

НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ



**ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ
В ЕНЕРГЕТИЦІ ІМ. Г.С. ПУХОВА**



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

24 листопада 2022 року

Київ – 2022

УДК [621.3+620.9]::[004[056.53+42+94] + 504.06]

ББК 31

Б-39

Рекомендовано до друку
Вченою радою Інституту
проблем моделювання в
енергетиці ім. Г.Є. Пухова НАН
України (протокол №11 від
28 жовтня 2022 р.)

Б-39 **Безпека енергетики** в епоху цифрової трансформації, IV науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України : матеріали (Київ, 24 листопада 2022 р.). Київ : ПІМЕ ім. Г.Є.Пухова НАН України, 2022. 93 с.

В-39 **Energy security** in the digital transformation era, IV scientific-practical conference of the G.E. Pukhov Institute for Modeling in Energy Engineering National Academy of Sciences of Ukraine : materials (Kyiv, November 24, 2022). Kyiv: PIMEE NAS of Ukraine, 2022. 93 p.

© Автори публікацій, 2022

© ПІМЕ ім. Г.Є.Пухова НАН України, 2022

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

**МАТЕРІАЛИ ІV НАУКОВО-ПРАКТИЧНОЇ
КОНФЕРЕНЦІЇ**

**БЕЗПЕКА ЕНЕРГЕТИКИ В ЕПОХУ ЦИФРОВОЇ
ТРАНСФОРМАЦІЇ**

**24 листопада 2022 року
м. Київ**

2022

Вельмишановний учасник _____

Запрошуємо Вас прийняти участь в роботі IV науково-практичної конференції «Безпека енергетики в епоху цифрової трансформації», яка буде проходити 24 листопада 2022 року в Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України (м. Київ).

ОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ

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

ПРОГРАМНИЙ КОМІТЕТ

Мохор Володимир Володимирович

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

Чемерис Олександр Анатолійович

доктор технічних наук,
заступник директора з наукової роботи

Артемчук Володимир Олександрвич

доктор технічних наук,
заступник директора з науково-організаційної роботи

Чьочь Вікторія Володимирівна

кандидат технічних наук,
т.в.о. заступника директора з науково-технічної роботи

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Артемчук Володимир Олександрвич

доктор технічних наук,
заступник директора з науково-організаційної роботи

Клименко Тетяна Михайлівна

завідувачка науково-організаційного відділу

Цуркан Оксана Володимирівна

молодший науковий співробітник

Dubovkina I.,

*Institute of Engineering Thermophysics of NASU, Ukraine,
leading researcher,
dubovkinai@ukr.net*

Myronchuk A.,

Institute of Engineering Thermophysics of NASU, Ukraine

ENERGY SAVING TECHNOLOGY OF HYDRODYNAMIC TREATMENT OF NUTRIENT SOLUTIONS

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. 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]. Hydroponic technology involves the use of a nutrient solution as the main source of nutrient supply to plants, while the root system is formed either freely or in an artificially created environment (basalt mat, coco mat, peat mixture).

Methods and methods of cleaning nutrient solutions are relevant for hydroponics. One of the promising methods of cleaning hydroponics solutions is hydrodynamic treatment. Bubbles of weakly ionized gas are formed in high-speed liquid flows under the conditions of hydrodynamic processing. At the same time, chemically active radicals are formed, which contribute to the oxidation of impurities of organic and inorganic nature in nutrient solutions. During the hydrodynamic

treatment of nutrient solutions, colloids and particles, inside which bacteria can be contained, are destroyed. Thus, disease-causing organisms are deprived of protection against other chemical and physical influences. The bactericidal effect of hydrodynamic treatment is directly proportional to its intensity, frequency or treatment time. The effect of hydrodynamic treatment on nutrient solutions of hydroponics is reduced to the splitting of water molecules in the bubbles that are formed as a result of the hydrodynamic effect of this method. The effect of hydrodynamic treatment leads to a change in the physical and chemical properties of nutrient media: an increase in pH, electrical conductivity, an increase in the number of free ions and active radicals, structuring and activation of molecules.

The influence of cumulative liquid jets, local pressure and temperature pulsations during the collapse of microbubbles can cause the death of bacteria, which leads to the disinfection of hydroponic solutions.

The control of potential of hydrogen is extremely important, not only in hydroponics but in soil as well. Plants lose the ability to absorb different nutrients and fertilizers when the potential of hydrogen varies. In hydroponics system, potential of hydrogen is constantly changing during the plant grows.

If potential of hydrogen changes less than 0,1 unit then this does not significantly affect. Therefore pH control is a requirement in hydroponic solutions, because the plant growth depends on this. The pH range from 5,5 to 7,5 is most favorable for the availability of nutrients from most water nutrient solutions[3].

Prepared examples of water and water solutions were used as the model mediums in hydroponic system for experiments. Determination of change of potential of hydrogen of liquid samples of the model systems is carried out with use analogue pH-meter-millivoltmeter pH-150 M with external electrodes.

Study was carried out at the pilot unit designed and created at the IET HASU, the main part of the unit is a rotary pulsed apparatus in which realized alternating impulses of pressure. Through researches increases pH of the pure water on 15% have been established, thus the hydrogen potential of the water prepared on technology for hydroponic system has raised on 14-17,5%.

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

As a result of research, it was found that the energy saving technologies technology of hydrodynamic treatment by alternating impulses of pressure can greatly reduce energy, power and resource consumption, increase efficiency of the growing crops.

REFERENCES

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

3. Dubovkina Iryna (2017). Change of physical and chemical parameters of the liquid binary systems by alternating impulses of pressure, Ukrainian Food Journal, Volume 6, Issue. 1, p. 142-154.

Ковальчук Людмила Василівна,
ІПМЕ ім. Г.Є. Пухова НАН України,
провідний науковий співробітник, доктор технічних наук, професор,
lusi.kovalchuk@gmail.com

Кучинська Наталія Вікторівна,
ІН ФТІ КПІ ім. Ігоря Сікорського,
доцент, кандидат технічних наук,
n.kuchinska@gmail.com

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ СМАРТ-КОНТРАКТІВ В ЕНЕРГЕТИЦІ ТА НАЯВНІ ВРАЗЛИВОСТІ, ЯКІ ПОТРІБНО ВРАХУВАТИ ДЛЯ МОЖЛИВОСТІ ЇХ ВИКОРИСТАННЯ

Анотація. Смарт-контракт - це програмний код, основою якого є блокчейн і який виконуються відповідно до закладених в цей код інструкцій. Внаслідок незмінності блокчейну після ініціації в блокчейні смарт-контракт не можна модифікувати або оновлювати. Тобто розробники змушені врахувати всі загрози безпеці функціонування смарт-контрактів перед їх розгортанням в мережі блокчейн. В даній роботі авторами розглянуто основні категорії атак на смарт контракти; а саме атаки на протокол консенсусу блокчейн, помилки в смарт-контракті, зловмисне програмне забезпечення і шахрайські дії. Обговорюються також перспективи і напрямки безпечного використання смарт-контрактів в енергетичній галузі.

Abstract. Smart contract is a program code, the basis of which is the blockchain and which is executed according to the instructions embedded in this code. Due to the immutability of the blockchain, once initiated on the blockchain, the smart contract cannot be modified or updated. That is, developers are forced to take into account all security threats to the operation of smart contracts before deploying them in the blockchain network. In this work, the authors considered the main categories of attacks on smart contracts; namely attacks on the blockchain consensus protocol, bugs in smart contract, malware and fraudulent activities. Prospects and directions for the safe use of smart contracts in the energy industry are also discussed.

Технології смарт-контрактів дозволяють користувачам формувати децентралізовані цифрові угоди без участі третьої сторони. На поточний момент часу технологія смарт-контрактів залучила такі сектори, як охорона здоров'я, управління бізнесом, енергетика та страхування. Проте поступове розповсюдження технології привертає увагу потенційних зловмисників, що призводить до серйозних зловживань. В даній статті розглянуто можливі вразливості та атаки на технологію смарт-контрактів.

Вважається, що вперше ідею смарт-контрактів висловив Нік Сабо у 1996 р. [1, 2], хоча незалежно від нього схожі ідеї також висловлювали також –

Девід Чаум, Марк Міллер. У своїх роботах він визначає смарт-контракт як «цифрове подання набору зобов'язань між сторонами, яке містить протокол виконання цих зобов'язань» та зазначає, що «нові інституції і нові способи формалізації відносин цих інституцій стали можливими» завдяки використанню смарт-контрактів.

В сучасній літературі існує велика кількість різних визначень смарт-контракту, при цьому кожне визначення підкреслює якісь певні особливості, що є актуальними у відповідному контексті. Наведемо деякі з них.

Смарт-контракт (англ. *smart contract* — «розумний контракт»):

- різновид угоди в формі закодованих математичних алгоритмів, укладення, зміна, виконання і розірвання яких можливі лише з використанням комп'ютерних програм (блокчейн платформ) в рамках мережі Інтернет;

- набір обіцянок у цифровому форматі, включно з протоколами, за якими сторони виконують ці обіцянки;

- частина коду спеціального призначення, який виконує складний набір інструкцій у блокчейні [3];

- комп'ютеризований протокол транзакцій, який перевіряє, чи дотримуються учасники транзакцій правила, попередньо визначені в умові контракту [4];

- регулювання відносин сторін шляхом закріплення їх вираженої волі у формі певного коду, який придатний для зчитування комп'ютером.

Смарт-контракт сам по собі не є ні контрактом, ні володіє внутрішнім «розумом» – це просто певний програмний код, що активується з особистого облікового запису (акаунту) та має доступ до виконання функцій, які в ньому прописані. Контракт не має внутрішнього «розуму», окрім аспекту автоматичного виконання. Смарт-контракт просто перевіряє, чи дотримуються учасники транзакцій правила, попередньо визначені в смарт-контракті. Якщо вони це роблять, транзакцію перевіряють, якщо ні, транзакцію відхиляють. Смарт-контракти швидше потрібно сприймати ефективними та автоматичними, ніж «розумними».

Не зважаючи на те, що смарт-контракти є дійсно зручним інструментом, вони на даний час не набули значного поширення на рівні державних органів – впершу чергу через те, що їх законодавчий статус не визначений. Так, єдиною країною, де смарт-контракти визнані законодавчо, є Білорусь (2016) [5].

