. Наприклад, можуть бути використані методи навчання з підсиленням або методи онлайн-навчання, які дозволяють моделі швидко адаптуватися до змінних умов та навчатися на ходу. Для кращого розуміння, розглянемо конкретний приклад застосування нейронних мереж у виявленні дефектів на акустичних зображеннях. Наприклад, у медичній діагностиці зображення ультразвукових сканів може містити різні аномалії та патології, такі як пухлини або кісти. Використання нейронних мереж дозволяє автоматично виявляти ці аномалії на зображеннях, підвищуючи точність та швидкість діагностики.

Таким чином, розробка та оптимізація нейронно-мережевих підходів у виявленні дефектів на акустичних зображеннях є важливою та актуальною задачею, що потребує комплексного підходу та використання сучасних технологій у галузі машинного навчання та обробки сигналів. Останнім часом спостерігається зростання обсягу інформації, яка перетворюється, передається та обробляється у цифровому форматі. Це зростання пов'язане з широким використанням цифрових технологій у науці, техніці та повсякденному житті. Це створює потребу у постійному вдосконаленні алгоритмів та методів обробки цієї інформації. Розв’язання задач кластеризації та класифікації, а також кодування і стискання зображень стають все більш актуальними. Ці завдання потребують обробки великих обсягів даних у реальному часі. Оскільки ці задачі зазвичай мають складну

структуру, традиційні методи їх розв'язання часто неефективні. Тому в багатьох випадках доцільним є використання нейронних мереж. Для цього потрібно вибрати відповідний тип мережі та налаштувати її параметри за допомогою алгоритму навчання, що мінімізує обраний функціонал похибки.

Серед великої кількості існуючих штучних нейронних мереж широке застосування в задачах обробки зображень знайшли штучні нейронні мережі статичного типу, такі як багатошаровий персептрон, радіально-базисні мережі, мапи Кохонена та інші. Однак на останній час динамічні штучні нейронні мережі, зокрема ті, які базуються на теорії адаптивного резонансу (ART), здобули значну увагу дослідників. Незважаючи на значні теоретичні відомості про властивості цих мереж та їх потенційне застосування в обробці зображень, наразі відсутні загальні рекомендації стосовно їхнього практичного використання для конкретних завдань.

Тому актуальною стає науково-технічна проблема розробки ефективних методів обробки оперативної інформації на основі штучних нейронних мереж, методів навчання мереж для розв'язання задач кластеризації, класифікації та обробки зображень, а також методів підвищення швидкості навчання мереж та оптимізації їх роботи.

На світовому рівні розробки методів навчання нейронних мереж для використання в задачах обробки оперативної інформації, зокрема реконструкції діагностичних зображень, спостерігається значний прогрес і активні дослідження. Одним із ключових напрямків досліджень є використання глибокого навчання для вирішення завдань з обробки медичних зображень. Зокрема, вчені працюють над розробкою та оптимізацією нейронних мереж, спроможних ефективно відновлювати та реконструювати діагностичні зображення з мінімальним рівнем шуму та артефактів. У цьому контексті використовуються різноманітні архітектури глибоких нейронних мереж, такі як згорткові нейронні мережі (CNN), автокодери, генеративно-зіставні мережі (GAN) та їх варіації. Ці методи дозволяють враховувати складні простори високорозмірних даних зображень та ефективно впроваджувати механізми адаптації та оптимізації для досягнення бажаного результату.

Одним із важливих викликів у цій області є забезпечення стабільної та надійної реконструкції діагностичних зображень навіть при обмежених обсягах вхідних даних або у разі наявності шуму та артефактів. Тому в дослідженнях активно досліджуються методи аугментації даних, регуляризації моделей та використання відповідних функцій втрат для забезпечення стійкості та високої точності відновлення зображень[1].

Крім того, важливою є інтеграція таких моделей в клінічну практику та забезпечення їхньої валідації на великих клінічних датасетах. Це вимагає виконання широкомасштабних досліджень, що охоплюють різноманітні медичні установи та враховують специфічні вимоги щодо конфіденційності та безпеки обробки медичних даних.

Загалом, розробки методів навчання нейронних мереж для використання в задачах обробки оперативної інформації, зокрема реконструкції

діагностичних зображень, є активною та перспективною галуззю досліджень, яка має потенціал значно покращити якість та доступність медичних послуг у майбутньому. Україна в останні роки активно розвивається у сфері наукових досліджень, зокрема в області штучного інтелекту та медичної обробки зображень[2]. Національний технічний університет України "Київський політехнічний інститут" виступає як один із центрів у цій сфері. Він має науково-дослідні лабораторії з комп'ютерного бачення та обробки зображень, які активно займаються розробкою методів навчання нейронних мереж для реконструкції діагностичних зображень.

Крім того, українські університети, які спеціалізуються на обробці сигналів та медичній інженерії, такі як Львівський політехнічний університет, Національний університет "Львівська політехніка", Товариство інтелектуальних систем та технологій (TICT), також можуть вносити вагомий внесок у дослідження у цій області.

Світові лідери:

1. Массачусетський технологічний інститут (MIT): Цей університет є центром високих технологій і відомий своїми передовими дослідженнями в галузі штучного інтелекту, включаючи медичну обробку зображень.
2. Стефанс технічний університет (ETH Zurich): Університет має відділ медичного обробки зображень та комп'ютерного зору, який відомий своїми дослідженнями в області обробки медичних зображень.
3. Стенфордський університет: Стенфорд є одним із світових лідерів у вивченні штучного інтелекту та медичних дослідженнях, включаючи обробку медичних зображень.
4. Університет Оксфорду: Він також відомий своїми дослідженнями в галузі медичних наук та застосуванні штучного інтелекту в медицині.
5. Університет Торонто: Університет Торонто також відомий своїми дослідженнями в області медичних технологій та комп'ютерного зору.

І в заключенні можна сказати, що ефективне використання нейронно-мережевого підходу є ключовим у виявленні дефектів на акустичних зображеннях, зокрема у медичній діагностиці. Вибір відповідного типу та методу навчання нейронної мережі є критичним для досягнення оптимальних результатів, особливо в умовах реального часу. Дослідження та розвиток цих методів є активною галуззю, яка відкриває нові перспективи в медичній та технічній сферах.

[1] Огір О.О. – Принципи діагностичної візуалізації об’єкта або середовища. // Фаховий науковий журнал «Вчені записки Таврійського національного університету» імені В. І. Вернадського. Серія: Технічні науки. Том 32 (71) № 6, 2021. - С. 105–117

[2] Огір О.О. Дослідження ефективності алгоритмів та конфігурацій нейромереж у вирішенні задачі оптимізації якості діагностичних зображень. https://archive.interconf.center/index.php/conference-proceeding/article/view/3878

А.О. Лєпатьєв

ОПИС РОБОЧОЇ ДІЯЛЬНОСТІ РОЗРОБКИ ТРЕНАЖЕРНИХ ЗАНЯТЬ ДЛЯ ОПЕРАТИВНОГО ПЕРСОНАЛУ ПІДПРИЄМСТВ РОЗПОДІЛЬЧИХ МЕРЕЖ

Сучасні інструменти розробки застосунків відкривають нові можливості для підвищення ефективності розробки тренажерних занять для оперативного персоналу підприємств розподільчих мереж. В якості інструменту для розробки занять був вибраний інструмент Unity. Unity дозволяє спроєктувати тренажерне заняття в якості комп'ютерної гри, де користувач має виконати певні послідовні дії для успішного проходження тренажерного заняття. Як і в комп'ютерних іграх, користувач може пройти заняття не успішно, якщо не вкладеться в попередньо заданий час, або перевищить кількість дозволених помилок під час проходження заняття.

Для полегшення роботи непрограмуючих спеціалістів, які конструюють тренажерні заняття, всі компоненти зроблені у вигляді префабів[1]. Префаб - це особливий тип набору(будь-який предмет, який можна використати у проєкті Unity)[2], що дозволяє зберігати весь ігрових об'єктів з усіма компонентами та значеннями властивостей. Префаб виступає в ролі шаблону для створення екземплярів об'єкта, що зберігається в сцені. Будь-які зміни в префабі негайно відображаються і на всіх його екземплярах, при цьому не можна перевизначати компоненти, але є можливість налаштувати кожний екземпляр окремо.

Першим кроком для створення тренажерного заняття за допомогою шаблону тренажера виконання бланка перемикань є створення проєкту. У вікні створення проєкту Unity необхідно вибрати: тип проєкту(2D, 3D чи 2D UPR(Universal Render Pipeline)); назву проєкту; директорію на запам'ятовувальному пристрої, де буде зберігатись проєкт.

Після створення проєкту та визначення його типу необхідно додати зображення в проєкт Unity. В проєкт додаються зображення об'єктів мережі, приміщень підстанцій тощо. Зазвичай все зображення, які використовуються в проєкті додаються в папку Assets -> Textures. В разі необхідності редагування зображення, можна використати будь який графічний редактор, оскільки Unity не має вбудованого редактору зображень. Редактор зображення може бути використаний для створення умовного зображення приміщення об'єктів чи приміщень підстанцій, у випадку заборони фотографування справжніх об'єктів чи приміщень.

Наступним кроком є створення сцени в середовищі. Сцени містять ігрові об'єкти. Вони можуть використовуватися для створення головного меню, окремих рівнів та інших цілей. Кожен файл сцени можна вважати окремим ігровим рівнем. У кожній сцені можна розмістити об'єкти оточення, загородження, декорації, шматочками створюючи дизайн і саму гру. Кожне окреме приміщення підстанції яке використовується під час тренажерного

заняття має мати окрему сцену в проєкті Unity.

Після створення сцени необхідно створити спрайт заднього фону сцени. Спрайти — це 2D-графічні об'єкти, які додаються на сцену. Для налаштування спрайту необхідно вибрати з вікна сцени Hierarchy екземпляр ігрового об’єкта, який відповідає за задній фон(в шаблоні цей об’єкт має назву Background). У вікні Inspector екземпляру необхідно знайти компонент Sprite Renderer, і в цьому компоненті знайти пункт Sprite. Спеціалісту під час вибору зображення буде представлений список з зображень, які є доданими у проєкт. Після вибори необхідного зображення вона миттєво з’явиться на сцені.

У випадку, якщо додана сцена є не першою в проєкті, необхідно додати на сцену екземпляр префабу кнопки повернення на попередню сцену(в шаблоні має назву Previous Button). Після додання екземпляра префаба на сцену необхідно задати номер індексу попередньої сцени. Індекси сценам присвоюються автоматично програмним шляхом. Чим пізніше сцену додали в проєкт, тим номер індексу буде більшим. Щоб переглянути індекси необхідно відкрити вікно Build Setting в редакторі Unity.

Якщо на зображені заднього фону сцени є об’єкти, завдяки яким можна перейти в інше приміщення, чи в об’єкт(двері в інше приміщення, кришки для панелей так пультів), то на ці об’єкти необхідно розмістити навігаційну кнопку, яка перенесе користувача на в інші територію робочої зони обхідника. Заповнення даних для екземплярів префабів цього компоненту відбувається аналогічно заповненню даних для кнопки повернення на попередню сцену.

Після налаштування навігації необхідно додати та налаштувати кнопки дії. Кнопки дії розміщуються поверх об’єктів які змінюють режим мережі(кнопки на об’єктах мережі, вимикачі, роз’єднувачі, кола управління і т.д.). Після того, як користувача натисне лівою кнопкою миші на кнопку дії зміниться зріз чи зрізи, заднього фону нинішньої сцени або задні фони інших сцен, які змінять режим. Новий зріз буде відображати нові дані, які відбулись після зміну режиму. Також, у вікні Inspector можна налаштувати: перехідні зрізи(коли кнопка знаходиться в натиснутому стані), порядок натискання кнопок(якщо кнопка дії буде натиснута не послідовно, то така дія буде зарахована як помилка), зміна кольору чи візуального виду при наведенні курсора на кнопку.

[1] Unity - Manual: Prefabs. (б. д.). Unity - Manual: Unity User Manual 2022.3 (LTS). https://docs.unity3d.com/Manual/Prefabs.html

[2] Unity - Manual: Asset Workflow. (б. д.). Unity - Manual: Unity User Manual 2022.3 (LTS). https://docs.unity3d.com/560/Documentation/Manual/AssetWorkflow.html

Ю.А. Матвєєва, Е.І. Богдан

ВПЛИВ ДІДЖИТАЛІЗАЦІЇ НА ВПРОВАДЖЕННЯ ПРИНЦИПІВ БЕЗВУГЛЕЦЕВОЇ ЕКОНОМІКИ[1]

У сучасних світових технологіях та цифрових трансформаціях вплив діджиталізації на екологічні проблеми стає все більш значним. На сьогодні цифрові технології переплітаються з усіма аспектами нашого життя, змінюючи парадигми та динаміку економічного розвитку. Впроваджуючи діджиталізацію в концепцію економіки з нульовим викидом вуглецю, світ стоїть на порозі нової ери, де взаємодія між цифровими інноваціями та екологічною стійкістю визначає нові стандарти успіху.

Впровадження цифрових технологій в концепцію економіки з нульовим викидом вуглецю визначає початок нової епохи розвитку. Взаємодія між цифровими інноваціями та екологічною стійкістю встановлює нові критерії успіху, що формуються у сучасному світі.

Необхідно зазначити, що наукові дослідження в контексті визначення впливу діджиталізації на розвиток низьковуглецевої економіки набувають все більшої актуальності. Так, згідно БД Scopus нами була визначена динаміка кількості документів по роках за ключовими словами digital AND low-carbon AND economy, яка відображає значний ріст праць за останні роки, рис.1.

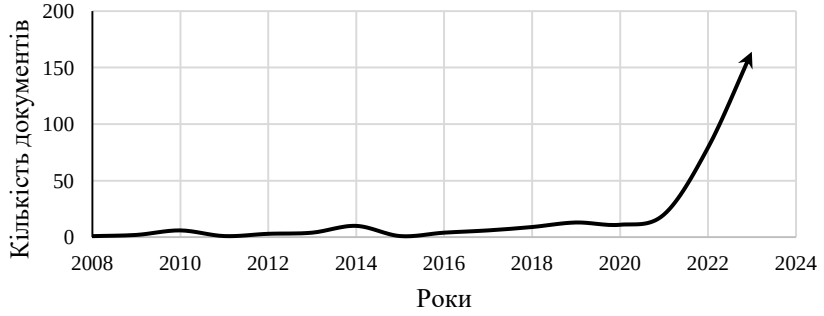


Рисунок 1 – Динаміка кількості документів по роках за ключовими словами digital AND low-carbon AND economy на базі використання БД Scopus

У 2008-2016 роках кількість документів коливалась від 1 до 10 в рік. Однак, починаючи з 2017 року, спостерігається позитивна тенденція у зростанні кількості публікацій, яка ще більше посилилась у 2021-2023 роках.

Рисунок 1 репрезентує збільшення обсягу публікацій, яке вказує на

[1] Ця робота була підтримана Міністерством освіти і науки України (науково-дослідна тема 0122U000769 «Трансфер зелених інновацій в енергетиці України: мультиплікативна стохастична модель переходу до вуглецево-нейтральної економіки».

посилення уваги до питань, що досліджуються з боку наукової спільноти, бізнесу та урядових структур, що сприяє подальшому розвитку та впровадженню цифрових технологій у низьковуглецевій економіці.

Особливий науковий інтерес тематика становить для країн: Китай, Велика Британія, Австралія, Німеччина, Сполучені Штати. Згідно БД Scopus саме за цими країнами визначено найбільшу кількість праць за тематикою. Україна також визначена в переліку країн, які здійснюють дослідження щодо впливу діджиталізації на розвиток низьковуглецевої економіки.

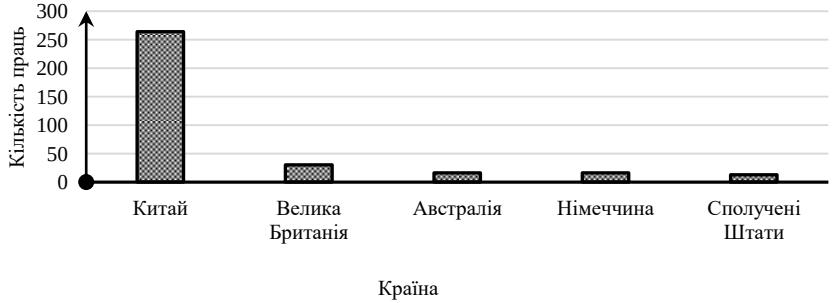


Рисунок 2 – Топ країни за кількістю документів за 2008 – 2024 рр. за ключовими словами digital AND low-carbon AND economy на базі використання БД Scopus

До організацій, що вивчають тематику відносяться: Пекінський педагогічний університет, Університет Цінхуа, Північнокитайський електроенергетичний університет, Сіньцзянський університет, Міністерство освіти КНР, Університет міжнародного бізнесу та економіки, Південно-Західний фінансово-економічний університет та ін. Серед вітчизняних визначено такі: Державний економіко-технологічний університет, Західноукраїнський національний університет. Фінансування здійснюють такі заклади: Національний фонд природничих наук Китаю, Національне бюро філософії та соціальних наук, Міністерство освіти КНР, Фонди фундаментальних досліджень для центральних університетів, Національна ключова програма досліджень і розвитку Китаю, Європейська Комісія, Фонд природничих наук провінції Шаньдун, Дослідницька рада інженерно-фізичних наук.

Проблематиці присвячують свої дослідження такі вітчизняні науковці: Максимова І., Савельєв Є., Зварич І, Куриляк В., Лизун М., Саченко С., Ліщинський І. [1], Кулішов, В. [2].

Цифрові технології дозволяють автоматизувати безліч процесів економіки та оптимізувати використання ресурсів. Діджиталізація є драйвером впровадження інноваційних методів управління енергоспоживанням, що сприяє скороченню витрат та економії енергії. Цифрові технології надають інструменти спектрального аналізу, що дають змогу більш точно аналізувати дані та приймати обґрунтовані рішення в

економіці. Цифрова трансформація призводить до появи нових інноваційних моделей бізнесу, орієнтованих на сталий розвиток.

Сучасні цифрові технології відіграють ключову роль у зниженні вуглецевого сліду. Діджиталізація забезпечує перехід від паперової документації до електронних систем, що значно скорочує використання паперу. Цифрові інновації в галузях розумних міст дозволяють раціонально використовувати ресурси та керувати енергетичною складовою. Використання датчиків та автоматизованих систем дозволяє знизити споживання енергії та зменшити викиди. Віртуальні технології, такі як віртуальна реальність та доповнена реальність, надають унікальні можливості для створення екологічно стійких рішень. Наприклад, віртуальні конференції та навчальні платформи зменшують навантаження на фізичні переміщення [3].

Діджиталізація відіграє ключову роль при оптимізації виробництва, у рамках безвуглецевої економіки. Впровадження передових технологій та цифрових процесів підвищує ефективність та зменшує негативний вплив на навколишнє середовище. Використання сучасних технологій, таких як інтернет речей (IoT), штучний інтелект (ШІ) та аналітика даних дозволяють застосовувати новітні методи управління виробництвом. Це забезпечує точне планування та оптимізацію процесів, скорочення витрат та підвищення продуктивності. Цифрові рішення дозволяють налаштовувати виробничі процеси відповідно до особливих вимог без забруднення навколишнього середовища. Застосування керованих систем контролю якості та виробництва допомагає мінімізувати втрати матеріалів та енергії, що сприяє створенню сталого виробничого середовища. Інтеграція чистих та екологічно безпечних технологій у виробничі процеси є основним принципом впровадження безвуглицевої економіки [4].

Цифрові технології впливають на споживання енергії та на способи управління нею. Значну енергоефективність цифрові технології забезпечують на базі використання автоматизованих систем розумних мереж та промислової автоматизації.

Застосування діджиталізації у виробничих процесах та енергетиці дозволяє більш точно контролювати витрати на електроенергію.

Розвиток концепції розумних міст, заснованої на цифрових технологіях, допомагає скоротити енергоспоживання за рахунок оптимізації міської праці, управління транспортом, а також забезпечити джерела енергії, що постійно оновлюються.

Однією з головних переваг діджиталізації є її позитивний вплив на екологічну стійкість та безвуглицеву економіку. Цифрові технології допомагають організаціям людей ефективно скоротити споживання паперу, енергії та інших ресурсів. Це призводить до скорочення кількості парникових газів та зменшення негативного впливу на навколишнє середовище. Цифрові інновації сприяють розвитку розумних транспортних систем, сприяючи стійкій мобільності та скорочення мобільних транспортних засобів в атмосфері. Це забезпечує створення більш екологічно чистих та ефективних

методів пересування.