Проте декілька штатів прийняли законодавство, що дозволяє використовувати смарт-контракти та технологію блокчейн у різних комерційних контекстах. Смарт-контракт, при цьому зазвичай визначається в такому законодавстві як програма, керована подіями, або комп'ютеризований протокол транзакцій, який працює в розподіленому, децентралізованому, спільному та реплікованому реєстрі (ledger), яка виконує контракт або будь-яке положення контракту, переймаючи під опіку та вказівки щодо перенесення активів у реєстр.

У 2017 році Арізона лідувала, прийнявши законодавство, яке дозволяє використовувати смарт-контракти в торгівлі та запобігає відмові в наданні контракту юридичної сили, дійсності чи примусового виконання лише через те, що контракт містить умову смарт-контракту. Законопроект також визнає підписи та записи, захищені за допомогою технології блокчейн, дійсними електронними підписами та записами відповідно до законодавства штату. Теннессі прийняв аналогічне законодавство в 2018 році. Наразі в законодавчих органах штатів Небраска, Нью-Йорк і Огайо розглядаються законопроекти, які дозволять використовувати смарт-контракти та умови смарт-контрактів у кожному штаті. Інші штати продовжують вивчати законодавство, що стосується використання як смарт-контрактів, так і технології блокчейн.

У Вермонті в 2018 році був підписаний законопроект, який дозволяє компаніям з обмеженою відповідальністю, організованим з метою «ведення бізнесу, який використовує технологію блокчейн для істотної частини своєї господарської діяльності», обирати статус компанії з обмеженою відповідальністю на базі блокчейну (blockchain-based limited liability company, BBLLC). Законопроект дозволяє BBLLC використовувати технологію блокчейн для різних аспектів корпоративного управління, включаючи використання смарт-контрактів для адміністрування процедур голосування BBLLC [6].

Смарт-контракти можуть існувати тільки всередині певного середовища, що має безперешкодний доступ виконуваного коду до об'єктів смарт-контракту. Найбільш розповсюдженим середовищем існування смарт-контрактів є блокчейн. Смарт-контракти на блокчейні – застосунок, середовищем існування якого є блокчейн. Вперше смарт-контракти були розроблені в блокчейні Ethereum (2013), співзасновником якого є засновник журналу Bitcoin Magazine В.Бутерін. Він висунув ідею універсальної децентралізованої блокчейн-платформи, в якій будь-хто бажаючий може програмно реалізувати різні системи зберігання та обробки інформації. Головна умова — дії повинні бути описані як математичні правила.

Слід зазначити, що некоректно написаний або реалізований смарт-контракт може завдати суттєвих збитків. Так, у червні 2016 року на мережу Ethereum була виконана атака, внаслідок якої з різних гаманців було виведено близько 50 млн USD.

Також було декілька атак на смарт-контракти, які коштували значних сум грошей. Однак атаки на DAO та Parity Wallet є найбільш обговорюваними. DAO - смарт контракт з відкритим кодом, який дозволяв будь-кому обмінювати токени DAO на Ether. Цей метод обміну допоміг зібрати близько \$ 150 мільйонів краудфандінгу. Учасникам з токенам DAO було дозволено голосувати за пропозиції і отримувати винагороди, якщо це принесло прибуток. Проте контракт DAO містив серйозні недоліки, що дозволяло зловмисникам зняти кошти. Існувала лазівка, яка дозволяла зловмиснику запитувати кошти від смарт-контракту численну кількість раз

до оновлення балансу. Вразливість сталася через помилки в коді, яких розробники не передбачили можливість рекурсивного виклику. Саме це і дозволило зловмисникам викрасти ефір на мільйони доларів за перші кілька годин.

Подібно чином відбувся злам Parity Wallet. Недолік дозволяв зловмиснику видалити понад 150 000 ETH (\$ 30 мільйонів). Для того, щоб провести атаку було виконано дві транзакції прагнучи придбати право власності на Multisig, так, щоб витратити всю валюту. Після того, як атака була здійснена, було ініційовано контракт Parity Multisig Wallet Library. Однак він містив помилку, яка дозволяла запускати будь-кому initWallet. Напад було здійснено двічі; тому ці атаки і називають Parity Wallet hack 1 і 2. Під час першої атаки зловмисник міг змінити статус гаманця ініціювавши виклик initWallet. У результаті зловмисник вважався власником і без жодних перешкод виводив кошти.

Виділимо основні умови існування смарт-контракту:

- можливість використання цифрового підпису та асиметричного шифрування;
- існування відкритих, децентралізованих, доступних сторонам контракту баз даних, яким вони довіряють, для виконуваних транзакцій, робота яких повністю виключає людський фактор;
- децентралізація середовища виконання розумного контракту;
- правдивість джерела цифрових даних. [7]

Зі смарт-контрактом пов'язані наступні об'єкти:

- підписанти — сторони смарт-контракту, які погоджуються з умовами або відмовляються від умов контракту з використанням електронних підписів;
- предмет договору — об'єкт, що знаходиться всередині середовища існування розумного контракту, або ж повинен забезпечуватися безперешкодний, прямий доступ розумного контракту до предмету договору без участі людини;
- умови повинні мати повний математичний опис, який можливо запрограмувати в середовищі існування розумного контракту;
- децентралізована платформа;
- об'єкти розумного контракту.

Зі смарт-контрактом пов'язані як мінімум два відкритих ключі підпису: ключ того, хто створив контракт, та ключ самого контракту. Активувати смарт-контракт можна лише з особистого аккаунта, але активований смарт-контракт в процесі виконання може звертатись до іншого смарт-контракту. Взагалі кажучи, змінити смарт-контракт, який вже розміщено у блокчейні, неможливо. Проте, за певних умов, його можна знищити і створити новий — лише в тому випадку, якщо в ньому є функція SELFDESTRUCT.

Виділимо основні властивості смарт-контрактів, які їх характеризують:

Розподіленість. Смарт-контракти відтворені а розподілені по всім нодам. (= децентралізація)

Детермінованість. Виконують дії, які в них записані, у відповідності до домовленостей, які в них записані. Результат завжди прогнозований.

Автономність. Можуть автоматизувати всі види задач, працюючи як самовоконувана програма. Якщо смарт-контракт не активізований, то він нічого не виконує. Не можна змінювати умови смарт-контракту після його розробки.

Незмінність. Неможна змінити процес роботи смарт-контракту після його розробки та активації. Лише якщо він містить певну функцію, через яку можна робити певні зміни.

Відсутність довіри. Сторони можуть взаємодіяти за допомогою смарт-контракту навіть не знаючи один одного.

Прозорість. Код смарт-контракту доступний розміщено у блокчейн і він доступний всім.

Економія. Не потрібні витрати на «бюрократизацію».

Дослідження показують, що більшість блокчейн атак підпадають під наступні категорії [8], які зловмисники використовують для ініціювання атак відповідно до своїх можливостей.

1. *Зловмисні дії*, які можуть включати розповсюдження зловмисного програмного забезпечення з метою оманити користувачів. Цей тип експлуатації переважно ініціюється через Інтернет для компрометації особи користувача або зловмисні дії за допомогою шкідливих програм або вірусів. Такі шкідливі дії можуть серйозно вплинути на фінансове становище жертви. Зловмисні атаки можуть виникати в будь-якій формі наприклад електронний лист із гаманця з проханням синхронізувати обліковий запис з мережею, яка щойно була розгалужена.

2. *Слабкості протоколу.* Блокчейн містить консенсусний протокол для забезпечення безперервної роботи мережі. Різні блокчейн-платформи працюють на різних протоколах. Зловмисні дії через слабкий протокол консенсусу були дуже поширені останнім часом, хоча часто проведення таких атак буде дорогим. Однак успішне виконання таких атак може видалити блоки з ланцюжка, повністю знищити блокчейн, або отримати повний контроль над ціною криптовалюти. 51% атак, нечесний майнінг, та 34% атак є деякими атаками техніки, які виникають через слабкість протоколів. Протокол PoW передбачає, що 50% мережевих майнерів завжди будуть чесними. Таким чином, зловмисники, які містять понад 50% потужностей, можуть отримати контроль над мережею. Слабкий консенсус також може призвести до багатьох атак, пов'язаних з мережею блокчейн. Атака Сивілли (англ. Sybil attack) дозволяє зловмиснику встановити кілька шкідливих вузлів через мережу блокчейну Bitcoin. Шкідливі вузли потім використовуються для пошкодження мережі, проведення непривілейованих транзакції або заміни дійсних транзакцій. Так само атака затемнення (Eclipse attack) може бути виконана для маніпулювання P2P-мережею, для отримання

повного контролю над інформацією ноди. Таким чином, незалежно від децентралізації мережа блокчейн все ще може бути скомпрометована через слабкий консенсус.

3. *Обман (Defraud)*. Дана вразливість обманює торговців, щоб скористатися перевагами нестабільності цифрових транзакцій. Обман може змусити торговця віддати товари до повного підтвердження транзакції. Так зазвичай, біткойн транзакція підтверджується після 6 транзакцій. Проте, споживач може переконати торговця відпустити товар без очікування до 6 транзакцій, так що, наприклад, можуть бути ініційовані атаки подвійної витрати на 1 підтвердження або n підтверджень. Подібним чином діють різні роздрібні торговці, що дозволяє споживачам отримувати їх продукт миттєво. Наприклад, купити каву з кав'ярні. Розглянемо сценарій, коли супротивник вдається витратити ту саму криптовалюту протягом короткого проміжку часу. Якщо друга транзакція буде прийнята майнерами пулу для обробки, тоді перша транзакція буде відхилена, потенційно залишаючи торговця без оплати за надані товари.

4. *Помилки програмного забезпечення*. Дана вразливість виникає, коли є помилка в коді смарт-контракту у випадку, коли розробники не змогли виявити помилки коду в децентралізованому додатку. Зловмисники здатні викачати всі гроші з гаманця контракту через прості помилки коду. Додатки для смарт-контрактів є схожі на веб-додатки, які працюють через блокчейн. Можливі помилки програми не тільки дозволяють зловмисникам викрасти гроші, але й впливають на додаток функціонувати по-різному.[9,10]

Розглянемо більш детально відомі атаки, які використовують помилки програмного забезпечення, та від для яких існує потреба в захисті при написанні смарт-контрактів.

Стан гонитви (race condition) Однією з основних небезпек виклику зовнішніх контрактів є те, що вони можуть взяти на себе контрольний потік і внести зміни у ваші дані, яких функція виклику не очікувала. Цей клас помилок може приймати різні форми, і обидві основні помилки, які призвели до краху DAO, були помилками такого роду.

- *Повторне використання (Reentrancy)*. Перша версія цієї помилки, яку було помічено, пов'язана з функціями, які можна було викликати повторно до завершення першого виклику функції. Це може призвести до деструктивної взаємодії різних викликів функції. Умови міжфункціональної гонитви.