Цифрові інструменти дозволяють вести безперервний моніторинг та аналізувати споживання ресурсів, що дозволяє визначити область, де можна заощадити або оптимізувати використання ресурсів. Автоматизація завдань із використанням цифрових технологій дозволяє ефективно економити ресурси. Цифрові платформи дають можливість контролювати енергоспоживання на початковому етапі, що забезпечує ефективніше використання ресурсів. Використання електронних інструментів для віртуального співробітництва дозволяє скоротити потребу у відрядженнях та фізичних зустрічах, що забезпечує максимальну економію ресурсів.

Однією з головних переваг сучасних технологій є їх високий рівень прозорості та безпеки. Завдяки розподіленій природній системі всі результати перетворюються у блоки, які чіпляються один за одного, що робить маніпуляції з даними практично неможливими. Застосування сучасних технологій у безвуглецевій економіці забезпечує скорочення витрат та спрощення процесів. Це також підвищує ефективність системи та скорочує час на обробку інформації.

[1] Maksymova, I., Savelyev, Y., Zvarych, I., Sachenko, S. Lishchynskyy, I. Global Differentiation of Climate-digital Projects in Terms of Low-carbon Economy. Proceedings of the IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications. IDAACS. 2023. P. 859–864. URL: https://www.semanticscholar.org/paper/Global-Differentiation-of-Climate-digital-Projects-Maksymova-Savelyev/8fc778b5c197ea918ffb548b82c48829f8c0e16d

[2] Maksymova, I., Mietule, I., Kulishov, V. Digital Solutions for a Climate Neutral Economy: International Framework of Eco-Digital Projects. Vide. Tehnologija. Resursi - Environment, Technology, Resources, 1, P. 123–127. 2023. URL: https://www.semanticscholar.org/paper/Global-Differentiation-of-Climate-digital-Projects-Maksymova-Savelyev/8fc778b5c197ea918ffb548b82c48829f8c0e16d

[3] Volynets V. Use of virtual reality technologies in education. Continuing Professional Education: Theory and Practice. 2021. P. 40–47. URL: https://doi.org/10.28925/1609-8595.2021.2.5.

[4] Бардадим С. А. Невмержицька С. М. Цалко Т. Р. Діджиталізація HR-процесів в організації. URL: https://er.knutd.edu.ua/handle/123456789/19577

О.С. Потенко, О.М. Дибач, С.Ф. Гончар

ЗАСІБ ОЦІНЮВАННЯ СУМИ РИЗИКІВ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Стейкхолдери інформаційних систем, у тому числі об'єктів критичної інфраструктури, прагнуть звести до мінімуму ризики кібербезпеки, а також мінімізувати витрати на заходи по мінімізації цих ризиків. Економічна доцільність застосування і вибір тих чи інших заходів по обробці ризику, включаючи як організаційні, так і технічні, визначається оціночним порівнянням вартості таких заходів з максимальною величиною збитків в результаті дії декількох ризиків. Результат оцінювання суми таких ризиків дають підстави для прийняття рішення щодо прийнятності їх рівня і необхідності чи економічної доцільності їх подальшої обробки. Під сумою ризиків будемо розуміти певну величину, що визначається збитками у результаті реалізації усіх складових ризиків, і ймовірністю реалізації цих ризиків. Така задача являється актуальною для визначення ризику складного проекту (може бути складна інформаційна система), що характеризується наслідками при реалізації даного проекту і ймовірністю цих наслідків.

Методи оцінювання суми ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури та структурні рішення відповідних обчислювальних систем запропоновані в [1-4].

На базі запропонованих методів та структурних рішень обчислювальних систем розроблено алгоритмічне забезпечення для реалізації відповідного програмного забезпечення і на його основі розроблено прикладну програмну систему.

Інтерфейс розробленої програмної системи розрахунку суми ризиків, наслідків від цих ризиків, ймовірності настання цих наслідків приведено на рис. 1.

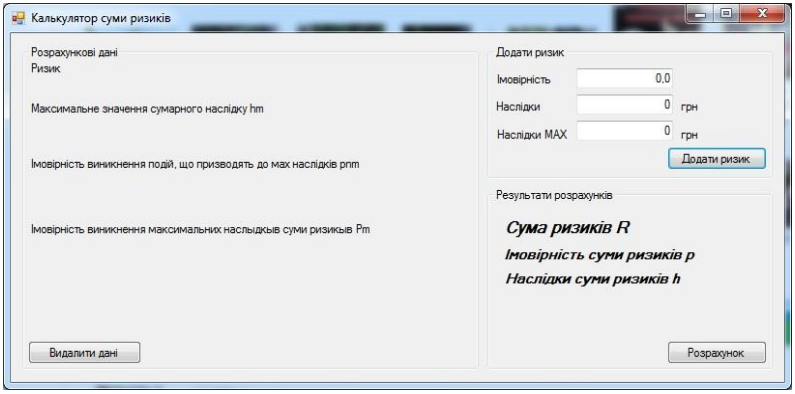


Рисунок 1 – Інтерфейс програми

Використовуючи запропоноване програмну систему виконано обчислення суми ризиків: від загроз, що можуть виникнути під час мережевої взаємодії, від загроз, що можуть виникнути під час роботи з прикладним програмним забезпеченням, від загроз, що можуть виникнути в мережевих операційних системах інформаційно-телекомунікаційної системи захищеного вузлу Інтернет доступу. Результат розрахунку приведено на рис. 2. Також здійснено розрахунок значення наслідків при реалізації кожної з груп загроз і ймовірність виникнення цих наслідків.

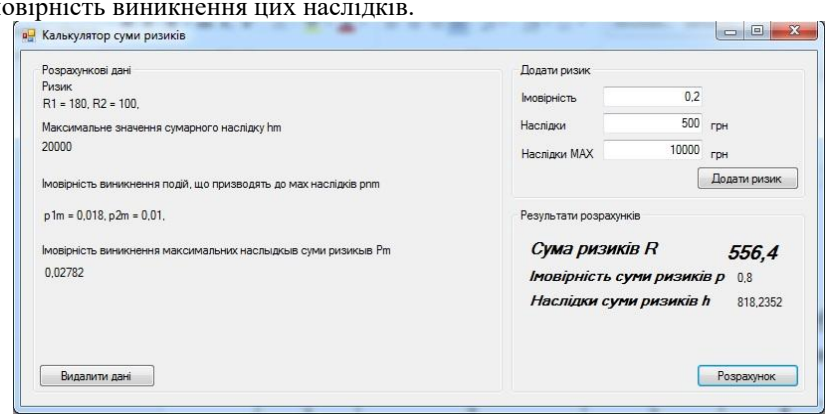


Рисунок 2 – Приклад розрахунку

Отримані результати можуть бути використані при визначенні ризику складного проекту (може бути складна інформаційна система), що характеризується наслідками при реалізації даного проекту і ймовірністю цих наслідків, а також дають підстави для прийняття рішень про економічну доцільність застосування заходів по зменшенню ризику.

[1] Мохор В.В., Гончар С.Ф., Дибач О.М. Методи оцінки сумарного ризику кібербезпеки об’єктів критичної інфраструктури // Ядерна та радіаційна безпека. 2019. №2(82). С. 57-61. https://doi.org/10.32918/nrs.2019.2(82).01.

[2] Мохор В.В. Оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури / Мохор В.В., Гончар С.Ф. // Електронне моделювання. – 2019. – Т.41. – № 6. – С. 65-76.

[3] Гончар С.Ф. Метод агрегування ризиків у випадку множини сумісних випадкових подій / Гончар С.Ф., Бакалинський О.О., Дибач О.М., Дімітрієва Д.О. // ДНТЦ ЯРБ. 2022. № 1(93) – С.44-50. https://doi.org/10.32918/nrs.2022.1(93).05.

[4] Гончар С.Ф., Потенко О.С. Методологія оцінки суми ризиків кібербезпеки інформаційної системи об’єктів критичної інфраструктури // Захист інформації. – 2023. – Том 25, № 3. – С. 159-165.

В.С. Ракович, В.В. Цуркан

СПОСІБ ЗАХИЩАННЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ НА ОСНОВІ ЗАМКІВ ВИСОКОЇ БЕЗПЕКИ ЗА ТЕХНОЛОГІЄЮ ДОПОВНЕНОЇ РЕАЛЬНОСТІ

Під об'єктами критичної інфраструктури розуміються об'єкти інфраструктури, системи, їхні частини та сукупність. Ознакою їх належності є, *по-перше*, важливість для економіки, національної безпеки та оборони. *По-друге*, порушення функціонування таких об'єктів може призводити до шкоди життєво важливим національним інтересам [1]. Окремим різновидом убезпечення об'єктів критичної інфраструктури є охорона. Тоді як одним з її організаційних заходів є забезпечення фізичного доступу працівників на такі об'єкти. Для цього використовується широкий спектр способів – від охоронця на дверях до складних систем контролю та управління доступом.

Для надання або відмовлення у доступі до певних частин об'єктів критичної інфраструктури може використовуватися певний «секрет», який реалізовано в матеріальному (наприклад, ключ, карта доступ) або цифровому (наприклад, біометричні дані працівника) виді. Для видавання такого «секрету» та забезпечення можливості його використання пропонується застосовувати технологію доповненої реальності. Завдяки цьому можливе додавання віртуальних предметів до реального оточення та організування взаємодії з ними [2]. Тож отримання доступу працівником за основу можна взяти деякі віртуальні предмети та/або операції над ними. Як тригер для їх появи пропонується використовувати маркер (наприклад, певне графічне зображення, QR-код). У запропонованому способі для реалізування «секрету» запропоновано використовувати послідовність символів – «mnemonic code». Це узгоджується з вимогами чинного законодавства [3].

Для створення замка високої безпеки [3] необхідно встановити біля точки доступу на об'єкт критичної інфраструктури або його частину деяке, попередньо узгоджене, зображення (у прикладі реалізації запропонованого способу буде використовуватися QR-код [4], що додатково дозволить закодовувати в ньому певну інформацію, наприклад, адресу сервера, на який треба надсилати код для перевірки). До того ж необхідно реалізувати можливість віддаленого керування.

Однією з умов використання запропонованого способу є наявність у працівника пристрою (наприклад, смартфон, гарнітура), який забезпечує доступ за технологією доповненої реальності. В найбільш типовому випадку – це може бути особистий смартфон із встановленим на ньому відповідним програмним забезпеченням.

Отже, реалізування способу отримання доступу до об'єкту критичної інфраструктури або його певної частини пропонується у такій послідовності:

1) працівник підходить до точки доступу (наприклад, двері, ворота, люк) та сканує код спеціальним застосунком смартфону (гарнітурою);

2) екран смартфону відображає вид зі задньої камери, тобто людина бачить на екрані те, що знаходиться перед нею;

3) на екрані смартфону з'являються віртуальні предмети, наприклад, куби з різними цифрами на кожній стороні (рис. 1);

4) завдання працівника взаємодіяти зі смартфоном (гарнітурою) або натисканням на екран, або проведенням пальцем по екрану, або виставленням певним чином положення смартфона у просторі домогтися правильного розташування віртуальних предметів. Наприклад, перевернути кожен куб так, щоб на його стороні була певна цифра і послідовність цифр на кубах відповідала певному коду. Це код тлумачиться як є код доступу для даної точки;

5) після цього працівник приводить в дію тригер (наприклад, натискає віртуальну кнопку, звичайну кнопку на смартфоні) перевірки комбінації. Якщо код правильний, то працівник отримує доступ до визначеної точки (двері відкриваються).

Рисунок 1 – Приклад реалізації послідовності віртуальних фігур

З технологічного погляду відбувається таке:

1) застосунок на пристрої (смартфоні, гарнітурі) працівника обробляє дані з різних датчиків та камер та розташовує віртуальні фігури у реальному середовищі і відображає це працівнику;

2) застосунок на пристрої (смартфоні, гарнітурі) створює інтерфейс взаємодії співробітника з віртуальними об'єктами та забезпечує аналіз поточного положення фігур;

3) після задіяння тригера перевіряння комбінації віртуальних фігур (працівник виставив фігури у потрібних положеннях та натиснув кнопку для відправлення коду) застосунок відправляє виставлений код на пристрій аналізування і прийняття рішення щодо надання доступу у даній точці (наприклад, сервер MQTT [5], Bluetooth-пристрій [6] відмикання). Якщо код вірний, то відбувається надання доступу у точці (відчиняються двері, піднімається шлагбаум).

Переваги запропонованого способу:

1. Забезпечення більш високої захищеності системи надання доступу завдяки застосуванню мережевих протоколів зі шифруванням та можливій реалізації інших захисних протоколів.

2. Забезпечення гнучкості при налаштуванні та можливості швидкого змінення конфігурації системи без великих матеріальних витрат.

3. Забезпечення масштабування та створення систем доступу різної складності.

4. Забезпечення контролю проходження точок доступу працівниками в реальному часі.

З огляду на це, запропоновано спосіб підвищення результативності захищання об'єктів критичної інфраструктури на основі замків високої безпеки за технологією доповненої реальності. Його використання дозволяє гнучко вибудовувати систему контролювання доступу до локацій на об'єкті критичної інфраструктури та створювати масштабовані рішення відповідно до потреб. Реалізування запропонований спосіб не вимагає великих витрат та не залежить від кількості працівників об'єкту критичної інфраструктури.

Крім того з урахуванням визначень відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» під об'єктом критичної інформаційної інфраструктури розуміється комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури [7] Тож створена в результаті реалізування запропонованого способу система захищання від несанкціонованого доступу може розгядатися як складник критичної інформаційної інфраструктури.

[1] Про критичну інфраструктуру : Закон України від 16.11.2021 р. № 1882-IX. Дата оновлення: 01.01.2024. URL: https://zakon.rada.gov.ua/ laws/show/1882-20#Text (дата звернення: 03.05.2024).

[2] Peddie J. Augmented Reality Where We Will All Live. Cham : Springer, 2023. 398 p. DOI: https://doi.org/10.1007/978-3-031-32581-6.

[3] ДСТУ EN 1300:2019. Засоби безпечного зберігання. Замки високої безпеки. Вимоги, класифікація та методи випробування на опір взламуванню та несанкціонованому відмиканню (EN 1300:2018, IDT). [Чинний від 2020-01-01]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2020. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=87665 (дата звернення: 03.05. 2024).

[4] QR-code specification. URL: https://www.qrcode.com/en/about/standards.html (access date: 03.05.2024).

[5] What is MQTT? URL: https://aws.amazon.com/what-is/mqtt/?nc1=h_ls (access date: 03.05.2024).

[6] Bluetooth specification. URL: https://www.bluetooth.com/specifications/ (access date: 03.05.2024).

[7] Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. Дата оновлення: 04.04.2024. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 03.05. 2024).

Д.М. Семенюк

МЕТОД ВИЯВЛЕННЯ ПРИХОВАНИХ ВИТОКІВ В НЕ НАПІРНИХ ПОЛІМЕРНИХ ТРУБОПРОВОДАХ ФІЛЬТРАЦІЇ БАСЕЙНІВ ЗА ДОПОМОГОЮ АКУСТИЧНОГО ТЕЧЕШУКАЧА А-10Т3

Витоки води в трубопроводах - досить поширене явище. Як правило аварії сталевого трубопроводу спричинені корозією труби, але і при використанні полімерних трубопроводів аварійні витоки є достатньо часте явище. Полімерні трубопроводи, що використовуються в будівництві басейнів, втрачають герметичність по різним причинам: неякісний монтаж при монтуванні, просадка грунту, розморожування взимку та ін.. Виникають втрати води, яку потрібно постійно добавляти, що охолоджує температуру води в басейні, вносити додатково реагенти для знезараження води. Потрапляння надлишкової вологи під фундамент басейну може викликати просадку та руйнування самої чаши басейну та пошкодження інших інженерних мереж.

Враховуючи те, що трубопроводи фільтрації басейнів приховані та працюють з малими тисками, для визначення місця пошкодження трубопроводу потрібно застосування технічних засобів з підвищеною чутливістю та спеціальних методичних прийомів.

Серед пристроїв, що давно використовуються для пошуку витоків в трубопроводах, працюючих під тиском, широке застосування отримали акустичні течешукачі. Як вже писалося раніше в роботах [1,2], було вдосконалено акустичний течешукач А-10Т3 виробництва ІПМЕ ім. Г.Е.Пухова НАН України [3]. Застосування п'єзоелектричного перетворювача з більшим коефіцієнтом перетворення значно покращило чутливість датчика та розширило практичне застосування приладу.

Щоб використати акустичний метод, для пошуку прихованих витоків в не напірних полімерних трубопроводах фільтрації басейнів за допомогою акустичного течешукача А-10Т3, штучно створено надлишковий тиск. Для забезпечення цього виходи трубопроводів були тимчасово заглушені. Під час експериментів були виготовлені та використані пневматичні заглушки, рис.1а.

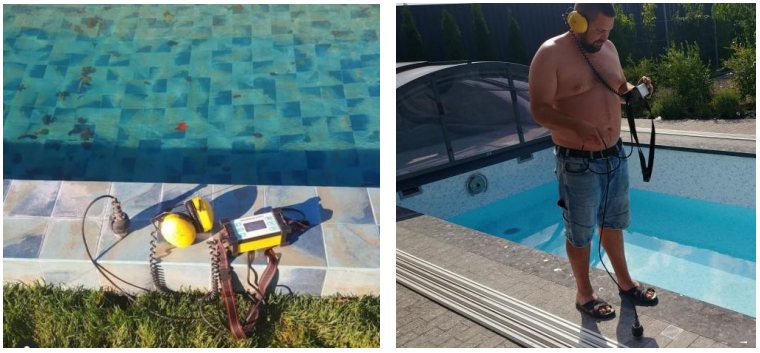
Використовуючи метод, описаний в роботах [1,2], подаючи одночасно повітря компресором та воду у заглушений трубопровід фільтрації басейну, під час витікання води з повітрям крізь дефект трубопроводу виникала достатньо потужна гідродинамічна кавітація. Даний методичний прийом дозволяє при низьких тисках створювати достатньо високі рівні акустичного шуму витоку для його реєстрації на поверхні покращеним датчиком ВДМ-6 течешукача А10Т3 [2], див.рис.1-4.

а) б)

Рис.1 Виготовлена пневматична заглушка для діаметру 50 мм (а) та місце монтажу (б)

а) б)

Рис.2 Застосування пневматичних заглушок (а) та комплексної методики з апаратурою додаванням повітря в трубопровід та використанням течешукача А-10Т3 з експериментальним датчиком (б) дало змогу при малому надлишковому тиску в полімерних трубопроводах фільтрації басейнів успішно знаходити приховані витоки.



а) б)

Рис.3 Акустичний течешукач А-10Т3 (а) та його застосування (б)

Рис.4 Виток з полімерного трубопровода фільтрації басейна

[1] Семенюк Д.М.. Виявлення прихованих мікровитоків в трубопроводах внутрішньо будинкових мережах за допомогою удосконаленого термоакустичного течешукача А-10Т3. 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. / ІПМЕ ім. Г.Є. Пухова НАН України. – 2023. – с127-129.

[2] Д.М. Семенюк Комплексні методи виявлення прихованих мікровитоків в полімерних трубопроводах внутрішньо будинкових мережах. Зб. матеріалів V Науково-практичної конференція «Безпека енергетики в епоху цифрової трансформації» Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України м. Київ , 22 листопада 2023 р. / ІПМЕ ім. Г.Є. Пухова НАН України. – 2023. с. 109-111.

[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.

А.В. Полухін, Я.П. Лукашевич

АЛЬТЕРНАТИВНА ГЕНЕРАЦІЯ ЯК ШЛЯХ ДО РОЗВИТКУ РОЗПОДІЛЕНОГО ВИРОБНИЦТВА ТА ЕНЕРГЕТИЧНОЇ БЕЗПЕКИ В УКРАЇНІ

На сьогоднішній день, як відомо, енергетичний становище в Україні перебуває в надскладному стані. Запорізька атомна станція окупована і фактично не приймає участі в роботі об'єднаної енергетичної системи України; Каховська ГЕС повністю зруйнована; частина теплових електростанцій обстріляна ракетами та не працює. Все це призводить до того, що є як і дефіцит генеруючих потужностей, так і маневрених блоків для оперативного управління енергосистемою України.

Однак, у кожній біді можна спробувати знайти шлях для покращення. І хоча, зрозуміло, що країни Заходу не будуть інвестувати у відновлення теплових станцій (оскільки це проти політики вуглецевої нейтральності, так і самі теплові блоки вже були певним чином зношені), наразі України може стати на шляху розвитку розподіленої генерації, сегментації та розвитку генеруючих установок «на місцях» – мова йде про відновлювальні джерела енергії. При цьому, про перевагу розподіленої «зеленої» генерації казало і само ПрАТ «НЕК «Укренерго» як оператор системи передачі та розподілу, наводивши приклад, що ворогу простіше завдати точкового руйнівного ракетного удару по крупним станціям, ніж намагатися влучити у тисячі розрізнених по всій країні невеличких станцій.