- *Міжфункціональний стан гонитви (Cross-function Race Conditions)*. Зловмисник може здійснити атаку, використовуючи дві різні функції, які мають однаковий стан.

Оскільки стан гонитви може виникнути в кількох функціях і навіть у кількох контрактах, будь-яке рішення, спрямоване на запобігання повторному входу, буде недостатнім. Натомість рекомендується спочатку завершити всю внутрішню роботу, а лише потім викликати зовнішню функцію. Проте потрібно не тільки уникати надто швидкого виклику

зовнішніх функцій, але також уникати викликів функцій, які викликають зовнішні функції.

Вище були наведені приклади стану гонитви, у яких зловмисник виконує шкідливий код в одній транзакції. Нижче наведено інший тип стану гонитви, притаманний блокчейн, який використовує той факт, що порядок самих транзакцій (всередині блоку) легко піддається маніпуляціям.

- *Залежність від упорядкування транзакцій або попередній запуск* (Transaction-Ordering Dependence (TOD) / Front Running). Оскільки транзакція знаходиться в пулі пам'яті протягом короткого часу, можна знати, які дії відбуватимуться, перш ніж вона буде включена в блок. Зауважимо, що пул пам'яті (англ. mempool) — це організована черга, де транзакції зберігаються та сортуються перед додаванням до новоствореного блоку, пул пам'яті містить непідтверджені транзакції (зберігаються як окремі транзакції), в той час, як блокчейн зберігає підтверджені транзакції, упаковані в блоки. Такий підхід може бути проблемою, наприклад, для децентралізованих ринків, де можна побачити транзакцію купівлі деяких токенів, а ринковий ордер виконується до включення іншої транзакції.

- *Залежність від позначки часу* (Timestamp Dependence). Майнер може маніпулювати позначкою часу блоку, тому слід враховувати всі прямі та непрямі використання позначок часу. Кількість блоків і середній час виходу блоку можна використовувати для оцінки часу, але це не є доказом у майбутньому, оскільки час виходу блоку може змінитись.

- *Переповнення та недоповнення цілих чисел* (Integer Overflow and Underflow). Варто звернути увагу на те, що існує близько 20 випадків переповнення та недоповнення.

- *DoS із (неочікуваним) поверненням* (DoS with (Unexpected) revert). Контракт може проходити через масив, щоб заплатити користувачам (наприклад, прихильникам у контракті краудфандингу). Зазвичай хочеться переконатися, що кожен платіж виконано успішно. Якщо ні, слід повернутися. Проблема полягає в тому, що якщо один виклик не вдається, то повертається вся система виплат, тобто цикл ніколи не завершиться. Ніхто не отримує гроші, тому що одна адреса викликає помилку.

- *DoS з обмеженням газу блоку* (DoS with Block Gas Limit). Кожен блок Ethereum може обробляти певний максимальний обсяг обчислень. Якщо цим знехтувати, то транзакція не вдається. Це може призвести до проблем навіть за відсутності навмисного нападу. Однак особливо погано, якщо зловмисник може маніпулювати кількістю необхідного газу. Наприклад, зловмисник може додати купу адрес, кожна з яких потребує дуже невеликого відшкодування. Таким чином, витрати на газ для відшкодування кожної адреси зловмисника можуть перевищити ліміт газу, блокуючи транзакцію відшкодування взагалі.

- *Примусове надсилання ефіру до контракту*. Розробники контрактів повинні знати, що Ether може бути примусово направлений до контракту, і повинні відповідно розробити логіку контракту.

Однією з *основних переваг* смарт-контракту є можливість взаємодіяти в умовах повної недовіри і без посередників (невиконання умов анулює контракт).

Проте смарт-контракти не позбавлені і недоліків:

- можливі помилки – людський фактор (як було у мережі Ethereum)
- невизначений юридичний статус (ускладнюється анонімністю, відсутністю посередників)
- не є універсальними; у певних випадках «класичні» договори зручніші.

- оплата за транзакцію, що містить/активує смарт-контракт (газ)

Смарт-контракти на платформі блокчейн для розрахунків в електроенергетиці, у порівнянні з "класичними" контрактами, мають такі переваги:

- швидкі розрахунки за фактом споживання;
- зручний вибір трафіку;
- відсутність боржників;
- відмова від послуг посередників (зниження ціни за електроенергію на 5-10%).

Такі смарт-контракти створюється за ініціативою однієї із сторін (споживач, мережа, генерація) і укладаються після погодження деталей.

Розглянемо очікування від застосування смарт-контрактів на технології блокчейн в сфері енергетики:

- зниження витрат при розрахунках за рахунок відмови від посередників;
- підвищення гнучкості пропозицій при виборі тарифу та схеми оплати;
- підвищення ролі рядових споживачів у плануванні обсягів споживання;
- можливість закупок безпосередньо у виробників;
- захист учасників від навмисних маніпуляцій показниками засобів обліку;
- захист мережевих та генеруючи компаній від банкрутства компаній-продавців;
- захист споживачів від недостовірних даних стосовно відключень.

DTEK стосовно застосування смарт-контрактів:

В рамках комплексного підходу «3D» (Decarbonization, Decentralization, Digitalization), для укладання P2P-контрактів у галузі зеленої енергетики.

Очікування від введення смарт-контрактів – дозволять використовувати P2P схему, що призведе до:

- спрощення багаторівневої системи, що складається з виробників електроенергії, операторів розподільних мереж, операторів оптових розрахунків, трейдерів та споживачів.
- всі транзакції – через Інтернет;

- електроенергія стане дешевшою;
- за рахунок P2P, будуть мінімізовані втрати при передачі на великі відстані (зараз - 11%, як в бідних країнах; найнижчі – 2-3%, Тринідад і Тобаго, за рахунок відсутньої передачі на великі відстані).

Перша спроба використання P2P контрактів: Бруклін, 2016, продаж «зеленої» енергії сусіду.

За один рік різні компанії (LO3 Energy, Siemens, ...) вклали в дану сферу більше за \$ 300 млн.

Серед світових трендів P2P-технологій варто виділити:

- форум BlockchainEnergyAsia в Сінгапурі;
- велика кількість азіатських блокчейн-проектів в енергетиці;
- P2P ринки електроенергії;
- в Японії запустили найбільший кластер розподілених систем накопичення енергії, що керується штучним інтелектом (більше 3500 домогосподарств), мета – розвантаження державної енергосистеми.

Проте важливо враховувати також такі проблеми на шляху розвитку P2P та смарт-контрактів у енергетиці, як:

- відсутність технологічної бази у вигляді сонячних панелей, вітроустановок, накопичувачів енергії;
- невизначений статус всієї криптоіндустрії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Nick Szabo - Smart Contracts: Building Blocks for Digital Markets. [Електронний ресурс] URL: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html Дата звернення: 15.11.2022.

2. Nick Szabo. Formalizing and Securing Relationships on Public Networks. [Електронний ресурс] URL: <https://firstmonday.org/ojs/index.php/fm/article/view/548/469> Дата звернення: 15.11.2022.

3. Tapscott, Don; Tapscott, Alex. The Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. ISBN 978-0670069972. [Електронний ресурс] URL: <https://archive.org/details/blockchainrevolu000taps> Дата звернення: 15.11.2022.

4. To Fork of Not to Fork? [Електронний ресурс] URL: <https://medium.com/blockchain-hub/to-fork-of-not-to-fork-a9b077718fe3#.xk7ojtacq> Дата звернення: 15.11.2022.

5. Беларусь первой в мире законодательно закрепила smart-контракт. [Електронний ресурс] URL: <https://www.belta.by/economics/view/belarus-pervoj-v-mire-zakonodatelno-zakrepila-smart-kontrakt-281784-2017/> Дата звернення: 15.11.2022.

6. Scott H. Kimpel & Christopher Adcock The State of Smart Contract Legislation <https://www.blockchainlegalresource.com/2018/09/state-smart-contract-legislation/>

7. Смарт-контракты: как использовать и насколько надежны для сделок [Электронный ресурс] URL: <https://cryptonet.biz/ru/smart-kontrakty-kak-ispolzovat-i-naskolko-nadezhny-dlya-sdelok/>

8. Atzei, Nicola & Bartoletti, Massimo & Cimoli, Tiziana. (2017). A Survey of Attacks on Ethereum Smart Contracts (SoK). 164-186. 10.1007/978-3-662-54455-6_8. [Электронный ресурс] URL: <https://eprint.iacr.org/2016/1007.pdf> Дата звернения: 15.11.2022.

9. Sayeed, Sarwar & Marco-Gisbert, Hector & Caira, Tom. (2020). Smart Contract: Attacks and Protections. IEEE Access. PP. 1-1. 10.1109/ACCESS.2020.2970495. [Электронный ресурс] URL: https://www.researchgate.net/publication/338926064_Smart_Contract_Attacks_and_Protections Дата звернения: 15.11.2022.

10. Known Attacks [Электронный ресурс] URL: https://ethereum-contract-security-techniques-and-tips.readthedocs.io/en/latest/known_attacks/ Дата звернения: 15.11.2022.

Сушко Сергій Володимирович,
ІПМЕ ім. Г.Є. Пухова НАН України,
молодший науковий співробітник,
sergii.sushko@gmail.com

Чемерис Олександр Анатолійович,
ІПМЕ ім. Г.Є. Пухова НАН України,
заступник директора з наукової роботи, доктор технічних наук,
a.a.chemeris@gmail.com

АСПЕКТИ ВПЛИВУ ОПТИМІЗАЦІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА ЕНЕРГОСПОЖИВАННЯ ОБЧИСЛЮВАЛЬНИХ СИСТЕМ

Анотація. В статті розглянуто деякі методи оптимізації програмного забезпечення. Основний акцент автори спрямовують на такі напрямки оптимізації як скорочення часу виконання програм та підвищення енергоефективності. Станом на листопад 2022 року мінімальне енергоспоживання пристроїв при забезпеченні їх функціональності є значущою задачею підтримання енергобезпеки країни. В статті робиться висновок про доцільність виконання оптимізації з метою загального зниження енергоспоживання. Також підкреслюється, що нетривіальні методи оптимізації потребують часу на запровадження.

Abstract. The article discusses some methods of software optimization. The main emphasis of the authors is directed to such areas of optimization as reducing of program execution time and increasing energy efficiency. As of November 2022, the minimal energy consumption of devices while supporting their functionality is a significant task of maintaining the country's energy security. The article concludes about an expediency of performing optimization for purpose of overall reduction of energy consumption. It is also emphasized that non-trivial optimization methods require time to implement.

Проблема зниження енергоспоживання є актуальною впродовж тривалого часу [1-3]. Останнім часом набула популярності концепція так званих «зелених» обчислень [4]. Ця концепція базується на підході, що всі етапи проектування, впровадження, використання та утилізації засобів обчислення мають вносити мінімальну шкоду довкіллю. В загальну концепцію зелених обчислень включається також широко відома задача оптимізації обчислень, тобто зниження використання необхідних ресурсів (енергії, часу виконання) при тому ж вихідному результаті. Задача зниження енергоспоживання обчислень достатньо комплексна, наприклад створення спеціалізованих наборів інструкцій для конкретного застосування [5].

Розглядаючи задачу оптимізації програмного забезпечення, варто відзначити наявність багатьох методів та технік оптимізації. Велика кількість методів оптимізації вже наявна в компіляторах. Використання або невикористання таких методів досягається вибором опцій компілятора в графічному редакторі розробки. Деякі методи є відносно новими та потребують додаткових зусиль для застосування. Зрештою, експериментальні методи оптимізації стають більш дослідженими і з часом включаються у відомі компілятори.

Одним з напрямків оптимізації програмного забезпечення є підхід, коли вихідний код програми при використанні одного або декількох методів оптимізації перетворюється на інший вихідний код, але вже оптимізований. Застосування такого підходу, на відміну від компіляторів, дозволяє зосередитися розробникам методів оптимізації безпосередньо на самих методах, а не створювати неймовірно складний компілятор. Останнім часом з'явилися програмні реалізації перетворення код-в-код, що виконують перетворювання в автоматичному режимі. Таким чином, задавши параметри оптимізації дослідник або розробник отримує інший код, який в подальшому компілюється і використовується як звичайний код. Одним із таких засобів є Pluto [6]. Цей пакет використовує різні модифікації методу розбиття обчислювальних циклів на блоки та розпаралелювання. Методу розбиття обчислювальних циклів на блоки – метод оптимізації, що додає вкладеності малого розміру у обчислювальні цикли. Такий підхід покращує локальність даних. Авторами проведено експерименти на тестових програмах Polybench [7] для визначення як прискорення виконання тестових програм, так і для визначення енергоефективності обчислень. Детально отримані результати наведено в [8]. Як критерій енергоефективності обчислень авторами було взяте значення електричної енергії, необхідної для виконання обчислень. Також одним із критеріїв може слугувати відсоток збереження електроенергії необхідної для обчислень у порівнянні з необхідною енергією, що була отримана на неоптимізованому коді, див. Рис. 1.

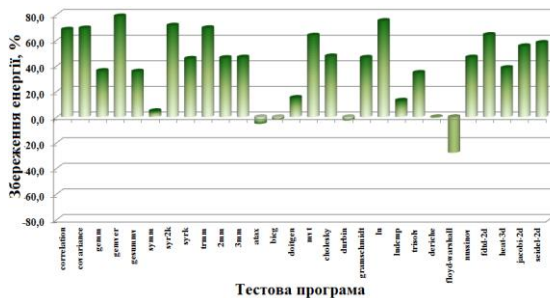


Рис. 1. Коефіцієнти енергоефективності для різних тестових програм при використанні методу розбиття на блоки та розпаралелюванні

Із графіка випливає, що загалом не всі програми можуть бути ефективно оптимізовані за допомогою методу розбиття на блоки. В деяких випадках енергоефективність не покращується. Проте для більшості тестових програм вказаний метод оптимізації показав свою доречність і можна спостерігати суттєве покращення енергоефективності обчислень.

Як висновок варто відзначити, що використання методів оптимізації, спрямованих на прискорення часу виконання комп'ютерних програм та розпаралелювання також опосередковано може впливати на енергоефективність обчислень загалом. Особливо це помітно при розпаралелюванні – електрична потужність зростає, проте за рахунок кратного прискорення енергоефективність обчислень покращується.

Як недолік варто відзначити, що застосування просунутих засобів оптимізації вимагає додаткового часу на впровадження та налаштування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Piguet C. Low-power processors and systems on chips. Boca Raton: CRC Press, 2005.
2. Pillai A. S., Isha T. B., Factors Causing Power Consumption in an Embedded Processor - A Study. International Journal of Application or Innovation in Engineering & Management, Vol. 2:7, с. 300-306, 2013.
3. Ellis C., Controlling energy demands in mobile computing systems. San Rafael: Morgan & Claypool, 2007.
4. Hindle A., Green Software Engineering: The Curse of Methodology. Proceedings: IEEE 23rd International Conference, 2016.
5. Glöckler T., Design of energy-efficient application specific instruction set processors. Dordrecht: Kluwer academic publishers, 2004.
6. Bondhugula U., PLUTO automatic parallelizer. [Електронний ресурс] URL: <https://sourceforge.net/projects/pluto-compiler>. Дата звернення 08.12.2020.
7. Pouchet L. PolyBench/C the Polyhedral Benchmark suite. [Електронний ресурс] URL: <http://web.cse.ohio-state.edu/~pouchet/software/polybench/#description>. Дата звернення 08.12.2020.
8. Сушко С., Чемерис О., Визначення енергоефективності обчислень на різних обчислювальних системах. Моделювання та інформаційні технології. Київ, Том 85, с. 34-39. 2018.

Артемчук Володимир Олександрович,
ІПМЕ ім. Г.Є. Пухова НАН України,
заступник директора з науково-організаційної роботи,
доктор технічних наук, старший науковий співробітник,
ak24avo@gmail.com

Каменева Ірина Петрівна,
ІПМЕ ім. Г.Є. Пухова НАН України,
старший науковий співробітник

Попов Олександр Олександрович,
ДУ «Інститут геохімії навколишнього середовища НАН України»,
заступник директора з науково-організаційної роботи

Яцишин Андрій Васильович,
ДУ «Інститут геохімії навколишнього середовища НАН України»,
провідний науковий співробітник

Кириленко Юрій Олександрович,
ІПМЕ ім. Г.Є. Пухова НАН України,
молодший науковий співробітник

ЗАСОБИ АНАЛІЗУ ДАНИХ В ЗАДАЧАХ ПІДТРИМКИ УПРАВЛІНСЬКИХ РІШЕНЬ В ГАЛУЗІ ЕКОЛОГІЧНОЇ БЕЗПЕКИ

Анотація. Запропоновано когнітивний підхід до аналізу даних моніторингу довкілля, який спрямований на структурування інформаційних ресурсів та побудову моделі знань в галузі екологічної безпеки. Наведено результати аналізу та візуального представлення територіальних ризиків, обчислених за даними моніторингу забруднення атмосферного повітря. В межах запропонованого підходу розроблено структуру моделі експертних знань для інформаційної підтримки прийняття рішень в галузі ядерної і радіаційної безпеки.

Abstract. A cognitive approach to the analysis of environmental monitoring data is proposed, which is aimed at structuring information resources and building a knowledge model in the field of environmental safety. The results of the analysis and visual representation of territorial risks, calculated from the data of atmospheric air pollution monitoring, are given. Within the framework of the proposed approach, the structure of the model of expert knowledge has been developed for informational support of decision-making in the field of nuclear and radiation safety.

В умовах підвищеної небезпеки, що склалися в Україні, починаючи з лютого 2022 р., особливої уваги потребує проблема аналізу та оцінювання техногенних ризиків для об'єктів і підприємств, що розташовані на територіях поблизу воєнних дій, зазнають пошкодження від ракетних ударів, снарядів або інших руйнівних наслідків. Зокрема, небезпечні ситуації було створено на ЧАЕС, що тимчасово була захоплена військовими РФ. Це призвело до підвищення радіаційного фону, виникнення лісових пожеж, забруднення довкілля та інших руйнівних наслідків для прилеглих територій. Наразі в центрі уваги світової спільноти події на Запорізькій АЕС (рис. 1), де через порушення російськими окупантами норм експлуатації виникли масштабні загрози і небезпечні наслідки як для енергозабезпечення, так і для стану довкілля [1].



Рис.1. Запорізька АЕС під час воєнного стану.

Для зменшення техногенного впливу, втрат енергетичних та матеріальних ресурсів, а також більш ефективного збереження виробничих потужностей необхідно забезпечити якісну інформаційну підтримку щодо своєчасного прийняття і корекції управлінських рішень. Такі рішення мають враховувати як накопичений досвід щодо подібних інцидентів та обсягів втрат, так і можливості передбачення на наступний період. Підкреслимо, що подібні задачі необхідно вирішувати на основі міжнародного досвіду управління ризиками [2], в рамках національного законодавства, з урахуванням урядових постанов і програмних документів.

Актуальність проблеми підтверджується важливими урядовими рішеннями та проектами, що визначають основні напрямки підвищення безпеки техногенних підприємств і стану прилеглих територій [3, 4].

Когнітивний аналіз ризиків. Когнітивний підхід до аналізу даних моніторингу в галузі екологічної безпеки базується на досягненнях в сфері когнітивної психології та штучного інтелекту. Основні положення, задачі та особливості когнітивного аналізу техногенних ризиків сформульовані в [5].

Когнітивний підхід спрямований на розроблення методів і засобів виявлення знань про небезпечні об'єкти або ситуації, які допомагають приймати обґрунтовані та ефективні рішення. Насамперед такий підхід надає можливості щодо вчасного виявлення і передбачення тенденцій розвитку особливо небезпечних ситуацій, з урахуванням великої кількості показників ризику. Зазначимо, що переваги засобів когнітивного аналізу полягають саме в тому, що вони орієнтовані на конкретні умови певної країни або регіону. Як правило, засоби та технології, розроблені за кордоном, потребують занадто високих затрат і досить складної адаптації до місцевих особливостей.

Когнітивний аналіз ризиків включає визначення основних факторів ризику в умовах підвищеної небезпеки на основі даних спостережень та вимірювання сукупності показників, що визначають рівні небезпеки; аналіз і структурування даних моніторингу, одержаних з різних джерел; побудову простору ризику, тобто визначення небезпечних подій, оцінювання та прогнозування імовірнісних характеристик цих подій, в тому числі, обсягів втрат та негативних наслідків.

Простір ризику запропоновано представити наступним чином. Кожна імовірнісна модель описує певну множину спостережень X , де визначено розбиття $E(X)$, яке утворює множину випадкових подій [5, 6]. На цій множині задається невід'ємна функція P , що задовольняє відомим властивостям імовірнісної міри і визначає імовірність випадкових подій з $E(X)$. Множина спостережень X , множина випадкових подій $E(X)$ і ймовірнісна міра P , задана на множині $E(X)$, утворюють імовірнісний простір ризику (X, E, P) .