Виробництво електричної енергії з альтернативних джерел розвивається навіть в умовах війни. Попри те, що Росія окупувала частину південних та східних територій України, знищила до 90% потужностей вітрової та 30% сонячної енергетики, за два роки нам вдалося додати до енергосистеми понад 600 МВт потужностей ВДЕ. Окрім того, як показав досвід блекаутів, «зелена» генерація може бути шляхом до забезпечення роботи критичної інфраструктури, виробництва товарів та послуг [1] та нормального життя населення (наприклад домашні СЕС).

Наразі 90% альтернативної енергетики приєднані до розподілених мереж [2]. З них 99% - до мереж, класом напруги 35 кВ і менше (рисунок 1). Тобто, розвиток розподіленої генерації в Україні і так відбувався, тому задача його інтенсифікації є надзвичайно актуальна та цілком можлива.

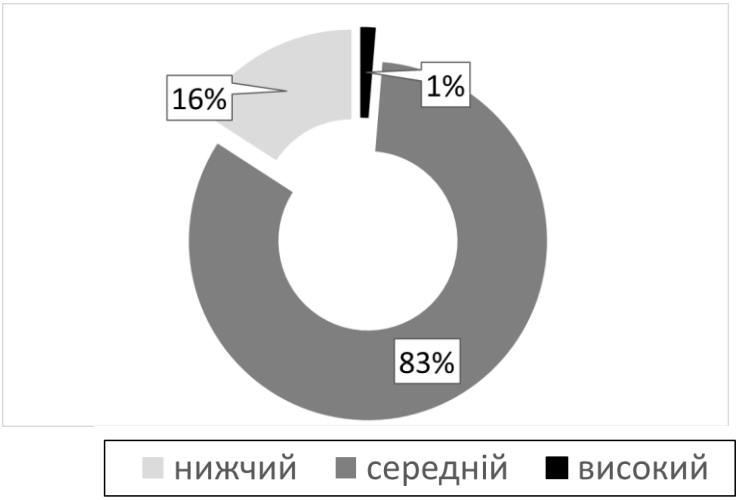


Рисунок 1 – Розподіл по класам напруги за встановленою потужністю станцій, де високий клас напруги – від 110 кВ, середній – від 1 кВ до 35 кВ, нижчий – до 1 кВ.

Споживання в Україні є нерівномірним. Так, наприклад, до війни найбільше споживання досягалось в Дніпропетровській області, де зосереджено значна кількість, у перші чергу, промислових підприємств. Другу сходинку впевнено посідали Київ, Київська, Одеська, Запорізька та Харківська області. Графічне порівняння рівня споживання представлене на рисунку 2.

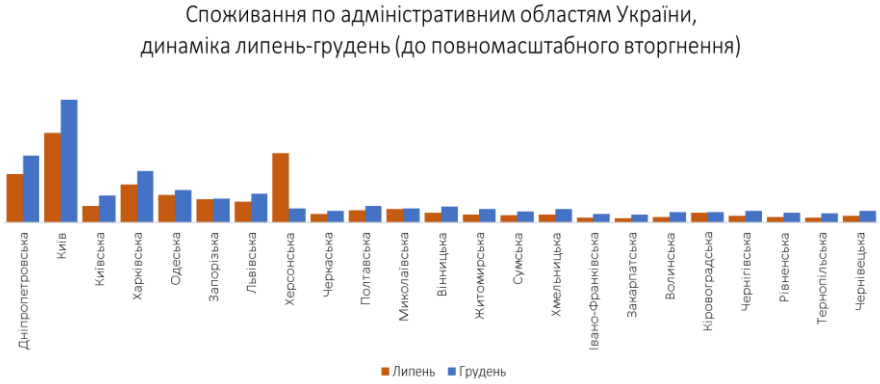


Рисунок 2 – Споживання по адміністративним областям України

Ураховуючи фактори щодо втрати генеруючих потужностей, наведені на початку, виникає проблема забезпечення електричною енергією віддалені

від потужних атомних блоків області. До того ж, вічно без зупинки вони (атомні блоки) працювати на можуть. А для транспортування електричної енергії на великі відстані треба підтримувати фактично значно більше виробництво ніж того потребує енергосистема, через природу втрат електричної енергії в електромережі.

Не варто забувати і те, що ворог систематично обстрілює лінії електропередачі, які є найбільш пристосованими для передачі електроенергії на великі відстані, а транспортування розподільними мережами збільшує втрати у мережі ще більше. І не останнім лімітуючим фактором є системі обмеження.

Тому можна дійти логічного висновку, що необхідно забезпечити покриття споживання генеруючи обладнанням «на місцях» – цю роль на себе може взяти розподілена генерація, наприклад, відновлювальна. На рисунку 3 і 4 відображено на скільки на сьогоднішній день відновлювальні джерела енергії покривають споживання в різних областях України на прикладі комунально-побутові споживачів.

Рисунок 3 – Покриття комунально-побутового споживання відновлюваної генерацією у липні

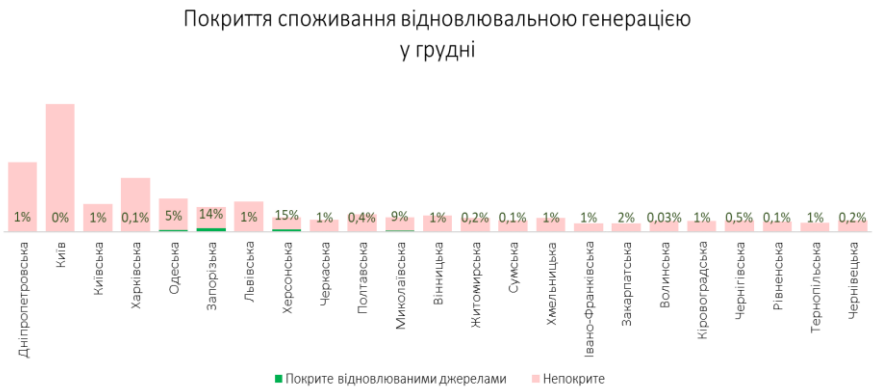


Рисунок 4 – Покриття комунально-побутового споживання відновлюваної генерацією у грудні

Як видно з рисунків, ступінь покриття споживання, а саме комунально-побутових споживачів, низький і нерівномірний. У Дніпропетровській, Вінницькій, Кіровоградській областях він особливо знижується у зимній період. При цьому, у Сумській, Волинській, Рівненській областях ступінь покриття дуже низький навіть влітку.

В областях, де багато сонячної і вітрової генерації (Херсонська, Запорізька, Миколаївська), ступінь покриття найвищий.

Виходячи з зазначеного можна дійти таких висновків:

— необхідна розбудова відновлювальних джерел на основі біомаси та біогази, оскільки вони мають найбільш рівномірний графік виробництва протягом доби;

— має бути встановлений такий обсяг генераторів, СЕС, ВЕС, малих модульних станціях та систем зберігання енергії, які забезпечують потреби в електроенергії, принаймні населення та житлово-комунальними господарствами окремого регіону.

Важливим є стимулювання розбудови відновлювальних станцій за регіональним принципом. Можливо, наразі найбільше стимулювати треба як раз ті станції, де вони найбільше необхідні. Якщо будується станція в дуже концентрованому регіоні, то до її стимулювання застосовується знижуючий коефіцієнт.

Зазначені заходи сприятимуть:

— розвитку регіонального виробництва та споживання;

— забудові альтернативними джерелами енергії в тих регіонах, де це потрібно, замість скупчення в одній області та навантаження на диспетчера;

— покращенню надійності електропостачання;

— можливість оперативно ліквідовувати наслідки уражень;

— обмеженості масштабу уражень за рахунок енергетичної

незалежності регіонів між собою;

— розвитку адаптації до змін.

Зрозуміло, що повністю забезпечити потреби регіонів буде неможливо, але забезпечити потреби об'єктів критичної інфраструктури, побутових споживачів, комунальних підприємств цілком можливо.

Розвиток розподіленої генерації реально реалізувати за рахунок використання власного ресурсного потенціалу регіонів (рисунок 5).

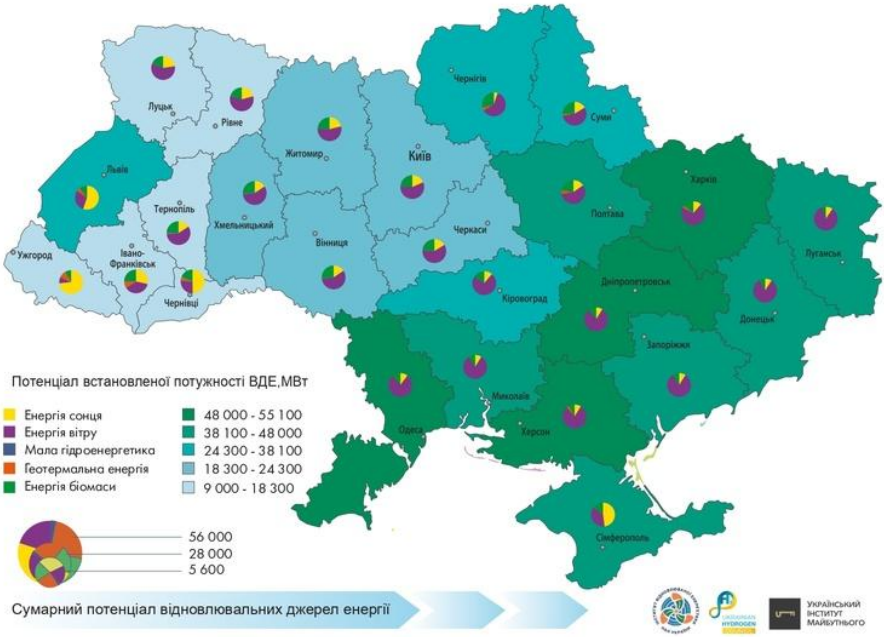


Рисунок 5 – Потенціал встановленої потужності ВДЕ, МВт [3]

Територіальні громади зацікавлені у своєму розвитку та втілюють проєкти, що мають забезпечити стабільну роботу енергомережі та безпеку свого регіону. Наприклад, Славутич планує на 100% перейти на відновлювані джерела енергії в усій громаді. Зокрема місто вже має «амбітний проєкт» на 6 млн євро, який передбачає встановлення міні-ТЕЦ на деревині [4]. Дві громади з Чернігівщини стали переможцями міжнародного проєкту, де встановлять сонячні електростанції. Одна з них з'явиться на водозаборі у Сосницькій громаді. У Менській громаді панелі розмістять на будівлі міської лікарні [5]. У Миргороді на одному з об'єктів «Тепловодсервісу» збудували сонячну електростанцію. Вона допоможе комунальному підприємству заощаджувати електроенергію і забезпечити хоча б мінімальне постачання води під час перебоїв зі світлом [6].

Проте цього все ще недостатньо для досягнення резильєнтоності

енергосистеми. Україна

Таким чином, проблема критичності енергетичного стану об'єднаної енергетичної може бути вирішена за рахунок розподіленого виробництва електричної енергії, стимулювання будівництва відновлювальних джерел енергії в усіх регіонах країни. Розвиток місцевого виробництва та споживання спонукатиме забезпеченню сталості роботи електромережі, забезпечення її резильєнтності. Створить умови для зменшення витрат операторів систем розподілу на закупівлю електричної енергії на власні потреби (втрати в мережі).

Розвиток розподіленої генерації є надзвичайно актуальною задачею. Він вже відбувається, але поки на рівні ініціативних територіальних громад. Вже є приклади і позитивний досвід забезпечення критичної інфраструктури електричною енергією з відновлюваних джерел, що може бути використано іншими. Разом з цим держава має забезпечити зрозумілу регуляторну перспективу розробки таких інвестиційних проєктів.

[1] СОНЯЧНІ ЕЛЕКТРОСТАНЦІЇ ПРАЦЮЮТЬ ВЖЕ НА 140 АЗК МЕРЕЖІ ОККО. https://www.okko.ua/sonyachni-elektrostanciyi-pracyuyut-vzhe-na-140-azk-merezhi-okko

[2] YaP Lukashevych Analysis of the dynamics of the development of alternative energy plants in terms of their connection to the power transmission networks. IOP Conference Series: Earth and Environmental Science 1254 012038 (2023), DOI: 10.1088/1755-1315/1254/1/012038, https://iopscience.iop.org/article/10.1088/1755-1315/1254/1/012038

[3] Можливості альтернативної енергетики дозволяють скоротити споживання традиційних енергоносіїв удвічі. https://mind.ua/publications/20205250-mozhlivosti-alternativnoyi-energetiki-dozvolyayut-skorotiti-spozhivannya-tradicijnih-energonosiyiv-udvichi

[4] Славутич анонсував стовідсотковий перехід на відновлювані джерела енергії. https://biz.liga.net/ua/all/tek/novosti/slavutych-anonsuvav-stovidsotkovyi-perekhid-na-vidnovliuvalni-dzherela-enerhii

[5] У двох громадах Чернігівщини встановлять сонячні електростанції. https://suspilne.media/chernihiv/685886-u-dvoh-gromadah-cernigivsini-vstanovlat-sonacni-elektrostancii/

[6] Енергонезалежність: у громаді встановлюють сонячні електростанції. https://myrgorod.pl.ua/news/energonezalezhnist-u-gromadi-vstanovljujut-sonjachni-elektrostantsiji

О.І. Клюзко

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ЗАКУПІВЕЛЬНОЇ ДІЯЛЬНОСТІ КОМПАНІЇ-ПОСТАЧАЛЬНИКА ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ

Для забезпечення постачання електричної енергії споживачам компанії-постачальники здійснюють купівлю-продаж електричної енергії на різних сегментах ринку: ринку двосторонніх договорів – РДД, ринку «на добу наперед» – РДН, внутрішньодобовому ринку – ВДР та балансуючому ринку – БР [1]. Компанія-постачальник забезпечує постачання всього обсягу фактичного споживання електричної енергії споживачами, тобто вона формує баланси:

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

Відповідно до правил ринку, година є часовим періодом, на основі якого визначаються ціни та обсяги купівлі-продажу електричної енергії. Таким чином, рівність (1) має бути забезпечена постачальником для кожної години t місяця постачання тривалістю T годин.

Близько 70% електричної енергії, поставленої споживачам, купується постачальниками на РДД. Найбільші обсяги електричної енергії реалізуються генеруючими компаніями через біржовий майданчик "Українська енергетична біржа" у формі пропозицій учасників, які відповідають умовам стандартних біржових продуктів. Відповідно, термін "продукт" застосовується для позначення пропозицій купівлі-продажу електричної учасниками ринку на РДД. Постачальники електроенергії конкурують за можливість забезпечення споживачів найнижчими та передбачуваними цінами. Зокрема, на форвардному сегменті ринку - РДД, де ціни фіксуються заздалегідь, це дозволяє мінімізувати ризики, пов'язані з волатильністю цін на спотових сегментах ринку електроенергії.

Рентабельність роботи постачальника залежить від здатності обрати оптимальний набір продуктів із запропонованих на ринку, який відповідатиме графіку споживання електроенергії. Однак складний асортимент продуктів, що включає базовий та індивідуальні профілі навантаження, ускладнює пошук оптимального набору для задоволення потреб споживачів та ефективного використання ресурсів.

Для вирішення задачі пошуку оптимального набору продуктів електричної енергії, що забезпечить покриття нерівномірного графіка споживання електричної енергії запропонована математична модель ринкової поведінки компанії-постачальника.

Прибуток постачальника визначається різницею між очікуваним доходом від продажу електроенергії та загальною вартістю закупівлі на різних сегментах ринку електричної енергії України [2]. Електропостачальник може купувати електроенергію у генеруючих компаній та спотовому ринку в обсягах, що забезпечать покриття очікуваного

(планового) графіку продажу електроенергії роздрібному покупцю.

Очікуваний дохід від постачання електричної енергії обчислюється як різниця між вартістю продажу електроенергії всім споживачам та на спотовому ринку, і вартістю купівлі на оптовому та спотовому ринках. Це можна представити як:

$$W = \sum_{\forall t \in T} \left(\begin{array}{l} \sum\limits_{\forall c \in C} P_{c,t} V_{c,t} + P_t^s S_t - \\ \sum\limits_{\forall g \in G} P_{g,t} V_{g,t} - P_t^b B_t \end{array} \right), \quad (2)$$

де: $W -$ очікуваний прибуток від обсягів $V_{c,t}$ продажу електроенергії для всієї множини споживачів C за цінами $P_{c,t}$, обсягів S_t продажу електроенергії на РДН за цінами P_t^s, обсягів $V_{g,t}$ купівлі електроенергії на РДД для всієї множини генеруючих компаній G за цінами $P_{g,t}$ та обсягів B_t купівлі електроенергії на РДН за цінами P_t^b. При цьому прибуток визначається для всіх інтервалів часу $t \in T$ прогнозного періоду T.

У зв'язку з тим, що постачальник згідно з вимогами законодавства має бути відповідальним за баланс, головною умовою успішної діяльності стає збереження рівноваги між обсягами купівлі та продажу електроенергії, тобто:

$$\sum_{\forall g \in G} V_{g,t} + B_t - \sum_{\forall c \in C} V_{c,t} - S_t = 0, \quad \forall t \in T. \quad (3)$$

що, відповідно, формує умову достатності обсягів $V_{g,t}$ та B_t купівлі електроенергії на РДД ($\forall g \in G$) та РДН для забезпечення виконання компанією-постачальником договірних зобов'язань перед споживачами в обсягах постачання $V_{c,t}$ ($\forall c \in C$), тобто:

$$\sum_{\forall g \in G} V_{g,t} + B_t \geq \sum_{\forall c \in C} V_{c,t}, \quad \forall t \in T. \quad (4)$$

Купівля електричної енергії у генеруючої компанії $\forall g \in G$ можлива згідно запропоновано продавцем часового графіку продажу електроенергії $\left\{ h_{g,t}, \forall g \in G, \ \forall t \in T \right\}$ з фіксованим обсягом H_g, що не перевищує максимальну пропозицію $H_g^{\max}$. Отже, маємо обсяги купівлі електричної енергії:

$$V_{g,t} = H_g \ h_{g,t}, \quad \forall g \in G, \quad \forall t \in T. \quad (5)$$

та обмеження зверху величин фіксованого обсягу H_g.

$$H_g \leq H_g^{\max}, \quad \forall g \in G. \quad (6)$$

де: $h_{g,t} -$ функція часового графіку продажу електричної енергії компанією $g \in G$ для $\forall t \in T$.

З метою уникнення можливих ризиків, пов'язаних з порушеннями обмежень щодо маніпулювання ринком, компанії-постачальники встановили ліміт обсягу продажу електроенергії на РДН у розмірі 10% від загального обсягу закупівлі електроенергії на РДД. Тобто, маємо обмеження:

$$S_t \le 0.1 \sum_{\forall g \in G} V_{g,t}, \quad \forall t \in T \,. \tag{7}$$

Стратегія ринкової поведінки компанії-постачальника електричної енергії полягає у максимізації місячного прибутку, тобто у визначені оптимальних значень обсягів закупівлі електроенергії на РДД та закупівлі-продажу електроенергії на РДН з метою максимізації прибутку (2). У формалізованому вигляді така стратегія представляється цільовою функцією:

$$W \xrightarrow[\{H_g, \forall g \in G\}, \{B_t, S_t, \forall t \in T\}]{} \max \tag{8}$$

Варто відзначити, що цільова функція (8), разом із функціональним виразом (2) та обмеженнями (3)-(7), є задачею лінійного програмування. Розв'язування задачі може здійснюватися за допомогою багатьох існуючих солверів. Зокрема, за допомогою IBM ILOG CPLEX Optimization Studio, як зручного інструменту формування комп'ютерної моделі ринкової поведінки компанії-постачальника електричної енергії та розв'язування задач моделювання. У процесі дослідження, розглянуто практичний випадок закупівлі електроенергії компанією-постачальником. Загалом розглянуто угоди про закупівлю електроенергії з різних джерел, зокрема від генеруючих компаній та спотового ринку РДН, з метою її подальшого перепродажу множині кінцевих споживачів. Мовою OPL сформовано комп'ютерну модель задачі, знаходження розв'язку якої здійснювалось програмним додатком IBM ILOG CPLEX Optimization Studio. За результатами, було отримано оптимальний план закупівлі електроенергії. Знайдені графіки закупівлі електричної енергії демонструють відповідність графікам споживання.

Отримані результати засвідчують, що розроблена модель може бути рекомендована до впровадження в енергетичних компаніях для вирішення задач пошуку оптимальних стратегій їхньої діяльності на ринку електроенергії. Наразі модель призначена для використання в умовах заздалегідь визначених погодинних графіків споживання. Передбачається, що розроблена модель буде удосконалюватися шляхом розвитку методів прогнозування графіків споживання.

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

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

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

В.В. Сичова

ЗАСТОСУВАННЯ ЙМОВІРНІСНИХ НЕЙРОННИХ МЕРЕЖ ДЛЯ ПРОГНОЗУВАННЯ ОБСЯГУ ПОПИТУ НА ПОСЛУГУ БАЛАНСУВАННЯ

Вступ. Послуга з балансування – послуга купівлі та продажу електричної енергії, що надається оператору системи передачі постачальником послуг з балансування з метою забезпечення достатніх обсягів електричної потужності та електричної енергії, необхідних для балансування в реальному часі обсягів виробництва та імпорту електричної енергії і споживання та експорту електричної енергії, врегулювання системних обмежень в об'єднаній енергетичній системі України [1].

Прогнозування обсягу попиту на послугу балансування справляє позитивний ефект при керуванні електроенергетичною системою та має велике значення для учасників ринку електроенергії [2-4], включаючи виробників та операторів системи передачі електроенергії в Україні. Позитивними наслідками точного прогнозування є: оптимізація виробництва та споживання електроенергії; врегулювання небалансів електроенергії [5-7]; максимізація використання ресурсів та їх економія; забезпечення стабільності електроенергетичної системи в цілому.

Метою цієї роботи є розробка та дослідження моделей на основі штучних нейронних мереж для прогнозування обсягу попиту на послугу балансування з інтервалом передбачення 72 години.

Матеріали і методи. Вибірка досліджуваних ретроспективних даних містить погодинні значення обсягів попиту на послугу балансування («вгору» і «вниз»). Досліджуваний період становить 13.10.2022-10.10.2023 (8704 точки).

В Таблиці 1 наведені результати попереднього статистичного аналізу вибірки передісторії.

Таблиця 1 – Результати попереднього аналізу досліджуваних вибірок

Вибірка	M, МВт	Me, МВт	min, МВт	max, МВт	σ, МВт	R_a, %	k_v, %
"вгору"	475,6	385,4	0	2647,2	393,9	89,32	82,9
"вниз"	362,78	208,7	0	4376,6	443,6	89,31	122,2

У випадку обох вибірок їхні середні значення *M* суттєво відрізняються від значень медіани *Me*, що свідчить про розподіл вибірок відмінний від нормального. Для даних «вгору» середньоквадратичне відхилення σ є близьким до середнього значення, що виражено в коефіцієнті варіації k_v, який становить понад 80% та вказує на значну варіабельність вибірки. Для даних «вниз» середньоквадратичне відхилення перевершує середнє значення, відповідно коефіцієнт варіації становить понад 100%, що свідчить про істотну нерівномірність та широкий розкид даних. Розмах обох вибірок

рівний максимальному значенню та є досить широким. Значення коефіцієнтів автокореляції R_a становлять 89%, що може свідчити про тісні залежності між даними у вибірці. Коефіцієнт кореляції між досліджуваними вибірками R становить 4,27% та свідчить про відсутність залежностей між цими вибірками. Також, варто зазначити, що обидві вибірки не є підпорядкованими нормальному, рівномірному розподілу та розподілу Пуасона.

Зважаючи на складну структуру даних, прийнято рішення про застосування для прогнозування моделей на основі імовірнісних нейронних мереж, які спрямовані на моделювання невизначеності в прогнозах і рішеннях. Для порівняння обрано баєсові мережі (BNN) [8] та генеративно-змагальні мережі (GAN) [9]. Оскільки BNN надають розподіл ймовірностей для прогнозів, вони можуть ефективно враховувати невизначеність у даних, що є особливо корисним у випадку високої невизначеності та варіативності даних. Моделі GAN можуть бути корисними для роботи з асиметричними розподілами, так як вони можуть адаптуватися до різних форм розподілу і враховувати його особливості.

Побудовано такі моделі:

1. Архітектура BNN:

Кількість вхідних вузлів 1, кількість виходів 1, кількість прихованих вузлів 5, параметр масштабу для апріорного розподілу 10, 2 приховані шари, що використовують лінійну трансформацію, функція активації – гіперболічний тангенс.

Всі ваги і зсуви шарів визначаються як зразки з апріорного розподілу, в даному випадку, нормального розподілу зі середнім значенням 0 і масштабом 10. Для навчання моделі використовується MCMC (Markov Chain Monte Carlo) з алгоритмом NUTS (No-U-Turn Sampler) – це вдосконалений алгоритм MCMC. NUTS дозволяє автоматично визначити кількість кроків і не вимагає встановленого розміру кроку.

2. Архітектура GAN:

Генератор: Вхідний шар (2 вузли) → Прихований шар (16 вузлів) з активацією ReLU → Прихований шар (32 вузли) з активацією ReLU → Вихідний шар (2 вузли).

Дискримінатор: Вхідний шар (2 вузли) → Прихований шар (256 вузлів) з активацією ReLU та Dropout (0,5) → Прихований шар (128 вузлів) з активацією ReLU та Dropout (0,5) → Прихований шар (64 вузли) з активацією ReLU та Dropout (0,5) → Вихідний шар (1 вузол) з активацією сигмоїдна функція.

Генератор і дискримінатор виконано у вигляді нейромереж прямого зв’язку (feedforward neural network (FNN)). Навчання триває протягом 100 епох з використанням оптимізатора Adam для оновлення параметрів дискримінатора і генератора. Функція втрати nn.BCELoss() використовується для обчислення бінарної крос-ентропії.

Результати. Тестовий період становить 21 добу (504 точки) з 11.10.2023 по 31.10.2023. Проведено 7 дослідів прогнозування по 3 доби (72 точки).

Метрикою оцінки результатів є середньоквадратична похибка RMSE:

$$RMSE = (n^{-1}\sum_{i=1}^{n}(y_i - y_i^{'})^2)^{1/2}; \quad (1)$$

де n – обсяг прогнозованої вибірки, y – фактичне значення, y' – прогнозоване значення.

Значення RMSE досліджуваних моделей для кожного досліду (1-7) та загальні (Σ) при прогнозуванні обох вибірок представлені у вигляді стовпчастих діаграм на рис. 1.

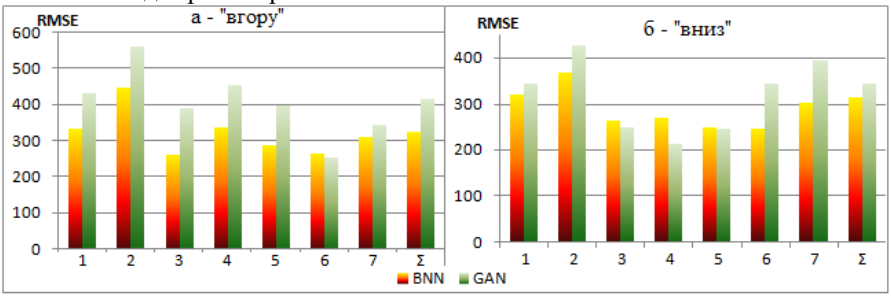


Рисунок 1 – Стовпчасті діаграми значень RMSE

Згідно із отриманими значеннями RMSE жодна із побудованих моделей не має переваги за точністю прогнозування. Проте за загальним значенням похибки для обох вибірок точність BNN є дещо вищою.

Роботу виконано в межах реалізації проєкту з виконання наукового дослідження і розробки «Моделі і засоби підвищення ефективності роботи гідро- та гідроакумулюючих електростанцій для балансування ОЕС України в умовах ринку електричної енергії та особливих технологічних обмежень» (реєстраційний номер 2022.01/0069), що фінансується Національним фондом досліджень України в межах конкурсу проєктів з виконання наукових досліджень і розробок «Наука для відбудови України у воєнний та повоєнний періоди» (КПКВК 2201300)

Висновки. В цій роботі проведено статистичних аналіз річних вибірок із погодинною дискретністю обсягу попиту на послугу балансування. Досліджені вибірки мають складну структуру та істотну варіативність. Тому для їх прогнозування побудовано моделі на основі ймовірнісних нейронних мереж BNN та GAN через їхню здатні до врахування невизначеності та здатність до гнучкості при моделюванні різноманітних залежностей у даних. Отримані результати є задовільними та вказують на потребу у вдосконаленні розроблених моделей.

[1] Закон України «Про ринок електричної енергії» № 2019-VIII (2017) https://zakon.rada.gov.ua/laws/show/2019-19#Text

[2] Blinov, I., Olefir, D., Parus, E., Kyrylenko, O. (2023). Improving the Efficiency of HPP and PSHPP Participation in the Electricity Market of Ukraine. Power Systems Research and Operation. Studies in Systems, Decision and Control, vol 220. Springer,

Cham. pp 51–74. DOI: https://doi.org/10.1007/978-3-031-17554-1_3

[3] Блінов І., Олефір Д., Парус Є. (2022). Модель оптимального використання ресурсів гідроелектростанцій на ринку електричної енергії. Технічна електродинаміка, 4, 42-47. DOI: https://doi.org/10.15407/techned2022.04.042 .

[4] Олефір Д.О., Бабіч В.Ю., Блінов І.В. (2021). Актуальні проблеми забезпечення ОЕС України ресурсами регулювання частоти та потужності. Енергетика: економіка, технології, екологія, 3, 39-46 DOI: https://doi.org/10.20535/1813-5420.3.2021.251196

[5] Blinov I., Miroshnyk V. and Sychova V. (2022). Comparison of models for short-term forecasting of electricity imbalances. 2022 IEEE 8th International Conference on Energy Smart Systems (ESS-2022)

[6] Blinov I, Miroshnyk V and Sychova V. (2023). Short-term forecasting of electricity imbalances using artificial neural networks. 4th International conference on sustainable futures: environmentak, technological, social and economic matters (ICSF-2023) DOI 10.1088/1755-1315/1254/1/012029

[7] Сичова В.В. (2023). Розробка штучної нейронної мережі для прогнозування небалансів електричної енергії в ОЕС України. Праці Інституту електродинаміки Національної академії наук України, 66, 58-63 DOI: https://doi.org/10.15407/publishing2023.66.058

[8] Russell, Stuart, and Peter Norvig (2012). Künstliche Intelligenz. Vol. 2. München: Pearson Studium.

[9] Ian Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio (2014). Generative adversarial nets. Advances in Neural Information Processing Systems, 27, 139–144.

А.І. Швайка, В.О. Артемчук, В.О. Бабак

АРХІТЕКТУРА MQTT БРОКЕРА TBMQ

Інтернет речей (IoT) стрімко розвивається, що призводить до зростання попиту на проміжне програмне забезпечення, яке надійно керує зв'язком між пристроями IoT. На цій конкурентній арені IoT платформа ThingsBoard стала передовою платформою IoT з відкритим кодом, привернувши увагу академічної спільноти [[1]]. Також зростає потреба у рішеннях, здатних забезпечити ефективний і надійний обмін даними, що призводить до зростання конкуренції на ринку брокерів MQTT.

Широке впровадження IoT платформи ThingsBoard корпоративними клієнтами значно покращило розуміння розробників ThingsBoard сценаріїв застосування MQTT. Це розуміння призвело до ідентифікації кількох ключових випадків використання, які необхідні брокерам MQTT для ефективної підтримки. Після оцінки пропозицій від провідних постачальників брокерів MQTT з відкритим кодом було створено індивідуальне рішення компанії ThingsBoard, адаптоване до конкретних вимог типових додатків IoT - MQTT брокер TBMQ. Розробка брокера TBMQ почалася в 2020 році, і до 2021 року він був інтегрований в комерційні проекти. Після доведеної ефективності у робочих налаштуваннях у червні 2023 року було прийнято рішення відкрити кодову базу брокера TBMQ.

Розробка TBMQ ґрунтувалася на ретельно розробленому наборі принципів проектування, спрямованих на вирішення ключових вимог, важливих для сучасних екосистем IoT. Ці принципи гарантують, що TBMQ виступає як надійна, масштабована та ефективна брокерська платформа MQTT [[2]]:

Маштабованість: TBMQ було розроблено для досягнення як вертикальної, так і горизонтальної масштабованості.

Відмовостійкість: В архітектурі TBMQ кожен вузол посередника в кластері розроблено таким чином, щоб бути функціонально ідентичним і використовувати ту саму кодову базу.

Постійність даних: TBMQ надає пріоритет безпеці даних через надійні механізми збереження даних. Повідомлення MQTT і деталі клієнтської підписки зберігаються з резервуванням у налаштованій кількості місць.

Компактність даних і операційна ефективність: Компактний двійковий формат Protocol Buffers Google (Protobuf) [[3]] значно зменшує розмір корисного навантаження, що приносить користь TBMQ, зберігаючи пропускну здатність і зменшуючи вимоги до пам’яті.

Розробка схем і сумісність: Protobuf дозволяє TBMQ розвивати свої формати повідомлень і структури даних завдяки зворотній і прямій сумісності.

Ефективність: Ефективність є відмінною рисою TBMQ, оскільки один серверний вузол здатний обслуговувати мільйони клієнтів, обробляючи сотні

тисяч повідомлень за секунду. У великому масштабі кластер TBMQ може похвалитися здатністю підтримувати вражаючу пропускну здатність щонайменше 100 мільйонів клієнтів і 3 мільйони повідомлень на секунду, демонструючи свою здатність обробляти масові розгортання IoT.

Рисунок 1 ілюструє центральні компоненти брокера, цифри всередині кіл показують послідовність передачі повідомлень.

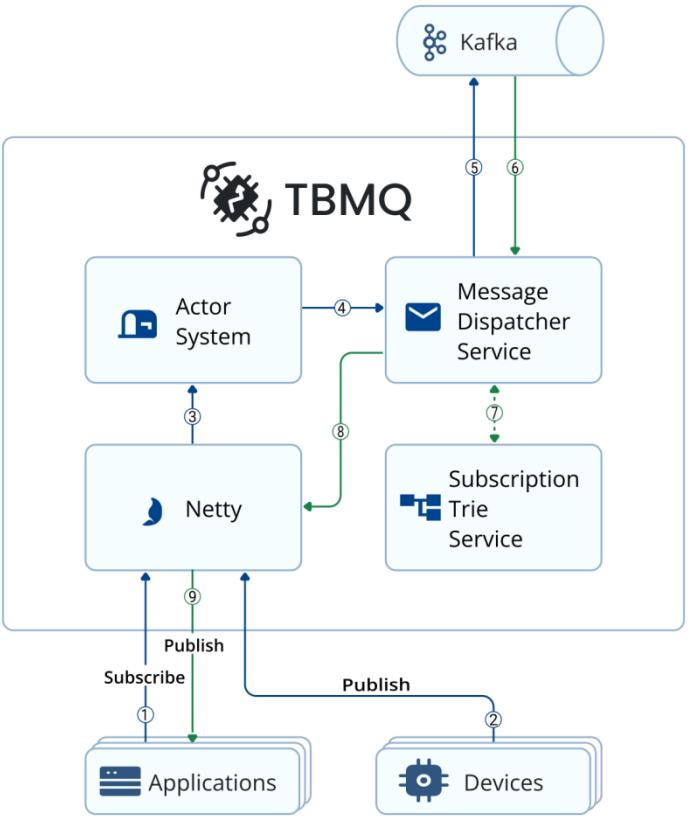


Рисунок 1 – Архітектура TBMQ [[2]].

Брокер використовує власну реалізацію системи акторів, спеціально розроблену для задоволення вимог TBMQ.

Прагнучи використовувати передову технологію, ми обрали Netty [[4]], для впровадження TCP-сервера, який підтримує протокол MQTT завдяки його перевіреній продуктивності та гнучкості.

Подібним чцрщфьш1ином Kafka [[5]], було обрано як платформу розподіленої потокової передачі подій за її бездоганність у надсиланні повідомлень між вузлами в кластері TBMQ.

Щоб адаптувати наш підхід до різноманітних потреб екосистеми IoT, TBMQ розділяє клієнтів MQTT на дві різні категорії DEVICE та APPLICATION, відповідно оптимізуючи обробку та зберігання повідомлень.

Класифікуючи клієнтів MQTT за цими двома категоріями, TBMQ ефективно узгоджує свої механізми обробки та зберігання даних із конкретними потребами кожного типу клієнта, оптимізуючи загальну ефективність системи та гарантуючи, що клієнти як DEVICE, так і APPLICATION отримують найвищий рівень обслуговування, адаптований до їхніх унікальних вимог.

Наша мета полягає в тому, щоб підвищити ефективність TBMQ та підтримувати до 500 мільйонів з'єднань шляхом вивчення передових методів керування даними та оптимізації пам'яті. Ці зусилля обіцяють ще більше вдосконалити продуктивність і масштабованість TBMQ, сприяючи розвитку масштабованих, надійних комунікаційних рішень IoT.

Підсумовуючи, TBMQ постає як надійний, високопродуктивний брокер MQTT, який має хороші позиції для вирішення складних завдань ландшафту IoT. Його розробка відображає продумане зближення галузевих ідей і технологічних інновацій, що робить його ключовим внеском у брокерські сфери IoT і MQTT.

[1] Di Felice, P. and Paolone, G., 2024. Papers mentioning things board: A systematic mapping study. Journal of computer science, 20(5), Mar, pp.574–584. Available from: https://doi.org/10.3844/jcssp.2024.574.584.

[2] ThingsBoard, 2023. TMBQ architecture. Available from: https://thingsboard.io/docs/mqtt-broker/architecture/.

[3] Google, 2016. Google. Protocol Buffers. Available from: https://developers.google.com/protocol-buffers.

[4] Netty.The Netty project. Available from: https://netty.io/.

[5] Apache Kafka. Available from: https://kafka.apache.org/.

О.І. Грамак, М.М. Ліневич

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ПРОЦЕСІ ПРИЙНЯТТЯ РІШЕНЬ. КІБЕРБЕЗПЕКА ТА ШТУЧНИЙ ІНТЕЛЕКТ В ЕНЕРГЕТИЦІ

В сучасних умовах (умовах гібридної російської воєнної агресії проти України) особливої актуальності набуває переосмислення існуючих підходів до функціонування системи управління в енергетичній сфері як складової забезпечення обороноздатності нашої Держави. Одним з напрямків розвитку цієї системи є розробка нових та підвищення ефективності роботи існуючих автоматизованих систем управління енергозабезпечення, систем підтримки прийняття рішень (далі – СППР), експертних та інтелектуальних інформаційно-аналітичних систем в тому числі з використанням штучного інтелекту (далі – ШІ), а також вдосконалення методів всебічного забезпечення їх надійного функціонування, насамперед – у сфері кібербезпеки.

Стрімкий розвиток та масове впровадження інформаційних та інших високих технологій призвело до формування нових ризиків і загроз у сфері національної безпеки й оборони держави, які реалізуються у кіберпросторі або через кіберпростір. Кібератаки стали більш руйнівними для державних установ, підприємств, економіки, транспорту, електроенергетики, об'єктів критичної інфраструктури. Для здобуття переваги під час збройного конфлікту або уповільнення сталого розвитку держави цілеспрямовані кібератаки на державні об'єкти, зокрема на об'єкти енергетики, можуть досягти такого рівня інтенсивності, який почне негативно впливати на стан національної безпеки й обороноздатності держави.

Сучасне суспільство практично повністю залежить від стану безпеки інформаційної інфраструктури. Через це забезпечення безпеки інформаційної інфраструктури, об'єктів критичної інфраструктури є надважливою умовою забезпечення обороноздатності держави, її економічного та соціального розвитку.

Актуальність цих питань визначається потребою в автоматизації процесів управління в енергетичній сфері, розвитку ШІ та системи кібербезпеки в Україні. Вимоги щодо цього містяться у Законах України "Про національну безпеку України", "Про основні засади забезпечення кібербезпеки України", Стратегії кібербезпеки України та Концепції розвитку штучного інтелекту в Україні. Штучний інтелект, розвиток розумних мереж, автоматизація технологічних процесів дозволять більш ефективно керувати режимами постачання та споживання енергії. При цьому використання технологій ШІ стає ефективним інструментом забезпечення сталого розвитку та операційної безпеки систем енергозабезпечення.

Також слід враховувати, що рф у своїх діях керується актуальними у XXI столітті принципами збройної боротьби: застосування невійськових

засобів у інформаційно-психологічних операціях, комбіновані гібридні атаки на об’єкти інфраструктури у кіберпросторі, фізичному, інформаційному та когнітивному вимірах для досягнення військових цілей, у тому числі – шляхом руйнування інформаційних систем та систем управління.

У ході кібератак противник може намагатись втрутитись в роботу систем управління енергозабезпечення, порушити стабільність та нанести іншої шкоди інформаційним ресурсам в енергетичній сфері за допомогою відомих хакерських методів: DDoS-атак, блокування ПЕОМ через програми-вимагачі, MITM-атаки, фішингові атаки (у тому числі китовий фішинг та цільовий фішинг), парольні атаки, SQL-ін’єкції, підміну URL-адрес, DNS-спуфінг, перехоплення tcp-сесії, Brute force-атаки, Web-атаки, атаки на ланцюжки поставок (supply-chain attack), Drive-by-атаки, викрадення даних через троянські віруси, Malware-атаки (наприклад, розповсюдження комп’ютерних хробаків), міжсайтовий скриптінг, атаки з підслуховуванням, а також проникнення агентури противника всередину інформаційної системи для здійснення диверсій.