Факторами ризику можуть бути фактори довільної природи (фізичні, хімічні, генетичні, психологічні, соціальні тощо), які мають вплив на порушення гомеостазу екологічної системи, зокрема, стану здоров'я людини. Для чисельної оцінки достовірності відношень між впливом і його наслідками, встановлених на емпіричному рівні, застосовуються відомі методи математичної статистики, які дозволяють враховувати невизначеності, що виникають як при вимірюванні самих впливів, так і при оцінюванні залежності між впливом і ефектом.

Засоби когнітивного аналізу. До засобів когнітивного аналізу ризиків відносимо методи інтелектуального аналізу, структуризації та інтеграції даних (зокрема, методи виявлення латентних знань), засоби просторового аналізу інформації з використанням геоінформаційних технологій та різноманітні засоби когнітивної комп'ютерної графіки.

Методи Data Mining [7] можна досить умовно поділити на статистичні та кібернетичні методи дослідження. Статистичні методи включають методи багатовимірної статистики (в тому числі, регресійний, факторний, дискримінантний і кластерний аналіз,). До кібернетичного підходу належить машинне навчання, розпізнавання образів та побудова класифікацій, нейронні мережі, еволюційні алгоритми тощо. Крім того, Data Mining

включає ряд технологій підтримки прийняття рішень, спрямованих на пошук прихованих закономірностей, які раніше практично не враховувались, але мають важливе значення для обґрунтування стратегічних рішень в різних сферах людської діяльності.

Методи інтеграції даних – це набір методів і засобів, спрямованих на інтегроване подання великих обсягів інформації, одержаних з різних джерел. Зокрема, в [6] аналізуються можливості аналізу та інтеграції даних з урахуванням семантичних аспектів багатовимірної інформації, які можна застосувати для побудови інтелектуальних систем прийняття управлінських рішень. До даного напрямку також можна віднести сучасні технології злиття даних (*data fusion*), видобутих з різних джерел з метою дослідження певного об'єкту або предметної області.

Просторовий аналіз даних охоплює методи та засоби геоінформаційних досліджень, спрямовані на структурний аналіз геопросторових даних з метою пошуку закономірностей та співвідношень у вихідних даних із врахуванням їх просторового розташування та топологічних відношень. Просторовий аналіз оперує рядом різних методів, що комбінують обчислювальні, статистичні та візуальні засоби, орієнтовані на дослідження геометричної (або топологічної) структури багатовимірної інформації.

Виявлення латентних знань. Латентні, або приховані знання потребують особливих методів дослідження. В психології для виявлення латентних (неявних) знань запропоновано використовувати методи експериментальної психосемантики, які вивчають структуру свідомості та рівень знань особистості на основі моделювання простору знань окремих фахівців [8]. Серед великого різноманіття сучасних методів і стратегій аналізу даних окремо виділимо методи багатовимірного аналізу, спрямовані на виявлення латентних (неявних) знань, тобто пошук лаконічного відображення найбільш суттєвих особливостей досліджуваної структури багатовимірних даних.

Методи виявлення латентних знань базуються на припущенні, що має бути невелике число провідних факторів, за допомогою яких можна досить точно охарактеризувати як вихідні показники аналізованих ситуацій, так і співвідношення між ними. Іноді такі чинники можна виділити серед первинних ознак, але частіше вони мають латентну природу, тобто їх можна описати (реконструювати) через окремі послідовності вихідних показників. Зокрема, такі комбінації можна виявити методами факторного аналізу і багатовимірного шкалювання [8].

Методи візуалізації даних і знань – методи, програмні засоби і технології графічного представлення результатів аналізу великих даних у вигляді рисунків, карт, схем, діаграм або інших графічних образів (з використанням сучасних інтерактивних технологій і засобів анімації) для спрощення сприйняття, визначення змістовних характеристик, полегшення інтерпретації, виявлення окремих тенденцій тощо. Зокрема, для візуалізації

простору знань бажано вибрати множину найбільш інформативних показників, які характеризують суттєві особливості вихідної інформації. Отже, виявлення латентних знань сприяє скороченню кількості ознак і зменшує розмірність досліджуваного простору знань, тобто суттєво спрощує візуальний аналіз багатовимірних даних.

Серед відомих способів визначення інформативних ознак можна назвати три окремих напрямки дослідження:

- Вибір найбільш інформативних ознак з вихідної сукупності всіх показників в межах конкретного кола задач.

- Формування вторинних ознак у вигляді лінійних або нелінійних комбінацій вихідних показників, які мають задовольняти певним критеріям інформативності.

- Побудова багатовимірних шкал, де вибір нового простору ознак здійснюється з урахуванням певних умов, зокрема, умови збереження відстаней або вимоги мінімізації для попарних відстаней між об'єктами.

Візуалізація багатовимірних даних має велике значення на перших етапах обробки і аналізу інформації. В першу чергу за обраним критерієм визначається відображення, яке забезпечує найбільш інформативні проєкції, а потім візуальні образи вихідних даних можна відображувати на моніторі та застосовувати для підтримки прийняття рішень.

Загалом, бажано обирати методи зниження розмірності, які з мінімальними похибками можуть відтворити структуру та особливості багатовимірної інформації. Відомо, що серед всіх лінійних перетворень таким вимогам відповідає метод головних компонент, що забезпечує найменше відхилення для суми відстаней між усіма парами обраних точок. Для нелінійних методів зниження розмірності аналогічну властивість можна довести лише для ряду окремих алгоритмів багатовимірного шкалювання.

Аналіз територіальних ризиків. В задачах техногенної безпеки необхідно враховувати, що штатні викиди енергетичних підприємств і аварійні ситуації викликають безліч різних наслідків. Тому бажано визначити єдину міру втрат або єдиний критерій, що зводить різні наслідки до єдиного базису. Інтегральний ризик визначається як сума або інтеграл щодо всіх наслідків небезпечних подій [9].

В якості єдиної міри ризику, що характеризує певний регіон, будемо розглядати потенційний територіальний ризик, тобто просторовий розподіл імовірності реалізації негативного впливу певного рівня. Зокрема, для оцінки ризику, пов'язаного з впливом шкідливих речовин, потенційний територіальний ризик в точці (x, y) оцінюється за формулою [18]:

$$R(x, y) = \sum_{ij} P(A_j) P_{ij}(x, y) P(L_i),$$

де $P(A_j)$ – імовірність розвитку ситуації за сценарієм j ,

$P_{ij}(x, y)$ – імовірність впливу i в точці (x, y) для сценарію j ,

$P(Li)$ – міра втрат (імовірність захворювання) при впливі i .

Потенційний територіальний ризик розглядається як потенціал максимально можливого ризику $R(x, y) = \max$ для зони впливу техногенних об'єктів підвищеної небезпеки. Щоб одержати ранжирування джерел небезпеки, потрібно побудувати розподіл потенційного ризику для кожного з них (з урахуванням різних сценаріїв розвитку небезпечних подій). В сучасних дослідженнях імовірнісний розподіл ризику (поле ризику) як правило будується для випадку найбільш небезпечної з можливих ситуацій на основі вже наявних статистичних даних та експертних оцінок.

Для інтерпретації екологічної інформації запропоновано два напрямки візуалізації даних: традиційну візуалізацію даних моніторингу у вигляді екологічних карт досліджуваних територій і візуалізацію графічних образів, що відображають розподіл ситуацій (або подій) у просторі інформативних ознак (тобто, візуалізацією відносно шаблонів).

На рис. 2 представлений імовірнісний розподіл ризику миттєвих токсичних ефектів для населення різних районів міста, побудований на основі даних моніторингу з урахуванням суб'єктивних експертних оцінок.

Модель знань в галузі ЯРБ. В задачах екологічної, енергетичної або радіаційної безпеки для інтегрованої оцінки стану безпеки енергетичного підприємства (зокрема, АЕС) запропоновано обрати ризики, які визначають рівень небезпеки та обсяг можливих збитків для досліджуваної множини небезпечних подій, що виникають внаслідок аварій або порушень нормальної роботи техногенних підприємств.

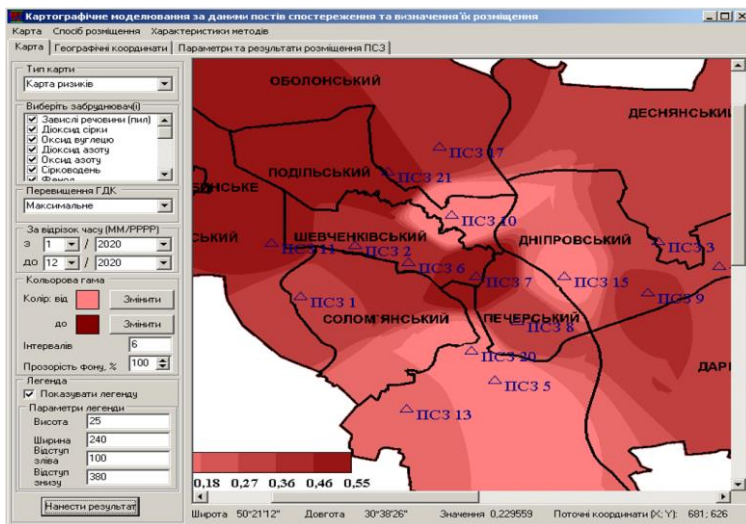


Рис. 2. Розподіл ризику для населення Києва

Модель знань забезпечує можливості для накопичення та систематизації досвіду, одержаного в процесі імовірнісного аналізу безпеки АЕС. Загальну структуру і окремі компоненти моделі розроблено в рамках розвитку та удосконалення інформаційних засобів підтримки прийняття рішень з метою підвищення безпеки АЕС та інших небезпечних підприємств, де використовується *ризико-орієнтований підхід* для обчислення імовірнісних показників ризиків на основі моніторингу стану безпеки [10].

Визначено основні компоненти інформаційно-аналітичного забезпечення, орієнтованого на виявлення і систематизацію знань, необхідних для безпечного обслуговування АЕС.

Модель включає блок імовірнісного аналізу безпеки, який можна розглядати як формальне представлення процесу накопичення досвіду. Велика кількість вихідних показників моніторингу безпеки об'єднана в три блоки (моніторинг зовнішніх факторів, моніторинг стану обладнання, моніторинг порушень і помилок персоналу). За даними моніторингу і результатами аналізу експертних знань розраховуються імовірнісні оцінки (ризики) виникнення аварій та інцидентів для АЕС або інших підприємств ЯРБ.

Для прогнозування небезпечних ситуацій, викликаних зовнішніми факторами або іншими порушеннями в роботі енергетичних підприємств, імовірність небезпечних подій та очікувані втрати (обсяги збитків) бажано оцінювати за умов певних зовнішніх пошкоджень (попадання ракети, бомби, снаряда тощо) або порушень нормальної роботи в результаті некомпетентних дій персоналу, неякісного обслуговування, виникнення конфліктних ситуацій на фоні важких умов роботи. Такі оцінки будуються на основі формул Байєса, які забезпечують обчислення умовних імовірностей небезпечних подій. Наслідками таких подій може бути перевищення норм забруднення повітря, підвищення радіаційного фону до небезпечних рівнів тощо.

Додаткової уваги також потребує вивчення та удосконалення нормативно-правових актів щодо моніторингу та контролю безпеки атомних станцій, які регламентують основні заходи, спрямовані на підвищення безпеки. В рамках цих документів необхідно оцінювати та регулювати стан безпеки атомних станцій, відповідність актуальних ризиків висунутим вимогам, а також розробку заходів для підвищення безпеки атомної енергетики в цілому.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. На Запорізьку АЕС прибула нова команда експертів МАГАТЕ. МАГАТЕ провело ротацію на ЗАЕС. (2022). https://lb.ua/society/2022/11/04/534778_zaporizku_aes_pribula_nova.html
2. Управление рисками в системах нормативного регулирования, ООН, Нью-Йорк, Женева (2014)

3. Указ Президента України №111/2021 від 23 березня 2021р. (2021). <https://www.president.gov.ua/documents/1112021-37505>
4. Уряд схвалив законопроект, який запустить реформу державної системи моніторингу довкілля. <https://mepr.gov.ua/news/39129.html>
5. Артемчук, В.А. Каменева, И.П., Яцишин, А.В.: Специфика применения когнитивного анализа информации в задачах обеспечения экологической безопасности. Электронное моделирование. 39(6), 107-124 (2017)
6. Каменева, И.П. Артемчук, В.А., Яцишин, А.В.: Вероятностное моделирование экспертных знаний с использованием методов психосемантики. Электронное моделирование. 41(2), 81-96 (2019)
7. Дюк, В., Самойленко, А.: Data Mining. СПб, Питер (2001)
8. Петренко, В.Ф.: Основы психосемантики. Москва, МГУ (1997)
9. Лисиченко, Г.В., Хміль, Г.А., Барбашев, С.В.: Методологія оцінювання екологічних ризиків: монографія. Одеса, Астропринт (2011)
10. Міжнародний режим ядерної безпеки. <https://www.iaea.org/mizhnarodnyj-rezhym-yadernoyi-bezpeky>

Артемчук Володимир Олександрович,
ІПМЕ ім. Г.Є. Пухова НАН України,
заступник директора з науково-організаційної роботи,
ak24avo@gmail.com

ПЕРСПЕКТИВИ РОЗРОБЛЕННЯ МЕТОДІВ І ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ РЕЗИЛЬЄНТНОСТІ ОБ'ЄКТІВ ЕНЕРГЕТИЧНОЇ ГАЛУЗІ УКРАЇНИ

Анотація. Визначено актуальність та перспективи розроблення методів і засобів забезпечення резильєнтності об'єктів енергетичної галузі України. Показано місце резильєнтності електроенергетики України як складової національної стійкості країни.

Abstract. The relevance and prospects of the development of methods and means of ensuring the resilience of the objects of the energy industry of Ukraine have been determined. The place of the resilience of the electric power industry of Ukraine as a component of the national stability of the country is shown.

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 у 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, зокрема в жовтні та листопаді 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 [1] 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 [2]: 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 впливає з характеру, різноманітності, надмірності та взаємодії між компонентами, залученими до створення різних функцій. Резильєнтність є атрибутом системи та застосовується до різних підсистем.

Соціальна та економічна значимість відповідних досліджень полягає в необхідності забезпечення резильєнтності електроенергетики України як складової національної стійкості країни, про що відмічено в національній доповіді «Національна стійкість України: стратегія відповіді на виклики та випередження гібридних загроз» [3].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 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
2. Elmqvist, T., Andersson, E., Frantzeskaki, N. et al. (2019) Sustainability and resilience for transformation in the urban century. *Nature Sustainability*, 2, 267–273.
3. Національна стійкість України: стратегія відповіді на виклики та випередження гібридних загроз: національна доповідь / ред. кол. С. І. Пирожков, О. М. Майборода, Н. В. Хамітов, Є. І. Головаха, С. С. Дембіцький, В. А. Смолій, О. В. Скрипнюк, С. В. Стоєцький / Інститут політичних і етнонаціональних досліджень ім. І. Ф. Кураса НАН України. Київ, 2022. 552 с. ISBN 978-966-02-9908-5.

Худинцев Микола Миколайович,
ІПМЕ ім. Г.Є. Пухова НАН України,
докторант, кандидат фізико-математичних наук, доцент,
mykola_khudyntsev@icu-ng.org

ЗАСТОСУВАННЯ ІНДЕКСІВ КІБЕРБЕЗПЕКИ ДЛЯ ОЦІНКИ СТАНУ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. Проведено аналіз світових індексів кібербезпеки, методології та методик їх формування. Запропоновано класифікацію індексів кібербезпеки. Досліджено застосування мережевих індексів кібербезпеки для опису стану секторальної (галузевої) кібербезпеки, а також стану кібербезпеки окремих об'єктів критичної інфраструктури.

Abstract. An analysis of global cyber security indices, methodology, and methods of their formation are provided. A classification of cyber security indices is proposed. The application of network cyber security indices for the describing of the state of sectoral (industry) cyber security, as well as the state of cyber security of individual critical infrastructure objects, is investigated.

Термінологія

Проблемам визначення термінів та вимірювання показників секторальної (галузевої) кібербезпеки лише останнім часом присвячені чисельні публікації (наприклад, [1-5]).

Суб'єктами індексування (рейтингування) у залежності від типу індексу (рейтингу) кібербезпеки є країни, галузі (сектори) економіки, корпорації та організації (*countries, sectors, entities*).

Об'єктами індексування (рейтингування) є процеси діяльності цих суб'єктів у сферах інформаційної безпеки та кібербезпеки, стан безпеки та рівень захищеності цих суб'єктів від загроз безпеки, а також окремі показники безпеки та захищеності.

До індексів кібербезпеки (*cybersecurity indices* в значенні індикаторів високого рівня або *cybersecurity indexes* в значенні кількісних показників) віднесемо регулярні (періодичні) інформаційні матеріали, які містять експертні, аналітичні, статистичні відомості про стан безпеки та рівень захищеності суб'єктів індексування (рейтингування), а також про окремі показники шкідливого впливу реалізованих загроз інформаційної безпеки та кібербезпеки. Як правило, індекси кібербезпеки складаються з метою оцінювання стану інформаційної безпеки та кібербезпеки, а також захищеності суб'єктів індексування (рейтингування) від загроз, результатом чого є оцінка ефективності впроваджуваних заходів з забезпечення інформаційної безпеки, кібербезпеки та кіберзахисту.

До рейтингів кібербезпеки (*cybersecurity ratings*) віднесемо індекси кібербезпеки, які характеризуються переліками (списками) суб'єктів індексування (рейтингування) з визначенням порядкового місця суб'єкта у переліку (списку, рейтингу).

Класифікація індексів кібербезпеки:

- за типами (глобальні, міжнародні, корпоративні)
- за категоріями (звіти, експертні, мережеві, набори даних, фінансові або біржові, комбіновані)
- за організацією доступу або іншими показниками (платформи, опитувальники, бібліотеки, додатки, автоматичні або автоматизовані, нормативніб технічні, маркетингові).

Методологія та методики формування

Предмет та об'єкт індексування (рейтингування) (англ. *objective*) визначається окремо для кожного індексу кібербезпеки. У широкому розумінні під індексуванням (рейтингуванням) ми розуміємо будь-який спосіб оцінювання, як правило, з подальшим порівнянням його результатів між собою.

Предмет індексування (рейтингування) включає:

- діяльність суб'єктів індексування (рейтингування) в сферах інформаційної безпеки та кібербезпеки
- стан інформаційної безпеки та кібербезпеки суб'єктів індексування (рейтингування)
- рівень захищеності суб'єктів індексування (рейтингування) від загроз інформаційної безпеки та кібербезпеки
- окремі показники інформаційної безпеки та кібербезпеки, а також захищеності від відповідних загроз
- окремі показники шкідливого впливу реалізованих загроз.

Показники (індикатори) індексування (рейтингування) – визначені параметри предмету індексування (рейтингування), які використовуються для опису та оцінювання індексу (в інших джерелах використовуються також терміни «індикатори», «елементи», «параметри», «домени»). Різні індекси кібербезпеки містять від 1 до 50 показників, які належать до предмету або об'єкту індексування (рейтингування) і можуть оцінюватися окремо (у якості субіндексу) або у складі основного індексу. Перелік показників (індикаторів) індексування (рейтингування) визначається окремо для кожного індексу, що складає основу методики формування відповідного індексу або рейтингу.

Способи індексування (рейтингування):

- експертиза – визначення та експертна оцінка показників (індикаторів) індексування (рейтингування);
- параметризація – кількісна оцінка показників (індикаторів) індексування (рейтингування);
- індексування – спосіб оцінювання, результатом якого є умовний чисельний показник (індекс, бал);

- рейтингування – спосіб оцінювання, результатом якого є чисельний показник (номер у рейтингу) у вигляді натурального числа.

Методологія формування індексів (рейтингів) базується на:

- методах експертних оцінок (методи асоціацій, парних (бінарних) порівнянь, векторів переваг, фокальних об'єктів, середньої точки, індивідуальне експертне опитування)

- індексному методі математичної статистики
- математичної теорії рейтингів
- теоретико-ігровій кооперативній ресурсній моделі.

Процедура формування індексів (рейтингів):

- створення експертної групи, аналіз предмету дослідження або вдосконалення процедури формування попередньої версії індексу (рейтингу);

- визначення предмету, об'єктів та суб'єктів індексування (рейтингування);

- збирання даних;

- розробка або вдосконалення методики формування індексу (рейтингу);

- підготовка та публікація звіту.