Отже, з огляду на поширені види кібератак та перспективи застосування ШІ для кібератак на системи управління енергозабезпечення, нами окреслені деякі питання кібербезпеки інформаційних ресурсів в енергетичній сфері та запропоновані можливі шляхи її поліпшення.

Передбачається, що рф та інші можливі противники найближчим часом можуть використовувати властивості і вразливості систем зі ШІ для створення нових викликів кібербезпеці, наприклад: проблеми з конфіденційністю даних – система зі ШІ може передати конфіденційну інформацію противнику у випадку недосконалої політики безпеки; втручання противника – внесення незначних змін до вхідних даних та алгоритмів з метою прийняття неправильних рішень або прогнозів, що становить загрозу точності і надійності системи зі ШІ; упередженість та дискримінація – принцип пріоритетності даних, що використовується для навчання моделей ШІ, може призвести до необ'єктивних результатів, ігнорування важливої інформації та прийняття невірних рішень; програмування на автоматизовані атаки – кібератаки на основі ШІ мають потенціал автоматизації та масштабування традиційних методів злому, що робить їх потенційно ефективнішими та більш руйнівними; можливість виходу системи з-під контролю – через помилки алгоритмів або втручання противника система може атакувати свого власника, запускаючи кібератаки з безпрецедентною швидкістю та точністю.

Спираючись на досвід останніх локальних воєнних конфліктів 2001 – 2023 років, а також сучасні тренди у сфері ІТ, перспективними напрямами розвитку підсистем кіберзахисту інформації в системах управління в енергетичній сфері є:

1. Технологія Blockchain (блокчейн) (базові цифрові платформи, які дозволяють будувати автоматичні, децентралізовані програми обліку). Ця технологія дозволяє реалізувати розумні контракти (Smart Contracts, які виконуються автоматично за встановленим алгоритмом), які можна

використовувати для фіксації операцій купівлі-продажу енергії багатьох учасників без посередника, для кращого керування енергосистемами.

2. Технологія обробки великих обсягів даних (Big data) – може вдосконалити організаційно-технічну структуру інформаційних систем і засобів кіберзахисту шляхом моделювання поведінки кіберзагроз в кібер-середовищі на об'єкти енергетики, пошуку вразливостей систем захисту, проведення навчань з кіберзахисту та тренування відповідних спеціалістів у віртуальному середовищі.

3. Тренування моделей ШІ з функцією експертних систем кіберзахисту – може автоматизувати процедури пошуку кіберзагроз, їх ізоляції, ідентифікації та вивчення, передачі інформації до банку даних кіберзагроз а також надати рекомендації щодо прийняття подальших рішень адміністратором з безпеки. Крім того, така модель зможе виявляти джерела кібератак і ознаки застосування при цьому систем зі ШІ, а також помилки алгоритмів роботи систем зі ШІ в своїй системі управління військами, які призвели до кіберінциндентів.

Також, для протидії майбутнім викликам ШІ, необхідно вдосконалювати методи шифрування даних, контролю доступу, політики безпеки, регулярної оцінки адекватності та тестування безпеки роботи власних систем зі ШІ, а також здійснювати регулярний моніторинг конфіденційності та цілісності даних в усіх інформаційних системах в енергетичній сфері.

Впровадження вищезгаданих ІТ дозволить підвищити стійкість управління енергосистем до кіберзагроз та безпеку їх інформаційних ресурсів у перспективі.

[1] Штучний інтелект в енергетиці : аналіт. доповідь / Суходоля О. М.– К. : НІСД, 2022. – 49 с. – https://doi.org/10.53679/NISS-analytrep.2022.09;

[2] Закон України "Про національну безпеку України", ВВР, 21.06.2018 №2469-19 (зі змінами) URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text;

[3] Закон України "Про основні засади забезпечення кібербезпеки України", ВВР, 05.10.2017 №2163-19 (зі змінами) URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text;

[4] Указ президента України "Про рішення РНБО Про Стратегію кібербезпеки України", 26.08.2021 №447/2021 URL:https://zakon.rada.gov.ua/laws/show/447/2021#Text;

[5] Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження Кабінету Міністрів України від 02.12.2020. № 1556-р.URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text.

П.В. Шиманюк

SMART GRID МОДЕЛЬ ДЛЯ ОПЕРАТИВНОГО КЕРУВАННЯ РОЗПОДІЛЬНИМИ МЕРЕЖАМИ НА ОСНОВІ МЕТОДІВ ШТУЧНОГО ІНТЕЛЕКТУ

Дослідження та розробка моделей Smart Grid обумовлена сучасним станом енергосистеми України [1-4] та тенденціями до керування режимами роботи розподільних мереж на основі Smart Grid моделей, що передбачають наявність достовірних результатів прогнозування навантажень та генерації ВДЕ у вузлах розрахункової схеми для різних горизонтів прогнозування.

Різкі зміни топології мережі призводять до підвищення похибки прогнозу втрат як єдиного часового ряду та знижують ефективність керування мережами. Більш якісно завдання керування можуть бути вирішені за допомогою прогнозів вузлового навантаження та моделювання режиму, що є актуальним для України в умовах постійних фізичних та кібернетичних атак на об'єкти енергосистеми.

Швидкий розвиток відновлюваних джерел енергії ускладнює прогнозування та керування майбутніми режимами роботи електричної мережі та ефективне використання інфраструктури. Для забезпечення надійності та якості електроенергії в мережі, а також для підвищення керованості мережі за рахунок використання послуг керування попитом (demand response), необхідно прогнозувати навантаження та генерацію сонячних та вітрових електростанцій [5-7], а також виконувати розподіл потоків потужності та напруги в мережі, визначаючи таким чином чутливі ділянки мережі. Це стає все складніше зробити швидко, використовуючи класичні моделі для оцінки режимів роботи електричних мереж через роботу станцій ВДЕ та змінних навантажень (зарядні станції електромобілів, теплові насоси, системи накопичення енергії/акумулятори)[8]. Тому необхідно розробити нову методологію та принципи управління для ефективного використання інфраструктури розподільної мережі з метою інтеграції більшої кількості сонячної та вітрової енергії і навантажень, які все частіше будуть доповнюватись новими технологіями. В даний час розподільна мережа моделюється при мінімальних та максимальних навантаженнях, описуючи мережу з точки зору параметрів її основних елементів (силові трансформатори, лінії електропередач, навантаження тощо). Однак даного моделювання недостатньо для ефективного використання інфраструктури розподільної мережі, для впровадження відновлюваних електростанцій (джерел енергії) та для відносно мінливих навантажень/нових технологій (зарядні станції для електромобілів, системи теплових насосів, системи зберігання енергії/акумулятори).

Новий підхід передбачає, що для тих частин мережі, де точний профіль (параметр) навантаження невідомий, режими роботи моделюється з допомогою розрахованих середніх типових навантажень. Що забезпечує

узагальнене середнє навантаження у вузлах мережі, які використовуються для розрахунку потоків потужності в лініях і значень напруги в вузлах мережі. Значення потужності генерації оцінюється за двома сценаріями - максимальному та мінімальному або нульовому навантаженні.

В рамках науково-дослідного проєкту буде запропоновано новий підхід та методологія оцінки режимів роботи мережі дозволити уникнути невизначеності та допоможе прогнозувати генерацію та навантаження, а також дозволить точно оцінити потоки потужності в лініях та напругу в вузлах мережі, що є важливим для нормальних та особливо після аварійних режимів роботи мережі.

Отримання прогнозних значень для вузлових навантажень – одне з важливих завдань керування Smart Grid мережами. На даний момент це завдання вирішується різними методами. В останні роки збільшилася кількість публікацій за даною темою [9-12], що демонструє інтерес вчених до вирішення такого типу завдань. Дослідження спрямовані як на однофакторне прогнозування, так і на багатофакторне з врахуванням температури повітря, а також інших факторів.

До класичних методів прогнозування можна віднести методи авторегресії часових рядів ARIMA (autoregressive integrated moving average), а також методи експоненційного згладжування Холта-Вінтерса . Методи на основі штучних нейронних мереж відносяться до сучасних методів прогнозування та є популярнішими завдяки своїй точності, швидкодії та ефективності навчання [13]. У статті [14] для однофакторного прогнозування використовувалась комбінована нейронна мережу на основі багатошарового перцептрону та алгоритму авторегресії для попередньої обробки даних. Апробація проводилася на даних енергосистеми PJM США. Для 96 вузлів за період 2014-2015 років із погодинною дискретністю. Ще одним прикладом комбінованої нейронної мережі є описана в [15] мережа, яка складалася з декількох нейронних мереж та модуля нечіткої логіки PROTREN для виявлення тренду. В якості даних для дослідження були використані дані ізольованої енергосистеми острова Крит, та температура повітря.

Для однофакторного прогнозування вузлових навантажень можна використовувати метод опорних векторів (SVM Support Vector Machine) [16], де описано застосування під час керування енергосистемою провінції Шаньдун у Китаї. У моделі враховується взаємозв'язок між сумарним активним навантаженням системи та вузла, а також між активною та реактивною потужністю вузла та зв'язок середніх значень потужностей усіх вузлів. Для перевірки ефективності метод опорних векторів порівнювали з нелінійною авторегресивною нейронною мережею для прогнозування активного навантаження вузла та адаптивним фільтром Калмана для прогнозування вузлових коефіцієнтів потужності.

Сучасні методи, які використовуються для задач короткострокового прогнозування вузлових навантажень, в більшості випадків є поліпшеними методами вже відомих підходів прогнозування як нейронних мереж, так і класичних методів. Основною особливістю методів штучних нейронних

мереж, є їх гнучкість і здатність ефективного навчання, висока точність прогнозування. Також точність прогнозування нейронними мережами можливо підвищити враховуючи додаткові фактори.

При прогнозуванні вузлових навантажень та генерації у вузлах з ВДЕ необхідно враховувати зв'язок між вузлами та доцільно розглядати вузлові навантаження як багатовимірний стохастичний нестаціонарний процес. Штучні нейронні мережі глибинного навчання, завдяки своїй гнучкості, узагальнюючій здібності та можливості моделювання багатовимірних даних найкраще підходять для вирішення даної задачі і можуть значно підвищити якість прогнозування у порівнянні з класичними підходами. На відміну від багатошарового персептрона та рекурентної мережі Елмана, мережі глибинного навчання зазвичай містять більшу кількість прихованих шарів. Теоретичні дослідження показують, що архітектура з великою кількістю прихованих шарів вимагає значно менше параметрів (вагових коефіцієнтів), ніж багатошаровий персептрон при однаковій якості результатів, що дозволяє використовувати потенціал великої кількості даних. Крім того, композиційна структура нелінійних перетворень у шарах мережі глибинного навчання краще відображає характер фізичних процесів.

Представлений матеріал є частиною спільного Українсько-Литовського науково-дослідного проєкту «Smart Grid модель для оперативного керування розподільними мережами на основі методів штучного інтелект»

Основною метою проєкту є створення тестової Smart Grid моделі для оперативного планування та керування розподільними мережами та оцінки значення втрат електричної енергії на основі прогнозування вузлових навантажень та генерації відновлюваних джерел енергії (ВДЕ) із застосуванням методів штучного інтелекту.

В рамках виконання роботи буде розроблено архітектуру нейронної мережі глибинного навчання для короткострокового прогнозування вузлових навантажень та генерації у вузлах з ВДЕ, як векторного процесу з урахуванням доступних зовнішніх факторів та використовуючи сучасні досягнення теорії машинного навчання.

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

[2] С.П. Денисюк, Р. Стшелецькі Формування складових інтелектуальної платформи керування енергетичними системами та мережами. Енергетика: економіка, технології, екологія. 2019. № 3. с. 7-22.

[3] Ivanov HA, Blinov IV, Parus EV, Miroshnyk VO. Components of Model for Analysis of Influence of Renewables on the Electricity Market Price in Ukraine. Technical Electrodynamics, vol. 2020. no. 4. 2020. pp. 72-75.

[4] Blinov I., Miroshnyk V., Shymanyuk P. Estimation of the cost of error of the forecast “for the day ahead” of technological losses in the electric networks of Ukraine. Tekhnichna elektrodynamika. 2020. No 5. Pp. 70-73.

[5] IRENA. Renewable Power Generation Costs in 2019. https://www.irena.org/publications/2020/Jun/Renewable-Power-Costs-in-2019

[6] Miroshnyk V., Shymaniuk P., Sychova V. Short Term Renewable Energy Forecasting with Deep Learning Neural Networks. Power Systems Research and Operation: Selected problems. editors: Kyrylenko O., Zharkin A. and other. 2022. pp. 121-142. DOI: 10.1007/978-3-030-82926-1_6
[7] Lezhniuk, P., Kravchuk, S., Netrebskiy, V., Komar, V., Lesko, V.: Forecasting hourly photovoltaic generation on day ahead. 2019 IEEE 6th International Conference on Energy Smart Systems (ESS).
[8] Kulyk, M., Zgurovets,O.: Modeling of power systems with wind, solar power plants and energy storage. Part of the Book Studies in Systems, Decision and Control book series (SSDC, volume 298), pp. 231–245. Springer. (2020).
[9] Miroshnyk V., Shymaniuk P., Sychova V., Loskutov S. Short-term load forecasting in electrical networks and systems with artificial neural networks and taking into account additional factors. Power Systems Research and Operation: Selected problems II. editors: Kyrylenko O., Denysiuk S. and other. 2022. pp. 87-105.
[10] P.O. Chernenko, V.O. Miroshnyk, P.V. Shymaniuk Univariable short-term forecast of nodal electrical loads of energy systems. Tekhnichna elektrodynamika № 2, 2020.. pp. 67–73. (ukr) DOI: https://doi.org/10.15407/techned2020.02.067
[11] Chernenko P., Sychova V. Improving the algorithm for determining the effect of air temperature on the overall electrical load of the power system to improve the accuracy of short-term forecasting. Tekhnichna elektrodynamika. 2. Pp. 77−83. (2021).
[12] Loskutov, S., Miroshnyk, V., & Blinov, I.. Comparison of widely-used models for multifactoral short-term photovoltaic generation forecast. Paper presented at the 2022 IEEE 8th International Conference on Energy Smart Systems. ESS 2022 – Proceedings. 123-126. doi:10.1109/ESS57819.2022.9969270
[13] Miroshnyk V., Shymaniuk P., Sychova V., Loskutov S. Short-Term Forecasting of Imbalances in the IPS of Ukraine. Power Systems Research and Operation: Selected problems III. editors: Kyrylenko O., Denysiuk S. and other. 2023. pp. 89-109.
[14] G. Hou, K. Xu, S. Yin, Y. Wang, Y. Han, Z. Wang, Y. Mao, Z. Lei A novel algorithm for multi-node load forecasting based on big data of distribution network. International Conference on Advanced Electronic Science and Technology (AEST 2016), Shenzhen, 2016, Pp 655-667.
[15] X. Wang, N. Hatziargyriou, L.H. Tsoukalas A New Methodology for Nodal Load Forecasting in Deregulated Power Systems. IEEE Power Engineering Review. May 2002. Pp 48-51.
[16] X.S. Han, L. Han, H.B. Gooi, Z.Y. Pan Ultra-short-term multi-node load forecasting - a composite approach. IET Generation, Transmission & Distribution. 2012. Vol. 6. pp.436-444.

A.O. Kharlamova

ENSURING CYBER RESILIENCE IN THE ENERGY SECTOR: CHALLENGES, STRATEGIES AND EXAMPLES OF SUCCESSFUL IMPLEMENTATIONS

"Secure cyberspace is the key to successful development of the country" [1].

In 2023, the Ukrainian energy system became the target of massive cyberattacks by enemy hacker groups. According to the State Service for Special Communications, in January-November 2023, about 55 attacks were recorded against the Ukrainian energy system[2]. These cyberattacks jeopardize the country's energy security. They can lead to serious economic losses, including the cost of restoring systems, loss of profits from business interruptions, and cybersecurity costs. In addition, if critical power systems fail, there may be a risk to vital services such as medical facilities, heating systems, water supply, etc.

In response to the challenges posed by cyber aggression, Ukrainian energy companies are actively strengthening their defense systems. For example, in 2023, Ukrenergo introduced a specialized Security Operation Center, which employs a staff of qualified cybersecurity specialists. The growing number of attacks on the energy sector prompts the search for new ways and technologies to protect it.

Ukraine receives significant support from international allies and partners in the field of cybersecurity. For example, Denmark provided three months of training for Ukrainian specialists aimed at improving cyber defense. In addition, companies such as Microsoft and ESET provide technical support and advice to prevent future attacks. For example, in April 2022, an attack on SCADA substation control systems launched by a Russian hacker group was prevented[3].

Cyber resilience strategies and their implementation. The growing number of devices connected to the network and the expansion of digital networks create new challenges for ensuring the cybersecurity of energy systems. One of the key tasks is to effectively respond to cyberattacks and ensure the resilience of energy systems. To achieve this goal, it is necessary to use a comprehensive approach to protecting networks, an example of potential actions to improve cyber resilience is shown in Table 1.

Examples of successful implementation of cyber resilience strategies are complemented by other innovative solutions in the energy sector. For example, the National Grid smart grid in the UK and electronic control systems for remote substations in the US demonstrate the effectiveness of an integrated approach to protecting energy systems. Additionally, it is worth noting the smart grids in Norway, which ensure a balanced and efficient operation of the power system and a high level of cybersecurity. These examples demonstrate the significant progress in cybersecurity in different countries and the importance of integrating innovative approaches to protecting your energy systems.

Ensuring cyber resilience in the energy sector requires not only monitoring and detecting cyber threats, but also strict adherence to security measures. This includes integrating cyber resilience principles into the corporate culture and risk

management system, assessing risks and developing risk management strategies, implementing effective response and recovery procedures, reviewing and improving existing security measures, and developing policies for cooperation and information sharing. These measures, together with monitoring strategies, the use of advanced authentication methods, and regular staff training, help ensure the resilience and security of energy systems in the digital environment.

Table 1 - Measures to improve cyber resilience

Interested party	**Actions**
Utilities	1. Integration of cyber resilience principles into the corporate culture and their implementation in the company's risk management system.
	2. Conducting a risk assessment and developing a risk management strategy to identify and manage cybersecurity.
	3. Implementation of effective response and recovery procedures aimed at maintaining the continuity of business processes during cyber attacks, with a clear division of responsibilities.
	4. Reviewing and improving existing security measures and implementing new ones based on the analysis of previous cyber incidents received from other companies.
	5. Developing mechanisms for threat detection and cyber threat intelligence in order to prepare for high-risk events.
Equipment suppliers	1. Participation in certification programs to increase the level of trust and safety in products, processes and services.
	2. Focusing cybersecurity standards on management approaches and processes that ensure security after the equipment is deployed.
	3. Promote cooperation between manufacturers to avoid fragmentation in regulatory requirements and ensure unity in cybersecurity standards.
Policy makers and regulators	1. Understand cybersecurity risks and communicate effectively to raise awareness among stakeholders.
	2. Utilize or adapt existing tools and guidelines to implement cybersecurity best practices.
	3. Developing a policy to support bank-wide cooperation and define procedures for responding to cyber incidents.
	5. Dissemination of best practices and vulnerabilities
	6. Support international centers for information exchange and cyber threat analysis.

[1] Стратегія енергетичної безпеки, схвалена Кабінету Міністрів України від 4 серпня 2021 року №907-р. https://zakon.rada.gov.ua/laws/show/907-2021-%D1%80#Text

[2] Російські хакери координують дії з військовими та посилюють атаки напередодні зими. Як Україна протистоїть кібератакам на енергосистему. https://forbes.ua/company/rosiyski-khakeri-koordinuyut-dii-z-viyskovimi-ta-posilyuyut-ataki-naperedodni-zimi-yak-ukraina-protistoit-kiberatakam-na-energosistemu-08112023-17242

[3] Війна Росії проти України: хронологія кібератак. https://ukraine.europarl.europa.eu/cmsdata/260475/0180_EPRS-Briefing-733549-Ukraine-cyber-attacks-timeline-FINAL-ForTrad.pdf

В.Р. Герасимов, В.В. Душеба

ОСНОВНІ ПІДХОДИ ТА ПРИНЦИПИ ОПТИМІЗАЦІЇ РОБОТИ РЕЛЯЦІЙНИХ БАЗ ДАНИХ

В епоху постійного розвитку технологій та стрімкого зростання обсягів інформації, реляційні бази даних (Oracle, MySQL, PostgreeSQL) залишаються одними з найбільш поширених інструментів для зберігання та управління даними (рис. 1). Однак, окрім реляційних БД в першу двадцятку найпопулярніших СУБД також входять нереляційні бази даних (NoSQL) такі як MongoDB, Redis, Cassandra. Дослідження та аналіз принципів оптимізації реляційних баз даних (РБД) дозволить не лише краще зрозуміти переваги та недоліки їх використання, але й оцінити можливість міграції на NoSQL для покращення швидкодії та оптимальності доступу до даних. Виокремлення та дослідження оптимальних стратегій оптимізації допоможе не лише впоратися з потенційними проблемами, що виникають у процесі міграції, але й сприятиме зростанню ефективності та продуктивності доступу до даних після міграції.