Вимоги до об'єкту індексування:

- готовність до обговорення умов обміну відомостями (чутливою інформацією) та участі у індексуванні (рейтингуванні);

- готовність надавати відповіді на питання опитувальників;

- готовність проходити передбачені методикою внутрішні (зовнішні) аудити інформаційної безпеки;

- готовність на отримання та використання відомостей мережевого моніторингу від зовнішніх постачальників та внутрішніх джерел;

- наявність сенсорів на вході до корпоративної мережі або даних про мережеву активність від партнерів (зовнішніх постачальників);

- готовність на передачу відкритої інформації про значення загального індексу до публічної сфери.

Світові мережеві індекси (рейтинги) кібербезпеки

Index			Editor			URL
Назва	Name	Abbr.	Name	Count	ry	
Автоматизована незалежна платформа оцінювання безпеки	Automate Third-Party Security Rating Platform	A3SRP	Panorays	PNR	USA	https://www.panorays.com/
Рейтингова платформа	Black Kite	BKCRRP	Black Kite Inc.	BKI	USA	https://blackkite.tech.com/

Index			Editor			URL
Назва	Name	Abbr.	Name		Country	
кіберризиків Black Kite	Cyber Risk Ratings Platform					https://blackkittetech.com/wp-content/uploads/2021/03/2021-Third-Party-Risk-Pulse_-_Credit-Unions-and-Vendor-Ecosystems.pdf
Платформа рейтингів безпеки BitSight	BitSight Security Ratings Platform	BSSR	BitSight Technology LTD	BST	USA	https://www.bitsight.com/national-cybersecurity
Індекс кібервпливу	Cyber Exposure Index	CEI	Cyber Intelligence House	CIH	SGP	https://cyberexposureindex.com/ , https://cyberintelligencehouse.com/
Індекс Cyber Green	Cyber Green Index	CGI	CyberGreen Institute	CGI	USA	https://stats.cybergreen.net
Монітор загроз Prevalent	Prevalent Vendor Threat Monitor	PVTM	Prevalent, Inc.	PRV	USA GBR CAN	https://www.prevalent.net/products/vendor-risk-monitoring/
Рейтинги кібербезпеки RiskRecon	RiskRecon Cybersecurity Ratings	RRCR	RiskRecon Co.,	RRC	USA	https://www.riskrecon.com
Платформа рейтингів Security Scorecard	Security Scorecard Ratings Platform	SSR	SecurityScorecard Co.	SSC	USA	https://securityscorecard.com/product/security-ratings

Index			Editor			URL
Назва	Name	Abbr.	Name		Count ry	
Платформа рейтингів UpGuard	UpGuard Ratings Platform	UGR	UpGuard Inc.	UGI	USA	https://www. upguard.com/ resources

Мережеві індекси кібербезпеки є метриками стану кібербезпеки окремих об'єктів критичної інфраструктури, а також стану секторальної (галузевої) кібербезпеки. Здійснюється пілотне впровадження індексів для кількісного вимірювання стану кібербезпеки суб'єктів паливно-енергетичного комплексу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Оцінка стійкості енергетичної інфраструктури України – аналітичний звіт, Павленко О., Антоненко А., Ніцович Р., Євтушок С., Суходоля О., ГО «Діксі Груп», 2022, 72 с.
2. Кібербезпека енергетики, науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України : матеріали, 27 травня 2022 р. Київ : ІПМЕ ім. Г.Є.Пухова НАН України, 2022. 128 с.
3. О. Потій, А. Семенченко, Д. Дубов, О. Бакалинський, Д.Мялковський, Концептуальні засади впровадження організаційно-технічної моделі кіберзахисту України, Захист інформації, т.23, №1, 2021. – с.47-60.
4. R. Boyarchuk, M. Khudyntsev, O. Lebid, O. Trofymchuk, Organizational and Technical Model of National Cybersecurity and Cyber Protection, Workshop on Cybersecurity Providing in Information and Telecommunication Systems, Kyiv, Ukraine, CPITS'2021, 2021. – V.2923, pp. 37-46, ISSN 1613-0073.
5. Худинцев М.М. (заг. ред.), Жилін А.В., Давидюк А.В. Світові індекси кібербезпеки: огляд та методики формування (Глобальний звіт / Каталог), Монографія, Міжнародний університет кібербезпеки, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. – К.: 2021. – 240 с. ISBN 978-966-136-887-2.

Чемерис Олександр Анатолійович,
ІПМЕ ім. Г.Є. Пухова НАН України,
заступник директора з наукової роботи,
a.a.chemeris@gmail.com

Резнікова Світлана Олександрівна,
ІПМЕ ім. Г.Є. Пухова НАН України,
молодший науковий співробітник,
Svetlana.reznikova@gmail.com

Р2Р РИНОК ЕЛЕКТРОЕНЕРГІЇ ДЛЯ МІКРОМЕРЕЖ

Анотація. Розглядається підхід організації функціонування електроенергетичної мікромережі через побудову Р2Р ринку електроенергії. Взаємовідносини між просьюмерами мікромережі регулюються з використанням блокчейн технології, алгоритму консенсусу та смарт-контрактів.

Abstract. The approach of the organization of functioning of the electric power microgrids through the construction of the R2P electricity market is considered. The relationships between the microgrid prosumers are regulated using blockchain technology, a consensus algorithm, and smart contracts.

Концепція організації мікромереж з подальшим об'єднанням в загальну мережу, в якій присутні також промислові генеруючі потужності – гідро-, тепло-електростанції, атомні електростанції та сонячні і вітряні енергосистеми все більше привертає увагу розробників електричних мікромереж.

Взаємовідносини між володарями генеруючих потужностей та споживачами регулюються шляхом

організації мікроринку, який можна побудувати на принципах централізації, де призначається оператор ринку, який оптимізує потоки, активує локальний попит та має спрямовати свої зусилля на максимізацію загального соціального благополуччя системи. Але такий підхід має недоліки.

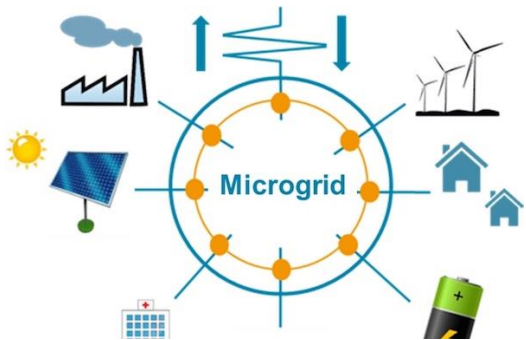


Рис. 1. Загальна схема мікромережі

На даний час росте популярність децентралізованих ринків електроенергії з врахуванням того, що частина володарів може бути як виробниками електроенергії, так і споживачами. Автори демонструють розподілену модель ринку peer-to-peer, де споживачі в місцевих енергетичних спільнотах оптимізують свої транзакції, використовуючи гнучкість системи. Прикладом проєктів в цьому напрямку є EnerPort, який підтримується спільно ірландським урядом та промисловістю, де технологія блокчейну використовується для розробки моделі енерготоргівлі peer-to-peer (P2P) для підтримки торгівлі енергією між мікрогрідами [2].

Блокчейн є перспективною платформою для обміну енергоресурсами, оскільки знижує витрати на торгівлю шляхом усунення третьої сторони для посередництва серед просьюмерами. Розглянута вартість та пропускна спроможність блокчейну системи енерготоргівлі. При цьому вартість одного вузла на основі блокчейна для системи обміну енергією залежить від обчислювальних ресурсів, які використовуються в для майнінгу. Для системи P2P-торгівлі використовується алгоритм консенсусу такий, як «доказ роботи блокчейну» (proof of work-based blockchain). Такий блокчейн винагороджує майнерів (які нові створюють блоки шляхом агрегування недокументованих транзакцій) за створення нових блоків.

Оцінити кількість енергії що можна провести через торгівельний проміжок $[t, t + 1]$ можна через кількість угод, що заключають гравці ринку. Для оцінювання кількості угод, необхідних для запису енергетичних торгів серед просьюмерів протягом цього часового вікна, розглядається $G = (V; E)$ — граф, що позначає множину просьюмерів V і з торговими сусідами просьюмерів проводиться обмін енергією E . Загальна енергія, яку потрібно обміняти за час t

$$\min(|\sum_{E_t^i < 0} E_t^i|, \sum_{E_t^i < 0} E_t^i).$$

Таким чином, P2P мікроринок для функціонування електроенергетичної мікромережі є перспективним підходом до побудови енергетичної інфраструктури. Є низка проблем яку потрібно вирішити. Одна з основних — оптимізація торгових транзакцій. Технологічні питань складають низку таких задач, як організація блокчейна для фіксації та зберігання транзакцій, пошук оптимального за продуктивністю та енергоспоживанням алгоритму консенсусу, тощо. Також важливими проблемами є кібернетична безпека мережі. Технологія смарт контрактів є одним з напрямків розробки для використання в P2P ринках торгівлі електроенергією.

REFERENCES

1. Folk E. How Waste-To-Energy Can Enable Microgrids [Електронний ресурс] / Emily Folk – Режим доступу до ресурсу: <https://www.2greenenergy.com/2020/06/23/energy-microgrids/>.
2. Verma, P., O'Regan, B., Hayes, B. et al. EnerPort: Irish Blockchain project for peer-to-peer energy trading. Energy Inform 1, 14, 2018. – 9 p., <https://doi.org/10.1186/s42162-018-0057-8>

Чемерис Олександр Анатолійович,
ІПМЕ ім. Г.Є. Пухова НАН України,
заступник директора з наукової роботи,
a.a.chemeris@gmail.com

Клименко Тетяна Михайлівна,
ІПМЕ ім. Г.Є. Пухова НАН України,
завідувачка науково-організаційного відділу,
klimenko-t@ukr.net

ПРОГРАМНІ ЗАСОБИ ДЛЯ ВИРІШЕННЯ МІР ЗАДАЧ

Анотація. До задач змішаного цілочисельного програмування (МІР) приводяться вирішення багато проблем з різних галузей економіки, індустрії, тощо. В статті розглядаються програмні пакети для МІР-задач як комерційні, так і вільного користування. Проводиться порівняльний аналіз програмних засобів для МІР задач.