419 systems in ranking, April 2024

Rank Apr 2024	Rank Mar 2024	Rank Apr 2023	DBMS	Database Model	Score Apr 2024	Score Mar 2024	Score Apr 2023
1.	1.	1.	Oracle	Relational, Multi-model	1234.27	+13.21	+5.99
2.	2.	2.	MySQL	Relational, Multi-model	1087.72	-13.77	-70.06
3.	3.	3.	Microsoft SQL Server	Relational, Multi-model	829.80	-16.01	-88.73
4.	4.	4.	PostgreSQL	Relational, Multi-model	645.05	+10.15	+36.64
5.	5.	5.	MongoDB	Document, Multi-model	423.96	-0.57	-17.93
6.	6.	6.	Redis	Key-value, Multi-model	156.44	-0.56	-17.11
7.	7.	↑ 8.	Elasticsearch	Search engine, Multi-model	134.78	-0.01	+6.29
8.	8.	↓ 7.	IBM Db2	Relational, Multi-model	127.49	-0.26	-18.00
9.	9.	↑ 12.	Snowflake	Relational	123.20	-2.18	+12.07
10.	10.	↓ 9.	SQLite	Relational	116.01	-2.15	-18.53
11.	11.	↓ 10.	Microsoft Access	Relational	105.40	-2.52	-25.97
12.	12.	↓ 11.	Cassandra	Wide column, Multi-model	103.86	-0.72	-7.94
13.	13.	13.	MariaDB	Relational, Multi-model	93.81	-1.22	-2.13
14.	14.	14.	Splunk	Search engine	88.71	-0.97	+3.27
15.	15.	15.	Microsoft Azure SQL Database	Relational, Multi-model	78.40	-0.11	-0.66
16.	16.	16.	Amazon DynamoDB	Multi-model	77.57	-0.15	+0.12
17.	17.	↑ 19.	Databricks	Multi-model	76.33	+1.99	+15.36
18.	18.	↓ 17.	Hive	Relational	62.59	-2.24	-9.07
19.	19.	↑ 20.	Google BigQuery	Relational	61.90	-0.77	+8.59
20.	↑ 21.	↑ 23.	FileMaker	Relational	49.73	+0.92	-0.27

Рисунок 1 – Рейтинг ситем управління базами данних [1]

Під оптимальною роботою реляційних баз даних розуміється створення умов, за яких можна отримати максимальну швидкодію при мінімальних витратах ресурсів [2]. Основні напрямки управління швидкістю доступу до даних включають:

1. Оптимізацію схеми реляційних баз даних;
2. Оптимізацію запитів;
3. Оптимізацію клієнтського додатку.

Оптимізацію роботи з реляційною базою даних можна виконувати за допомогою наступних методів:

Нормалізація даних: Цей підхід передбачає розбиття бази даних на набори пов'язаних таблиць для уникнення дублювання даних та забезпечення консистентності. Він допомагає зменшити розмір бази даних та підвищити ефективність управління даними.

Денормалізація: Цей підхід полягає у злитті пов'язаних таблиць для підвищення продуктивності операцій з даними шляхом зменшення кількості з'єднань між таблицями та швидкості виконання запитів. Однак це може призвести до збільшення обсягу даних та складності управління ними.

Поділ таблиць (Partitioning): Розділення великих таблиць на менші фізичні частини дозволяє покращити продуктивність завантаження та зменшити час виконання операцій з даними.

Реплікація: розміщення копії даних на різних серверах, що дозволяє розподілити навантаження читання між ними. Це може підвищити швидкодію доступу до даних для запитів, оскільки кожен сервер-репліка може відповідати на запити від користувачів [3].

Шардування: розділення великої РБД на менші логічні частини (шарди), кожен з яких може зберігатися на окремому сервері. Це розділення навантаження може покращити швидкодію доступу до даних, оскільки запити можуть бути розподілені між різними серверами, що обробляють різні шарди.

Оптимізація запитів до баз даних - це процес покращення продуктивності та ефективності виконання запитів до бази даних. Це включає в себе різні стратегії та методи, спрямовані на зменшення часу виконання запитів, оптимізацію використання ресурсів та покращення загальної продуктивності бази даних. Деякі з основних способів оптимізації запитів включають:

Створення індексів: Індекси створюються на полях, які часто використовуються в запитах, таких як поля, за якими здійснюється пошук, фільтрація або сортування. Індекс дозволяє базі даних швидше знаходити та вибирати дані, оскільки забезпечує швидкий доступ до відповідних записів.

Використання оптимізованих операторів та конструкцій: Оптимізовані оператори та конструкції, такі як JOIN, WHERE, GROUP BY, дозволяють ефективніше обробляти запити до бази даних. Наприклад, використання правильного JOIN типу для об'єднання таблиць або WHERE умов для фільтрації даних може значно покращити продуктивність запитів [4]

Кешування (Caching) результатів запитів: Кешування зберігає результати запитів у пам'яті або на диску для майбутнього використання. Коли той самий запит повторюється, результат може бути отриманий з кешу, що значно зменшує час виконання запиту та навантаження на базу даних.

Паралельне виконання запитів: Паралельне виконання дозволяє базі даних обробляти кілька запитів одночасно, використовуючи різні потоки або процеси. Це може значно зменшити час виконання запитів, особливо у випадках, коли запити не залежать один від одного та можуть бути виконані паралельно [5]

Проведені дослідження та аналіз основних принципів оптимізації роботи з реляційними базами даних дозволяє визначити шляхи покращення їхньої продуктивності та ефективності, а саме: створення індексів, використання оптимізованих операторів, кешування результатів запитів та паралельне виконання запитів.

При переході від реляційних баз даних до NoSQL виникають проблеми з перетворенням даних. Зокрема, актуальною стає проблема автоматичного перетворення форматів даних та збору даних різного типу. Більшість досліджень у цій області спрямовані на вирішенні завдань оптимізації доступу до даних в рамках системи управління РБД і не ставлять за мету розв'язання проблеми перекладу реляційної бази даних у формат NoSQL.

[1] DB-Engines Ranking. — URL: https://db-engines.com/en/ranking (дата звернення: 2024-04-24)
[2] Garcia-Molina, H., Ullman, J. D., & Widom, J. Database Systems: The Complete Book. "Pearson", 2021
[3] Schwarz, B., Zaitsev, P., & Tkachenko, V. (2023). High-Performance MySQL: Optimization, Backups, and Replication. "O'Reilly Media".
[4] Shamsi, K. Optimizing Oracle Performance. "Apress", 2022
[5] Ridman, M. SQL Performance Explained. "Markus Winand", 2020

А.О. Тарановський

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ АВТОНОМНИХ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ ДЛЯ СТВОРЕННЯ ТЕСТОВИХ ЗАВДАНЬ НА ПРИКЛАДІ LLAMA

Як це демонструється при створенні курсів контролю знань, технології штучного інтелекту з обробки природньої мови на основі великих мовних моделей є придатними до розуміння й генерування текстів на прикладному рівні [1]. З одного боку, використання таких технологій отримало підтвердження для всіх основних типів тестових завдань [2]. З іншого боку, не всі такі інструменти є доступними з точки зору вартості, закладених розробниками обмежень, інформаційної безпеки, кібербезпеки. Разом із тим, вже пропонуються архітектури та прототипи [3, 4] використання технологій штучного інтелекту для обробки природньої мови на власних обчислювальних потужностях на прикладі призначеної для незалежного вільного використання великої мовної моделі Llama компанії Meta. Питання тоді в тому, наскільки такі автономні моделі можуть бути придатними для розуміння й генерування текстів взагалі та для створення тестових завдань зокрема.

Продовжуючи рухатись у напряму відкритих моделей, компанія Meta представила широкому загалу Llama 3 як наступне покоління відкритої великої мовної моделі, що відповідає сучасному рівню технології обробки природньої мови [5]. Ця модель пропонується із 8 млрд та 70 млрд параметрів й у двох варіантах: суто переднавчена та налаштована для виконання інструкцій із оптимізацією для діалогового режиму. За основну мету для цієї моделі окреслено задоволення потреби широкого загалу в обробці природньої мови на умовах відкритої моделі на рівні із найкращими на цей час пропрієтарними великими мовними моделями. Так само як й попереднє покоління [6], Llama 3 із 8 млрд та 70 млрд параметрів призначена для дослідницького й комерційного використання для англійської мови [7], однак тепер використання для інших мов вважається використанням не за призначенням із приміткою про те, що розробники можуть вдаватися до тонкого налаштування моделей для таких інших мов за межами англійської.

Llama 3 є доступною до завантаження за окремим запитом, проте використання цієї моделі локально все ще вимагає відповідних обчислювальних потужностей. Натомість сторонні розробники пропонують інструменти для використання Llama 3 за допомогою веб-додатків, серед яких можна зазначити Chat with Meta Llama 3 on Replicate [8] та Perplexity Labs Playground [9], адже за першим прослідковується компанія Replicate, серед інвесторів якої зазначені такі визначні постаті у венчурній індустрії, як Andreessen Horowitz, Sequoia Capital, Y Combinator [10], а в якості інвесторів розробника другого згадуються зокрема Jeff Bezos, Jeff Dean, Yann LeCun, Andrej Karpathy, Nvidia, Databricks [11]. Таке визнання з боку інвесторів та їх

бізнес-моделі дають підстави розглядати ці ресурси як такі, що дозволяють дійти розуміння щодо можливостей Llama 3 із 8 млрд та 70 млрд параметрів у варіанті налаштування для виконання інструкцій із оптимізацією для діалогового режиму.

Ці інструменти дозволили провести експеримент зі створення тестових завдань за запропонованими для цього шаблонами [2] із використанням Llama 3[2] та скласти уявлення про потенціал цієї великої мовної моделі для обробки природньої мови. Отриманні результати загалом відповідають задекларованій розробником цієї моделі меті — в цілому, тестові завдання створені на рівні актуальних пропрієтарних великих мовних моделей, що вони використовувалися у попередніх експериментах.

Дійсно, в окремих випадках результати отримані англійською мовою та не у всіх випадках отриманий результат у повній мірі відповідає поданому запиту. Але за уточнюючим запитом повторити те саме українською все ж таки отримується очікуваний результат. Та такі вади у більшій мірі мають прояв для моделі із 8 млрд параметрів. У будь-якому разі, на цій стадії дослідження відсутня можливість дійти висновку щодо того, чи слід атрибутувати недоліки отриманих результатів до безпосередньо моделі або ж це є наслідками оптимізації на рівні інструменту доступу до цієї моделі з боку його розробника.

Натомість цілком повноцінна обробка української мови коли розробником моделі прямо обумовлено, що належним є використання цієї моделі виключно для англійської мови, за нереалізованого поки тонкого налаштування для української мови, свідчать про неабиякий базовий потенціал цієї моделі. На рівні розуміння природньої мови, якісні показники моделі перебувають поза будь-якими сумнівами. На рівні генерування природньої мови відповідно до наведених у запиті інструкцій, ця модель якщо й поступається пропрієтарним, то аж ніяк не кардинальним чином. При тому, що розробником на фундаментальному рівні цієї моделі закладено можливість тонкого налаштування не тільки для певної мови, а й для певної предметної області.

Так чи інакше, якісні характеристики Llama 3 вказують на безумовний потенціал цієї великої мовної моделі та можливість нівелювати вплив негативних факторів, що поза будь-яким сумнівом буде розкрито в ході подальших досліджень. А здатність цієї моделі задовольнити потреби безпекового характеру мають навіть більш вагоме значення.

Таким чином, на прикладі призначеної для незалежного вільного використання великої мовної моделі Llama компанії Meta, використання призначених для цього великих мовних моделей на власних обчислювальних потужностях демонструє придатність такого підходу до розуміння й генерування природньої мови на необхідному для сфери контролю знань

[2] Експериментальні дані створення тестових завдань з використанням Llama 3 та допоміжних інструментів сторонніх розробників доступні для ознайомлення й завантаження за наступним посиланням: https://gist.github.com/artemtaranowski/4494248994cb9357b24c1cbf97a9364c

рівні та свідчить про перспективність використання автономних мовних моделей для створення тестових завдань і далеко за межами цього вузького напряму.

[1] Самойлов, В. Д., Абрамович, Р. П., Тарановський, А. О. (2023). Перспективи побудови тестів контролю знань персоналу АЕС з використанням штучного інтелекту. Ядерна та радіаційна безпека, 3(99), 67–74. https://doi.org/10.32918/nrs.2023.3(99).07

[2] Тарановський, А. О., Самойлов, В. Д. (2024). Створення основних типів тестових завдань за допомогою штучного інтелекту. Електронне моделювання, 46(2), 88–100. https://doi.org/10.15407/emodel.46.02.088

[3] Tsypliak, O. O., Artemchuk, V. O. (2023). Prospects for the use of Llama 2 architecture neural network based chat bots for training of critical infrastructure repair personnel. У Технології створення і використання засобів підготовки персоналу на об'єктах критичної інфраструктури – 2023 (с. 42–47). ІПМЕ ім. Г.Є. Пухова НАН України.

[4] Ципляк, О. О., Артемчук, В. О. (2024). Перспективи застосування автономних нейронних мереж архітектури типу Llama для автоматизації аналізу наукових публікацій. У Використання штучного інтелекту в наукових дослідженнях та прикладних розробках (с. 17–21). ІПМЕ ім. Г.Є. Пухова НАН України.

[5] Introducing Meta Llama 3: The most capable openly available LLM to date. (2024, 18 April). AI at Meta. https://ai.meta.com/blog/meta-llama-3

[6] Touvron, H., Martin, L., Stone, K., Albert, P., … Scialom, T. (2023). Llama 2: Open Foundation and Fine-Tuned Chat Models. arXiv. https://doi.org/10.48550/arXiv.2307.09288

[7] llama3/MODEL_CARD.md at main · meta-llama/llama3. (2024, 11 April). GitHub. https://github.com/meta-llama/llama3/blob/main/MODEL_CARD.md

[8] Chat with Meta Llama 3 on Replicate. Chat with Meta Llama 3 on Replicate. https://www.llama2.ai

[9] Perplexity Labs Playground. Perplexity Labs. https://labs.perplexity.ai

[10] About Replicate. Replicate. https://replicate.com/about

[11] Perplexity.ai. Wikipedia. https://en.wikipedia.org/wiki/Perplexity.ai

О.О. Ципляк, В.О. Артемчук

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ АВТОНОМНИХ НЕЙРОННИХ МЕРЕЖ АРХІТЕКТУРИ LLAMA ДЛЯ ПОБУДОВИ ГРАФІВ ЗНАНЬ

Деякі теми через комбінацію економічних та соціальних факторів викликають особливу цікавість науковців, що призводить до появи значної кількості публікацій, яку складно проаналізувати за допомогою стандартних методів.

В якості прикладу розглянемо широку тему штучного інтелекту. Згідно даних відомої бібліографічної бази даних Scopus за останні 5 років опубліковано понад 100 тисяч статей у цій тематиці, більше ніж за усю історію до цього. Варто зазначити, що 96% публікацій було виконано англійською мовою.

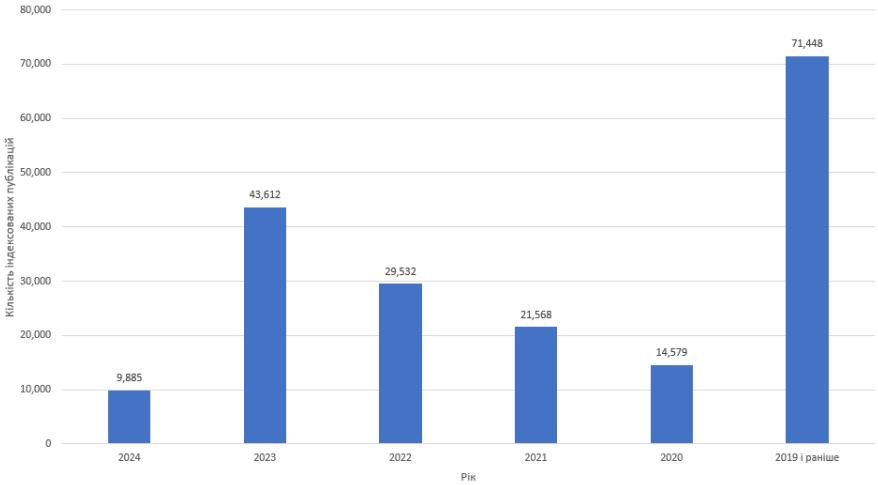


Рисунок 1. Кількість публікацій у темі AI індексованих у Scopus по роках

Використання автономних мовних моделей для відбору статей релевантних темі дослідження можливе за допомогою прототипу висвітленого у тезах[1]. Таким чином може бути зменшена кількість статтей, що потребують аналізу.

Текстовий аналіз кожної обраної статті можна виконати за допомогою генерації стислого змісту кожного окремого абзацу[2]. Для того щоб читання кожного такого абзацу було швидших ніж читання повного тексту.

Але навість застосування вищезгаданих підходів залишає надмірно великий об’єм інформації для аналізу. Проблемами такого аналізу будуть:

— Складність побудови взаємозвязків між головними ідеями статтей

— Виявлення ідей, концепцій, термінів що часто згадуються але

сформовані різними словами у багатьох обраних дослідженнях

— Узгодженність висновків групового дослідження. Декілька людей що працюють над одним дослідженням не зможуть швидко ділитись отриманими знаннями

Згідно китайсько-англійского дослідження[3] з дещо схожими проблемами зіштовхуються дорослі студенти, що отримують другу освіту і мають в короткі терміни обробляти великі масиви інформації.

Одним із ефективних рішень вище згаданої проблеми являється побудова онтологічних моделей досліджуваних питань у форматі інтелектуальних карт.

Інше дослідження [4] показує що якщо будувати такі карти за допомогою програм і мати чітку стратегію їхньої розбудови то ефективно можна аналізувати масштабні галузі з усіма їх подробицями без втрати швидкості аналізу.

Крім того, існують підходи для автоматизації переведення таблиць та діаграм у формат інтелектуальних карт [5]. Оскільки за допомогою ряду підказок до пропрієтарних великих мовних моделей доведено можна генерувати навіть якісні тестові матеріали [6], доцільним являється застосування генеративного штучного інтелекту до побудови інтелектуальних карт.

Такого роду карти мають будуватися автоматично із статтей, для того щоб:

— Візуалізувати взаємозвязки ідей в рамках однієї статті

— Візуалізувати взаємозвязки між статтями через спільну термінологію

— Надати основу для побудови інтелектуальної карти для групового дослідження

Для вирішення даних задач було спроектовано прототип інтегрований із розробкою в рамках дослідження [2]. Доповнена частина включає в собі наступну послідовність дій:

1. Після генерації абазаців із стислим вмістом обраної статті користувач вручну видаляє нопотрібні абзаци і запускає інший консольний додаток
2. Додаток доповню графову базу данних новими записами оперуючи:

a. повними текстами статтей
b. текстами обраних переказів
c. підказками для формування графу знань
d. підказками для інтеграції з існуючим графом
e. автономною мовною моделлю

3. Користувач може переглянути візуалізовану інтелектуальну карту за допомогою окремого модуля для візуалізаці MSSQL графової бази даних

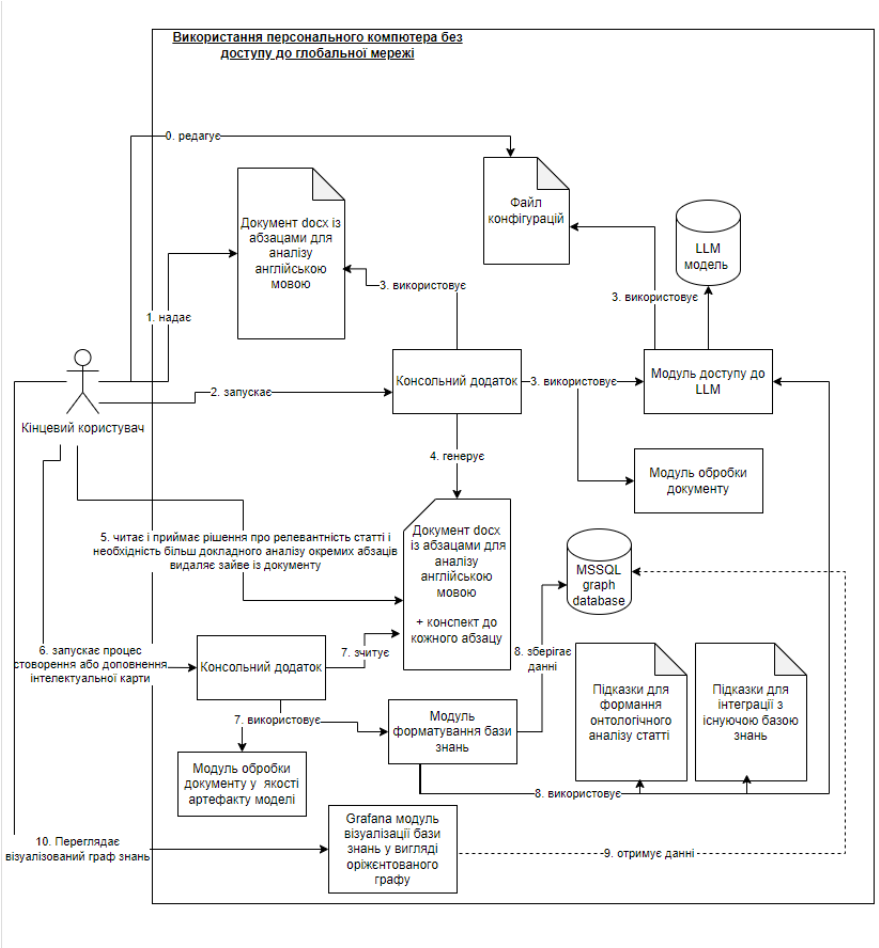


Рисунок 2. Архітектура прототипу

Отже, проблему аналізу великої кількості статтей можна частково вирішити за допомогою використання автономної мовної моделі для побудови інтелектуальної карти досліджуваної області на основі обраних статей.

Такі карти дозволять швидко та ефективно аналізувати велику кількість публікацій групам дослідників, що підвищить якість та звязність створюваних ними робіт, шляхом аналізу ключових ідей що містять числені роботи та онологічної спорідненості досліджень їх взаємозвязків.

[1] Ципляк О.О., Артемчук В.О. «Перспективи застосування автономних нейронних мереж архітектури типу LLAMA для автоматизації аналізу наукових публікацій. Використання штучного інтелекту в наукових дослідженнях та прикладних розробках» : збірник матеріалів науково-практичноїконференції, м. Київ, 11

квітня 2024 р., ІПМЕ ім. Г.Є. Пухова НАН України. – 2024. – с. 17-21.

[2] Ципляк О.О., Артемчук В.О. «Console application development for articles` highlights generation based on artificial intelligence designed using autonomous large language model» збірник матеріалів конференції “Інформаційні технології в освіті, науці й техніці” м. Черкаси, Черкаський державний технологічний університет - 2024

[3] Sun, M., Wang, M., Wegerif, R., & Peng, J. (2022). How do students generate ideas together in scientific creativity tasks through computer-based mind mapping? In Computers & Education (Vol. 176, p. 104359). Elsevier BV. https://doi.org/10.1016/j.compedu.2021.104359

[4] Charleer, S., Klerkx, J., Duval, E., De Laet, T., & Verbert, K. (2016). Creating Effective Learning Analytics Dashboards: Lessons Learnt. In Adaptive and Adaptable Learning (pp. 42–56). Springer International Publishing. https://doi.org/10.1007/978-3-319-45153-4_4

[5] Yurin, A. Yu., & Dorodnykh, N. O. (2020). Personal knowledge base designer: Software for expert systems prototyping. In SoftwareX (Vol. 11, p. 100411). Elsevier BV. https://doi.org/10.1016/j.softx.2020.100411

[6] Taranowski, A. O., & Samoylov, V. D. (2024). Creating the Most Common Types of Test Assignments Using Artificial Intelligence. In Èlektronnoe modelirovanie (Vol. 46, Issue 2, pp. 88–100). National Academy of Sciences of Ukraine (Co. LTD Ukrinformnauka) (Publications). https://doi.org/10.15407/emodel.46.02.088

Д.І. Швайка, В.О. Артемчук

ДИНАМІЧНА СЕРІАЛІЗАЦІЯ PROTOCOL BUFFERS У IOT ПЛАТФОРМІ THINGSBOARD: НОВІ МОЖЛИВОСТІ

У сучасному середовищі Інтернету речей (IoT), ефективність обробки та передачі даних стає ключовим чинником технологічного успіху. Протоколи серіалізації даних відіграють вирішальну роль у цій сфері, забезпечуючи структурований спосіб кодування та передачі даних. Їхня основна функція - стандартизація формату даних, що дозволяє пристроям читати та розуміти одне одного. Широко застосовувані протоколи, такі як JSON, Protocol Buffers та інші, забезпечують цей стандартизований підхід, допомагаючи різноманітним системам IoT здійснювати швидкий та надійний обмін даними.

Більшість платформ з відкритим вихідним кодом вибирають JavaScript Object Notation (JSON) [[1]] для комунікації з IoT пристроями. Google Protocol Buffers (Protobuf) [[2]] є сильним кандидатом на стандартизований метод зв'язку в IoT індустрії, зокрема завдяки їх зменшеним витратам на мережу.

Рішення про використання JSON або Protobuf (або будь-якого формату двійкової серіалізації) залежить від конкретного випадку використання. Наприклад, веб-інтерфейси API зазвичай використовують JSON через розповсюдженість і простоту використання з JavaScript. Однак для внутрішнього зберігання даних або зв'язку між IoT сервісами, особливо в середовищах з обмеженими ресурсами, краще використовувати двійковий формат [[3]].

Інтерес до використання Protobuf безпосередньо на рівні пристрою зростає. Інтеграція пристроїв, які використовують Protocol Buffers, в системи IoT є універсальною проблемою, яка не обмежується жодною конкретною платформою. Отже, для нашого аналізу ми обрали ThingsBoard як наш дослідницький інструмент. Платформа ThingsBoard, визнана однією з провідних платформ IoT з відкритим кодом. Недавні дослідження (2024) [[1]] підкреслили ключову роль, яку вона відіграє в академічному світі.

Статичний характер Protobuf вимагає додаткового втручання розробників для кожного нового типу пристрою, що підриває універсальність і масштабованість платформи, особливо в хмарних розгортаннях. Щоб інтегрувати новий Protobuf-сумісний пристрій, розробники повинні вручну визначити та скомпілювати схему пристрою в кодову базу платформи. Цей процес займає багато часу та може викликати помилки.

Примітним прикладом є інтеграція пристроїв Efento в ThingsBoard за допомогою мережевого протоколу CoAP. Цей пристрій використовує виключно формат Protobuf для серіалізації даних. Версії мікропрограми пристроїв постійно розвиваються та виникає сценарій, за яким платформа повинна постійно адаптуватися для підтримки нових або оновлених

пристроїв.

Вирішуючи цю задачу, ThingsBoard пропонує програмний інструмент, що дозволяє компілювати в режимі реального часу завантажені користувачами схеми Protobuf, що визначають формати даних, які використовуються для обміну інформацією між пристроями та платформою. Цей підхід відходить від традиційних методів, дозволяючи динамічну інтерпретацію схеми Protobuf, таким чином дозволяючи пристроям передавати свої дані в Protobuf без необхідності простою системи або повторної компіляції всієї кодової бази. Рішення інкапсульовано в платформі ThingsBoard через концепцію Device Profile [[5]], які пов'язують пристрої з відповідними схемами передачі даних.

На практиці кожна схема представляє окремий план зв'язку пристрою. Після автентифікації пристрою платформа знаходить пов'язаний з ним Device Profile та використовує відповідну Protobuf схему для інтерпретації повідомлень. Цей процес значно полегшує мережевий трафік, оскільки дані передаються в компактній формі Protobuf і перекладаються в більш детальний формат, як-от JSON, лише тоді, коли цього потребує взаємодія користувача або певні функції системи.

Інноваційне рішення компіляції Protobuf схем у реальному часі, кероване користувачем, може істотно підсилити гнучкість, масштабованість та загальну продуктивність платформ IoT. Цей підхід дозволяє платформі обмінюватися даними з пристроями за допомогою компактних форматів Protobuf, спрощуючи тим самим процес інтеграції нових пристроїв, що використовують цей формат для передачі даних. Для майбутніх досліджень і розробок було б корисно глибше заглибитися в те, як такі динамічні механізми серіалізації даних можуть бути додатково використані іншими сценаріями IoT.

[1] JSON (javascript object notation), 2001. Available from: https://www.json.org/json-en.html.

[2] Google, 2016. Google. Protocol Buffers. Available from: https://developers.google.com/protocol-buffers.

[3] Viotti, J.C. and Kinderkhedia, M., 2022. A survey of json-compatible binary serialization specifications. arxiv preprint arxiv:2201.02089. Available from: https://doi.org/10.48550/ arXiv.2201.02089.

[4] Di Felice, P. and Paolone, G., 2024. Papers mentioning things board: A systematic mapping study. Journal of computer science, 20(5), Mar, pp.574–584. Available from: https://doi.org/10.3844/jcssp.2024.574.584.

[5] ThingsBoard, 2023. Device Profiles. Available from: https://thingsboard.io/docs/user-guide/device-profiles/.

Є.С. Сметана

ОПИС ДІЯЛЬНОСТІ ДИСПЕТЧЕРА РОЗПОДІЛЬЧОЇ ЕЛЕКТРОМЕРЕЖІ ПРИ ОРГАНІЗАЦІЇ ПРОТИАВАРІЙНОГО ТРЕНУВАННЯ

Стратегія ПрАТ «НЕК «УКРЕНЕРГО» на 2017-2026р.р. [1] одним з основних факторів свого розвитку планує підготовку і підвищення кваліфікації персоналу. Характеризуючи поточну ситуацію в енергосистемі України «Стратегія …» констатує наявність тільки обов'язкових програм підготовки і перевірки знань персоналу. В перспективі передбачено створення сучасної професійної системи підготовки персоналу на базі новітніх інформаційних технологій навчання, перевірки знань і тренування, що дозволить сформувати основні компетентності оперативно-диспетчерського персоналу і створити корпоративну автоматизовану базу знань, спрямовану на розвиток його компетенцій.

Аналіз роботи оперативного персоналу [2] підтверджує, що як мінімум третина аварій і аварійних ситуацій в енергосистемі від впливу «людського фактору» є наслідком помилок в результаті браку знань, порушень правил і інструкцій, браку досвіду під час коригування нормальних режимів і локалізації аварійних відхилень і аварій в результаті низької дисципліни.

Незважаючи на велику кількість нормативних документів, що вимагають застосування технічних засобів підготовки при організації роботи з персоналом операторів систем розподілу (ОСР, колишні обленерго) і районних підрозділів (РП), що входять до складу ОСР, тренажери, окрім наявності в деяких мережах дослідних зразків, як правило відсутні. Разом з тим, на цьому рівні сконцентровано близько 40 тис. оперативно-диспетчерського персоналу, який здійснює цілодобове управління електричними мережами.

Малюнок 1 - Структура діяльності диспетчера ОСР.

Протиаварійні тренування є основною формою роботи з персоналом підприємств електричних мереж, покликаною формувати основні компетенції диспетчерського персоналу при управлінні електромережами:

- вміння аналізувати інформацію, отриману з пристроїв відображення і

на її основі ідентифікувати аварійну ситуацію;

— визначати пошкоджене обладнання і складати план дій;
— самостійно орієнтуватись в аварійних ситуаціях і швидко діяти у відповідності з планом дій, правилами і інструкціями для попередження, локалізації і ліквідації аварій;
— виконання перемикань, необхідних для відділення пошкодженого обладнання для запобігання розвитку аварій;
— вироблення стійкості до несприятливих емоційних реакцій, необхідної при ліквідації аварій.

В структурі діяльності диспетчера (мал.1) в якості складових можна виділити:

— мнемосхему (МС), що відображає топологію електромережі і поточний оперативний стан комутаційних апаратів, обладнання і пристроїв;
— модель електричного режиму, що характеризується набором режимних параметрів: генерацією {РГі, QГі}; споживанням {РСі, QСі}, струмом в лініях і обладнанні{ІЛі, ІТі}, напругою у вузлах {Ui};
— модель діяльності (МД) – дії диспетчера по управлінню об’єктом в залежності від поточної ситуації і у відповідності з вимогами нормативно-технічної і службової документації.

Основним елементом при організації протиаварійного тренування є модель робочої діяльності диспетчера в заздалегідь визначеній ситуації. Відповідно до [3] тренування повинно проводитись згідно з обраною темою, складеною програмою тренування і метою відпрацювання навичок.

В даний час на виробництві сценарій тренування готується у вигляді таблиць, що містять опис початкових умов об’єкта до аварії, порушення в системі після аварії, перелік об’єктів, на яких сталося порушення і персоналу, задіяного в ліквідації аварії. Дії персоналу по ліквідації аварії складається для кожного окремо. Це не зручно з точки огляду всієї діяльності одночасно.

Пропонується для представлення сценарію вертикальний пул, розділений на «доріжки», кількість яких відповідає кількості персоналу, задіяному в ліквідації аварії. В порядку підлеглості персонал фіксується зліва направо. Послідовність дій зверху вниз. Синхронізація в часі забезпечується послідовністю виконання дій і за рахунок надсилання і отримання доповідей, розпоряджень, повідомлень і т. і. Крім того, результати виконання розпоряджень персонал може спостерігати на МС об’єкта і оперативно-інформаційному комплексі (ОІК) за рахунок зміни оперативного стану комутаційних апаратів, параметрів режиму і т. і.

Таблична форма сценарію тренування зрозуміла спеціалістам галузі, які користуються нею при організації тренування. Ця форма взята за основу при графічному [4] представленні аналітичної моделі робочої діяльності диспетчера. Для формального представлення моделі робочої діяльності прийнятий опис в нотації BPMN 2.0 стандарту ISO/IEC 19510.

В табл.1 представлено реальний фрагмент протиаварійного тренування.

Таблиця 1 – Фрагмент сценарію тренування.

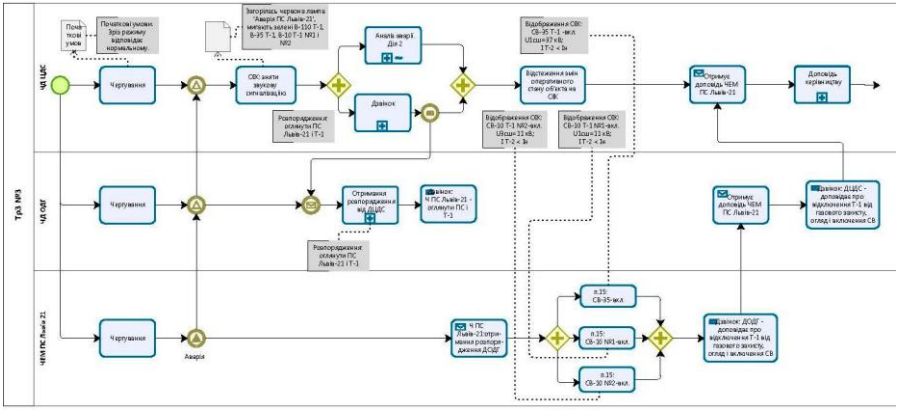
Сценарій тренувального завдання №3			
ЧД ЦДС		ЧД ОДГ	ЧЕМ ПС «Львів-21»
Початкові умови			
Будній день. 10^{00}. Схема мережі нормальна. Режим нормальний.			
Початок аварійної ситуації			
Спрацювала аварійна сигналізація На МС: ПС «Львів-21»: Загорілась червона лампа; В-110 Т-1, В-35 Т-1, В-10 №1,2 Т-1 – мигає зелена лампа		Спрацювала аварійна сигналізація МС: ПС «Львів-21»: Загорілась червона лампа; В-110 Т-1, В-35 Т-1, В-10 №1,2 Т-1 – мигає зелена лампа	Спрацювала центральна сигналізація ***панель 13*** – випав блінкер «Аварійна сигналізація», горить лампа «Блінкер не піднято» ***п.14*** – В-10 №1 Т-1, В-10 №1,2 Т-1, В-35 №1 Т-1, В-110 №1 Т-1 – мигає зелена лампа; ***п.15*** – ІСШ 110 кВ, ІСШ 35 кВ, ІСШ, ІІІСШ 10 кВ – U= «0»; ***п.7*** – спрацювало 11РУ2; В-110 Т-1, В-35 Т-1, В-10 №1 Т-1,В-10 №2 Т-1 – відключений;
Діяльність Д ЦДС по ліквідації аварії			
1	Знімає звукову сигналізацію		
2	Знімає невідповідність оперативного стану вимикачів		
3	Віддає розпорядження Д ОДГ: оглянути ПС Львів-21, Т-1	Отримує розпорядження Д ЦДС	
4		Віддає розпорядження ЧЕМ ПС Львів-21: провести огляд ПС Львів-21, Т-1	Отримує розпорядження Д ОДГ. Оглядає ПС

Де: ЧД ЦДС – черговий диспетчер центральної диспетчерської служби;

ЧД ОДГ – черговий диспетчер оперативної диспетчерської групи;

ЧЕМ ПС – черговий електромонтер підстанції.

Фрагмент аналітичної моделі робочої діяльності представлений на малюнку 2. Аналітична модель відображає власні дії персоналу і їх взаємодію по усуненню аварійної ситуації в часі.



Малюнок 2 – Фрагмент аналітичної моделі робочої діяльності.

На основі аналітичної моделі створюється модель учбової діяльності (тренування). Учбова модель відрізняється від аналітичної більш детальним опрацюванням. Вона відтворює всі дії персоналу з обладнанням, пристроями, ОІК, взаємодію з персоналом інших об'єктів. Модель доповнюється обмеженою кількістю заздалегідь прорахованих зрізів режимів, визначених сценарієм тренування, і модулем оцінки діяльності. Ця модель відтворюється тренажером в процесі тренування.

Для реалізації тренажерів/сценаріїв вибраний крос-платформний рушій UNITY.

При організації індивідуального тренування, діяльність решти персоналу імітується комп'ютером на основі відповідних моделей діяльності персоналу.

Розділ 10 [3] в якості однієї з основних функціональних можливостей тренажера вимагає наявність системи автоматизованої побудови тренувальних вправ у відповідності до сценарію тренування. Модель відтворюваної учбової моделі діяльності буде використана при подальшому створенні візуальної системи автоматизації побудови тренажерів.

[1] Стратегія розвитку ДП «НЕК «УКРЕНЕРГО» 2017-2026. http://reform.energy/media/728/fee7b5ac6f51ead00715132380bb7634.pdf, (2024, лютий,08).

[2] УДК: 612.825.8+613.685 Єна Т. А., Кальниш В.В., Кудієвський Я.В. Гігієнічна і психо-фізіологічна оцінка професійної діяльності диспетчерів енергосистем при аварійній ситуації, ДУ «Інститут медицини праці АМН України» №1,2009.

[3] ПРАВИЛА проведення протиаварійних тренувань персоналу електричних станцій та мереж. Наказ Міненерго України, №991, від 24.12.2013р.

[4] До вибору графічної специфікації діяльності персоналу енергопідприємств / А. О. Бальва, В. Д. Самойлов, Р. П. Абрамович // Моделювання та інформаційні технології. - 2018. - Вип. 85. - С. 45-52. - Режим доступу: http://nbuv.gov.ua/UJRN/Mtit_2018_85_9

Д.Р. Цвілій

ПОБУДОВА СТРУКТУРИ БАЗИ ДАНИХ ОБРОБКИ ФАКТОРНИХ ОЗНАК ДЛЯ ПРОГНОЗУВАННЯ ПОКАЗНИКІВ РОБОТИ ЕНЕРГЕТИЧНОГО РИНКУ

Одним із стратегічних секторів національної економіки є сектор енергетики, від якого залежить стабільність та сталість розвитку країни в цілому. Із-за великого набору стохастичних факторних ознак ринок електричної енергії, наприклад ціна різних сегментів ринку, демонструють поведінку, що є нетиповою для інших ринків: раптові піки, сезонність тощо. В результаті чого ринки електроенергії стають центральною точкою досліджень в енергетичному секторі, і точне прогнозування показників електроенергетичного ринку (цін, попиту тощо) – основним завданням енергетичних компаній. Адже підвищення точності прогнозування та наявність засобів прогнозування як таких, є запорукою економічного прибутку учасника. Це обумовлює необхідність проведення досліджень у напрямку створення простих у використанні, функціональних за призначення і об'єктом автоматизації комп'ютерних систем моделювання процесів конкурентного ринку в частині ціноутворення, які можуть інтегруватися з іншими централізованими організаційно-технічними системами енергоринку.

Однією з першочергових задач побудови такої системи є проектування структури бази даних для збереження та подальшої обробки множини факторних ознак, які будуть використані в процесі прогнозування тих чи інших показників роботи енергетичного ринку. В той же час при розробці структури БД слід враховати різні шляхи надходження таких даних (ручне завантаження користувачем, зовнішні API сервіси тощо) та різну природу даних (15-ти хвилинні часові ряди щодо роботи балансуючого ринку, погодинна інформація роботи ринків РДН та ВДР, щодобова та помісячна зведена інформація тощо). Враховуючи зазначене, структура БД повинна забезпечувати належний рівень гнучкості системи, враховувати різний рівень дискретності даних та можливу залежність факторних ознак між собою.

Таким чином, слід виділити основні сутності БД:

— об'єкти та суб'єкти ринку електричної енергії;

— параметри (перелік факторних ознак, що зберігаються в системі);

— рівні дискретності даних (15-ти хвилинні, погодинні, подобові тощо);

— зв'язки (перелік ієрархічних залежностей параметрами).

Для забезпечення семантичної єдності цих структур варто виділити підхід подання показників суб'єктів функціонування ринку, що безпосередньо пов'язані із обробкою даних, який забезпечить адаптованість структури бази до можливих змін у структурі суб'єктів ринку і особливостей їх функціонування в майбутньому. Цей підхід побудований на механізмі опису мета-даних через створення класифікаторів показників, їх зв'язків та сховища даних (див. рис. 1) [1, 2].

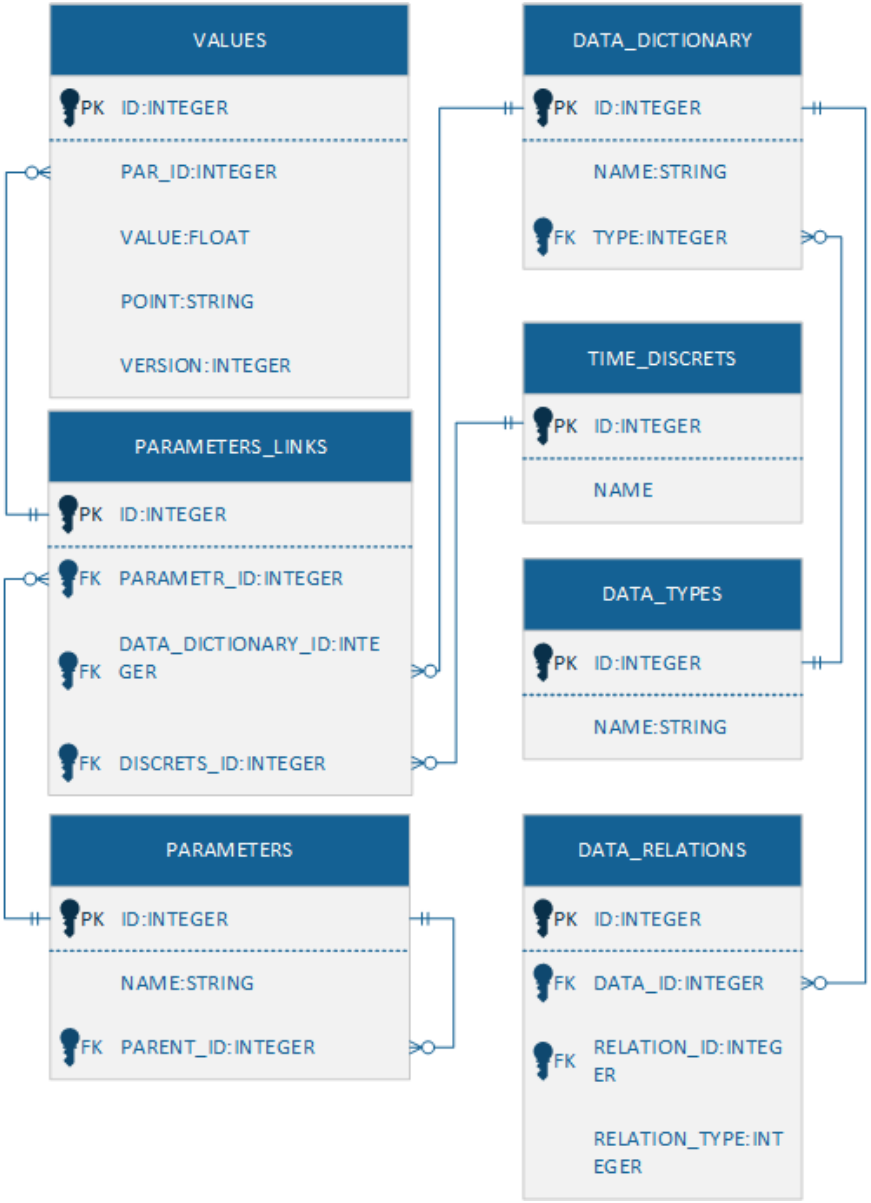


Рисунок 1 – Схема структури бази даних

Сутність DATA_DICTIONARY призначено для збереження довідника

об’єктів та суб’єктів енергетичного ринку (учасників ринку, станцій, блоків тощо), типізація яких визначається переліком типів сутності DATA_TYPES, в тому числі множинна ієрархічна підпорядкованість забезпечується сутністю DATA_RELATIONS.

Сутність PARAMETERS призначено для збереження переліку факторних ознак (ціна РДН/ВДР, обсяг продажу тощо). При цьому, за рахунок сутності TIME_DISCRETS, забезпечується визначення рівня дискретизації факторної ознаки.

Слід звернути увагу на використання символьного типу часової точки (сутність VALUES), що в свою чергу забезпечить належну гнучкість системи при роботі із різними рівнями дискретизації даних.

Враховуючи вищевикладене, використання зазначеного підходу до подання і збереження даних матиме ряд наступних переваг:

— простота та гнучкість роботи з даними;
— мінімізація часу для розробки SQL запитів;
— просте масштабування у випадку необхідності зберігання додаткових даних;
— наявність ієрархічних зв’язків для збереження структурованих даних.

[1] Сховище оперативних даних системи підтримки прийняття рішень для організаційного управління ринком електроенергії / Остапченко К.Б., Євдокимов В.А., Борукаев З.Х. // Електронне моделювання. 2022. Том 44, №3. С.101-112

[2] Проєктування інформаційних систем : Бази даних: [Електронний ресурс] : навч. посіб. для студ. спеціальності 151 «Автоматизація та комп’ютерно-інтегровані технології» / КПІ ім. Ігоря Сікорського ; уклад.: А. І. Жученко, Л. Д. Ярощук. – 2-ге вид., допов.

В.В. Станиціна, В.О. Артемчук, Н.П. Іваненко

ПЕРСПЕКТИВНІ НАПРЯМИ ДЕКАРБОНІЗАЦІЇ ВИРОБНИЦТВА ЦЕМЕНТУ В УКРАЇНІ

Виробництво цементу є енергоємним, вуглецевим і важливим виробництвом в економіці багатьох країн, відповідальним за 5-8% світових викидів вуглекислого газу. Україна входить до топ-40 світових виробників цементу. Заявлена мета ЄС та України щодо досягнення кліматичної нейтральності вимагає впровадження заходів з декарбонізації цього виробництва. Останніми роками у світі зростає увага до проблеми декарбонізації в цементній промисловості, про що свідчить кількість відповідних публікацій.

У виробництві цементу викиди вуглекислого газу утворюються в процесі випалу сировини та спалювання палива, а також є непрямі викиди, пов'язані зі споживанням електроенергії.

Реальні стратегії декарбонізації в Україні включають заміну сировини у виробництві клінкеру та цементу, використання альтернативних видів палива, енергозбереження та використання відновлюваних джерел енергії. Щодо заміщення сировини у виробництві клінкеру використовується зола-винос теплових електростанцій, доменних печей, конвертерний шлак. Спочатку ці відходи були значно дешевшими і замінювали до 20% сировини на деяких цементних заводах. Однак із збільшенням попиту економічна привабливість їх використання зменшилася, зменшивши частку сировини, що заміщавала карбонатну сировину [1, 2]. Підприємства, які експортують цемент до ЄС, під впливом механізму регулювання кордонів викидів вуглецю (CBAM), швидше за все, замінять сировину навіть дорожчими відходами. Крім того, можна очікувати збільшення використання палива, отриманого з відходів. Очікуване підвищення ставки податку на викиди CO2 ще більше стимулюватиме заміщення.

Всі заходи з декарбонізації цементного виробництва зрештою вплинуть на його енергоємність, обсяги та структуру паливно-енергетичних ресурсів, що використовуються у даному виробництві

[1] European Commission. Joint Research Centre. Institute for Prospective Technological Studies. (2013). Best available techniques (BAT) reference document for the production of cement, lime and magnesium oxide: Industrial Emissions Directive 2010/75/EU (integrated pollution prevention and control). Publications Office. https://doi.org/10.2788/12850

[2] Plasykhin S.V. (2020) Handbook on resource-efficient and clean production. Cement industry K.: Center for resource-efficient and clean production. 96 p

В.О. Артемчук, Ю.О. Гарбуз

РОЗВИТОК МЕТОДІВ І ЗАСОБІВ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ТА РЕЗИЛЬЄНТНОСТІ ЛОКАЛЬНИХ ДЕЦЕНТРАЛІЗОВАНИХ ЕЛЕКТРОЕНЕРГЕТИЧНИХ СИСТЕМ В УКРАЇНІ

Війна має суттєвий негативний вплив на роботу української енергетичної галузі. Через своє економічне, гуманітарне і геополітичне значення об'єкти енергетичної інфраструктури є особливо частими цілями російської агресії. Тим не менш, українська енергосистема демонструє високу стійкість, а енергетики – надзвичайну професійність у забезпеченні стабільної роботи галузі навіть в умовах війни.

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. Зокрема, найбільша в Європі АЕС (Запорізька) працює в енергосистемі України, але знаходиться під постійним тиском російських окупантів. Виробнича потужність цієї станції складає 6000 МВт, або 43% від загальної потужності усіх українських атомних електростанцій.

Масштабні атаки на об'єкти енергетичної інфраструктури, що тривають з жовтня 2022 року, створюють нові виклики не тільки для стабільного функціонування енергетики України, а й європейської енергетичної системи ENTSO-E, до якої Україна приєдналася 16 березня 2022 року.

На цьому фоні вкрай важливими є дослідження щодо забезпечення та підвищення резильєнтності (від. англ. resilience – резильєнтність, стійкість, життєстійкість, спроможність відновлюватись) енергетичної галузі України. Крім того, актуальність досліджень в цьому напрямку підтверджується чітким трендом на збільшення релевантних наукових публікацій в світі (від десяти публікацій в наукометричній базі Scopus в 2013 році до більше ста в 2022 р.).

Про актуальність та перспективність досліджень в цій галузі також свідчить той факт, що в плані цифровізації енергетичної системи ЄС (Digitalising the energy system - EU action plan. Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions, Strasbourg, 18.10.2022) вступ та окремий розділ (Strengthening Cybersecurity and Resilience in the Energy System) пов'язані саме із забезпеченням резильєнтності енергетики.

Не дивлячись на те, що наразі ще не існує єдино прийнятого визначення «резильєнтності» в наукових публікаціях та нормативних документах в світі, але одним з найбільш повних можна вважати визначення, що запропоноване на основі публікації Elmqvist, T., Andersson, E., Frantzeskaki, N. et al. (2019) Sustainability and resilience for transformation in the urban century. Nature

Sustainability, 2, 267–273: резильєнтність певної системи – це здатність системи протидіяти гібридним загрозам, поглинати збурення, реорганізовуватися, підтримувати, по суті, ті самі функції та зворотні зв'язки з часом і продовжувати розвиватися за певною траєкторією. Ця здатність випливає з характеру, різноманітності, надмірності та взаємодії між компонентами, залученими до створення різних функцій. Резильєнтність є атрибутом системи та застосовується до різних підсистем.

Разом з тим, внаслідок збройної агресії Росії електроенергетична галузь України загалом і понад 1000 МВт потужностей ВДЕ потребують відновлення. Тому, враховуючи також нові виклики нестабільності та невизначеності, створювані повномасштабною війною, стан енергосистеми України та світові тенденції до декарбонізації, децентралізації та діджиталізації (3Д-стратегія), 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 ВДЕ приєднані до розподільних мереж, а лише 10% - до високовольтних мереж. Відповідно, розвиток ВДЕ є важливою складовою розвитку розподільної генерації. А отже критично важливим є завдання створення концептуальної моделі «зеленої» трансформації локальної резильєнтної енергетичної системи України.

Також варто відзначити, що мікро/міні гідроелектростанції (ГЕС) як один з видів ВДЕ, є актуальним напрямком як в контексті 3Д-стратегії та і при загрозі виникнення блек-ауту, адже мікро/міні ГЕС можуть працювати як автономно, так і на централізовану мережу. Підвищення енергоефективності мікро/міні ГЕС можливе завдяки реалізації цифрової сучасної автономної ГЕС за допомогою використання технічних засобів і методів керування параметрами системи на основі гібридного методу при неповній визначеності параметрів навантаження, що дозволить покращити якість регулювання електричних і технологічних параметрів з забезпеченням заданих показників якості споживаного з мережі струму навантаженнями та забезпеченням електромагнітної сумісності з мережею живлення. Окрім підвищення енергоефективності вирішується завдання інтеграції з ОЕС України та її подальшої інтеграції в ENTSO-E. Таким чином, вирішується завдання Енергетичної стратегії України до 2050 року, що передбачає відновлення енергетичного сектору за найсучаснішими технологіями, зміцнення стійкості системи та посилення енергетичної безпеки України і європейського континенту в цілому. Ключове завдання цієї стратегії - перетворення України на енергетичний хаб Європи, який допоможе континенту остаточно позбутися залежності від російського викопного палива завдяки виробленій в Україні чистій енергії, що особливо важливо у повоєнний період на фоні стрімкого відновлення та розвитку промислового виробництва та, як наслідок, збільшення попиту на електричну енергію.

Метою роботи є підвищення ефективності та резильєнтності локальних децентралізованих електроенергетичних систем в Україні. Зміст роботи

зводиться до вирішення заступних завдань: 1) критичний аналіз сучасного стану розробок, проблем та попиту щодо методів, засобів та алгоритмів підвищення ефективності функціонування резильєнтної локальної енергосистеми з використанням альтернативних джерел енергії та накопичувачів, та, зокрема, щодо регулювання параметрів мікро/міні гідроелектростанцій із застосуванням гібридних систем живлення та інтелектуальних систем керування; 2) розроблення моделі резильєнтної локальної енергосистеми зі застосуванням альтернативних джерел енергії та накопичувачів; 3) оцінювання моделі «зеленої» резильєнтної локальної енергосистеми на прикладі територіальної громади, району або області; 4) розроблення математичної моделі мікро/міні гідроелектростанції з урахуванням особливостей автономного режиму роботи та невизначеності параметрів споживання; 5) розроблення методичних рекомендацій щодо впровадження моделі «зеленої» резильєнтної локальної енергосистеми України; 6) дослідження впливу застосування альтернативних джерел енергії та накопичувачів в резильєнтній локальній енергосистемі на зміну локального споживання та зменшення витрат операторів систем розподілу на розподіл електричної енергії; 7) розроблення нового методу регулювання параметрами мікро/міні гідроелектростанцій із застосуванням гібридних систем керування, які поєднують класичні і інтелектуальні методи та виконують технічні вимоги при неповній визначеності параметрів мережі живлення (споживання), а також забезпечують задані показники якості споживаного та генерованого струму (електромагнітну сумісність), що у підсумку дає змогу підвищити енергоефективність системи; 8) проведення експериментальних досліджень розробленого методу регулювання на діючій міні/мікро гідроелектростанції. Виконання роботи здійснюється на базі отриманих результатів багаторічних досліджень в ІПМЕ ім. Г.Є.Пухова НАН України, а також Інституту електродинаміки НАН України дослідницькою групою молодих вчених згаданих вище установ.

М.В. Антонішин, Є.М. Харламов

РИЗИКИ ВИКОРИСТАННЯ МОБІЛЬНИХ ПРОГРАМНИХ ЗАСТОСУНКІВ В ЕНЕРГЕТИЧНІЙ СФЕРІ

Забезпечення кібербезпеки енергетичної сфери є стратегічною ціллю №2 Стратегії Енергетичної безпеки України [1]. Використання мобільних програм все зростає, як для контролю витрат електроенергії пересічними користувачами та проведення через ці програми оплати за послуги енергопостачання, так і для управління спеціалізованими системами через спеціально розроблене програмне забезпечення або тонкий клієнт. Тому в Стретегії кібербезпеки визначено, що необхідно: «розробити нові національні стандарти у сфері кібербезпеки, організаційні та технічні вимоги, що стосуються безпеки застосунків, мобільних пристроїв, робочих станцій, серверів і мереж, моделей хмарних обчислень, з урахуванням європейських та міжнародних стандартів» [2]. Основними ризиками, які можуть нести мобільні програмні застосунки, які використовуються в енергетичному секторі це:

- **несанкціонований доступ до даних.** Зловмисники можуть отримати доступ до конфіденційних даних, таких як дані про клієнтів, комерційну таємниц. та дані про електромережі, використовуючи вразливості в мобільних програмах, шляхом зламу користувацьких акаунтів;
- **шкідливе програмне забезпечення.** Зловмисники можуть розповсюджувати шкідливе програмне забезпечення через мобільні програми, яке може пошкодити обладнання, викрасти дані або вивести з ладу електромережі;
- **відмова в обслуговуванні (DDoS).** Зловмисники можуть завдати шкоди енергетичним компаніям шляхом DDoS-атак, перевантажуючи їх сервера за допомогою генерації запитів з мобільних програм трафіком, який може призведе до перебоїв в роботі та забезпечення надання сервісів.
- **фішинг.** Зловмисники можуть використовувати мобільні програми для розповсюдження фішингових атак, щоб обдурити користувачів та змусити їх розкрити свої конфіденційні дані.

Схематично типова схема атаки на інформаційно-комунікаційну інфраструктуру візуалізовано на Рисунку 1.

Для запобігання ризиків кібербезпеки мобільних програмних продуктів необхідно:

- **забезпечити процес безпечної розробки мобільних програмних застосунків.** Мобільні програми повинні розроблятися з урахуванням найкращих практик кібербезпеки, щоб мінімізувати можливість появи уразливостей, в тому числі проведення тестування наявність уразливостей. Для цих цілей використовуються спеціалізовані інструменти – сканери уразливостей;

- **впровадження та використання надійних методів аутентифікації.** Захист акаунтів має використовувати надійні методи аутентифікації, такі як багатофакторна аутентифікація;
- **виконувати регулярне оновлення мобільних програм та операційних систем.** Регулярне оновлення мобільних програм, мобільних операційних систем та компонентів, які використовуються в процесі розробки зменшують ризики появи уразливостей;
- **проведення навчання особовго складу.** Персонал повинен пройти навчання з питань кібербезпеки та навчитися розпізнавати та уникати кіберзагрози;
- **використання рішень з кібербезпеки для мобільних пристроїв та операційних систем.** Енергетичні компанії повинні використовувати рішення з кібербезпеки, такі як мобільні антивіруси та системи моніторингу.

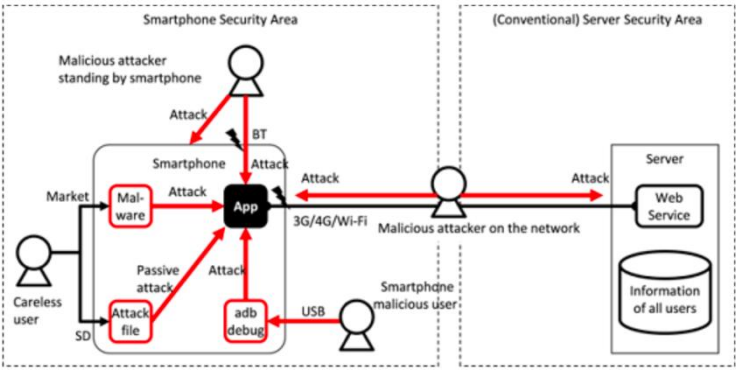


Рисунок 1 – Типова схема атаки на серверну архітектуру через мобільний застосунок

[1] Стратегія енергетичної безпеки, схвалена Кабінету Міністрів України від 4 серпня 2021 року №907-р. https://zakon.rada.gov.ua/laws/show/907-2021-%D1%80#Text

[2] Проект Стратегії кібербезпеки України (2021-2025 роки). https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf

[3] Five in 5: Cybersecurity in the energy sector. Deloitte article. https://www2.deloitte.com/us/en/pages/consulting/articles/cybersecurity-energy-sector.html

XLII
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
15 травня 2024 р.

Collection of materials of the XLII 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 15, 2024 / PIMEE of NAS of Ukraine. - 2024. - 171 p.

Збірник матеріалів XLII Науково-технічної конференції молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, м. Київ, 15 травня 2024 р. / ІПМЕ ім. Г.Є. Пухова НАН України. – 2024. – 171 с.

Інформаційна підтримка:

Сторінка конференції на сайті Інституту

Telegram канал РМВ НАН України