Abstract. A lot of problems in different branches of economy, industry, etc. are solved by tasks of mixed integer programming (MIP). The article considers software packages for MIP-tasks both commercial and free use. The comparative analysis of software frameworks and MIP solvers is carried out

Загальну задачу лінійного програмування можна сформулювати таким чином: знайти оптимум лінійної функції цілі $Y(\bar{x})$, якщо обмеження $F_i(\bar{x})$ лінійні й вектор змінних $\bar{x}$ невід’ємний. При аргументах цілочисельного ряду говоримо про задачі цілочисельного програмування. Якщо деякі аргументи представлені не дискретними функціями, то це визначає задачу змішаного цілочисельного програмування (МІР – mixed integer programming). Відповідно до [1], задачу МІР визначаємо, як

$$\max\{c^T x: b^1 \leq Ax \leq b^2, d^1 \leq x \leq d^2, x_j \in \mathbb{Z} \text{ для } j \in S\},$$

де $b^1, b^2 \in \mathbb{R}^m$, $c, d^1, d^2 \in \mathbb{R}^n$, A – дійсна матриця розміром $m \times n$, x – n -вектор змінних, $S \subseteq \{1, \dots, n\}$ – множина цілочисельних змінних.

Для пошуку оптимальних значень використовують програмні пакети як комерційного розповсюдження, так і ті, що вільно розповсюджуються. В якості основних кандидатів на використання були такі солвери, як CPLEX, Gurobi – комерційні програми (використано академічну ліцензію) та некомерційні програми: 1. lp-solve 2. MIPCL та 3. GLPK. Для порівняння використано програмний тестовий пакет MIPLIB 2017, який включає набір з 240 задач. З практичних міркувань, набори бенчмарку були обрані з урахуванням різних обмежень щодо розв’язності та числової стійкості.

В [2] наведено порівняння між різними солверами в термінах простору проблем (Таблиця 1).

Проведений аналіз щодо часу рішення задач, то найкращий результат показує пакет GuRoBi. Солвери lp_solve і GLPK показують значно гірший результат, відповідно, в 4.75 та в 6 разів потрібно більше часу для отримання рішення.

Таблиця 1. Порівняння солверів

Солвер	Розробник	Задача						
		LP	CP	MIP	MILP	MIQP	MISOCF	LP
CPLEX	IBM	+	+	+	+	+	+	+
GuRoBi	GuRoBi	+		+	+	+	+	
XPRESS	FICO	+	+	+	+	+	+	+
lp_solve	Michel Berkelaar	+		+	+	+		
GLPK	GNU project	+		+				
Lindo	Lindo Systems	+		+	+	+		+
OML	Ketron Management	+			+	+		
FrontLine	FrontLine Systems			+				
MIDACO	ASTER Labs	+		+				+

Таким чином, підвищення продуктивності солверів є актуальною задачею. Одним зі шляхів зменшення часу пошуку рішення є використання багатопроцесорних комп'ютерних систем, на яких проходить розпаралелювання пошуку оптимального рішення задачі. Роботу виконано в рамках цільової програми «Підтримка пріоритетних для держави наукових досліджень і науково-технічних (експериментальних) розробок Відділення фізико-технічних проблем енергетики НАН України на 2022—2023 рр.» з кодом програмної класифікації видатків 6541230 (прикладні дослідження).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Н.Н. Писарук. Смешанно-целочисленное программирование. [Електронний ресурс] / Н.Н. Писарук – Режим доступу до ресурсу: <http://pisaruk.narod.ru/slides/OR/MIP.pdf>
2. Rimmi Anand, Divya Aggarwal, Vijay Kumar A comparative analysis of optimization solvers / Journal of Statistics & Management Systems, Vol. 20, No. 4, 2017. - pp. 623–635. DOI : 10.1080/09720510.2017.1395182

Борукаєв Зелімхан Харитонович,
*ІПМЕ ім. Г.Є. Пухова НАН України,
завідуючий лабораторією математичного моделювання енергоринків,
доктор технічних наук, старший науковий співробітник,
zelimh1948@gmail.com*

Остапченко Костянтин Борисович,
*НТУУ-КПІ ім. Ігоря Сікорського,
доцент кафедри інформаційних систем та технологій,
кандидат технічних наук, доцент,
okb2003@ukr.net*

Євдокімов Володимир Анатолійович,
*ІПМЕ ім. Г.Є. Пухова НАН України,
провідний науковий співробітник,
кандидат наук з державного управління,
ievdokimov40@gmail.com*

ОСОБЛИВОСТІ ПОБУДОВИ МОДЕЛІ КОРОТКОСТРОКОВОГО ПРОГНОЗУВАННЯ ЕЛЕКТРОСПОЖИВАННЯМ ПОСТАЧАЛЬНИКАМИ НА ОПТОВОМУ РИНКУ ЕЛЕКТРОЕНЕРГІЇ

Анотація. Розглядаються результати комплексного аналізу особливостей задач прогнозування електроспоживанням постачальниками електроенергії на оптовому ринку та рекомендації щодо побудови комп'ютерної моделі короткострокового погодинного прогнозування електроспоживання постачальниками на сегменті оптового ринку «на добу наперед».

Abstract. The results of a comprehensive analysis of the specifics of the tasks of forecasting electricity consumption by electricity suppliers in the wholesale market and recommendations for building a computer model for short-term hourly forecasting of electricity consumption by suppliers in the wholesale market segment "a day ahead" are considered.

Система організаційного управління енергопостачальної компанії, окрім своєї основної функції пов'язаної із автоматизованим первинним збором, накопиченням та попередньою обробкою даних для забезпечення моніторингу показників функціонування технологічних процесів, передбачає також виконання функції їх прогнозування та наступного планування обсягів купівлі електроенергії (е/е) на різних сегментах оптового ринку з метою вироблення взаємопов'язаних управлінських рішень, спрямованих на оптимізацію режимів погодинного енергопостачання регіонів. Тому, суб'єкти електроенергетики при встановлених правилах роботи електроенергетичного

ринку економічно зацікавлені у вдосконаленні методів і підвищенні точності прогнозування основних його параметрів.

На даний час проводяться багато досліджень моделей різного призначення та здійснюється публікація результатів цих досліджень щодо прогнозування цін та обсягів споживання (навантаження) для застосовування на різних ринках е/е, із врахуванням багатьох чинників та особливостей їх функціонування. Серед цих публікацій слід виділити оглядові статті [1-5], які зосереджені на аналізі ефективності застосування різних типів моделей, їх класифікації та вироблення рекомендацій подальшого розвитку саме предмету дослідження, пов'язаного із прогнозуванням основних показників функціонування ринку е/е – обсягів купівлі продажу, цін.

За результатами аналізу у цих роботах стверджується, що для прогнозування ринкової ціни на е/е можна використовувати три великих різновиди методів (класи) - теорію ігор, часові ряди та методи імітаційного моделювання, а моделі прогнозування часових рядів включають статистичні моделі і моделі, засновані на штучному інтелекті.

Найбільш широке застосування отримали статистичні моделі прогнозування цін на е/е. Крім того, результати аналізу в даній області застосування статистичних моделей, дають передумови для розробки методів оцінки ризику при прийнятті рішень на ринку е/е.

У моделях, заснованих на теорії ігор, моделюються стратегії поведінки учасників оптового ринку е/е. С використанням різних моделей досягнення рівноваги досліджується вплив поведінки окремих виробників на рівноважну ціну і формулюються стратегії їх поведінкової діяльності для участі в аукціонах на ринку та його сегментах.

У моделях, заснованих на імітаційному моделюванні, будується досить точна модель енергосистеми. Беруться до уваги фізичні явища, що управляють процесами виробництва і передачі е/е. До переваг цих моделей відносять те, що вони забезпечують детальне розуміння процесу формування цін на е/е. Однак, істотними недоліками вважається складність реалізації імітаційної моделі, що вимагає істотних витрат на створення і підтримку в актуальному стані інформаційної бази, необхідної для наповнення моделі, а також висока обчислювальна складність і витрати.

Моделі, засновані на штучному інтелекті, зокрема штучних нейронних сіток, здатні враховувати наявність нелінійних залежностей між вхідними та вихідними параметрами. Недолік таких моделей в тому, що функціональна форма цих залежностей є неявною. Тому, подальший аналіз можливостей їх застосування, наприклад, аналіз чутливості моделей до змін їх параметрів, представляється скрутним.

Отже, систематизуючи підходи до використання моделей прогнозування можна визначити наступні особливості їх побудови і застосування.

1) Аналіз характеристик часових рядів цін на електроенергію на оптових ринках.

На динаміку попиту на е/е значно впливають економічна і господарська активність, а також погодні умови. Ці ключові фактори пояснюють високу частоту коливань цін на е/е, помічену для всіх оптових ринків. Розрізняють добову, тижневу і сезонну періодичність. У ряді робіт також відзначалися коливання цін в святкові дні - календарні ефекти.

Практично всі досліджувані ряди цін на е/е (як часових, так і середньодобових) мають розподіл, відмінний від нормального з наявністю піків (коефіцієнтами ексцесу) і «важкими хвостами» (асиметрією).

На довгостроковому горизонті ціни на е/е показують властивість повернення до середнього значення, апроксимуючи середній рівень (іноді змінюється в часі).

Висока і змінювана в часі волатильність, а також кластеризація волатильності характерна для всіх оптових ринків е/е. Спостережувані різкі короткострокові стрибки цін можуть бути викликані погодними умовами, позаплановими зупинками генеруючого обладнання або аваріями в системі передачі е/е. Встановлено, що на ринку з переважною гідрогенерацією ціни мають більш стійкий характер, ніж в порівнянні з іншими ринками.

Отже, наведені характеристики рядів цін на е/е підтверджують їх не стаціонарність.

У зв'язку зі складними характеристиками часових рядів цін на е/е часто безпосередньому процесу побудови моделі прогнозу передують первинне коригування рядів у вигляді логарифмування, взяття різниці вихідного ряду. А в окремих роботах застосовується видалення викидів в аналізованому ряді, а для зручності аналізу - центрування вихідного ряду.

2) Часові параметри в моделях прогнозування.

У переважній більшості робіт часовий горизонт прогнозу становить 1 добу (в часовому або добовому розрізі). Однак, зустрічаються роботи, в яких прогнозуються ціни на 1-3, 1-7 або 1-30 днів наперед.

Підбір і тестування моделей реалізовано на досить широкому діапазоні даних:

- на російському оптовому ринку підбір моделей здійснювався на ретроспективних даних в діапазоні від 912 до 1461 дня, тестування на даних за 214 днів;

- на американських оптових ринках підбір моделей - на даних в діапазоні від 28 до 844 днів, тестування моделей - на даних в діапазоні від 1 до 365 днів;

- на європейських оптових ринках підбір моделей - на даних в діапазоні від 73 до 1561 дня, тестування моделей - на даних в діапазоні від 7 до 365 днів.

Для обліку періодичності (сезонності) в цінах на е/е використовуються такі підходи:

- включення в модель фіктивних змінних, що враховують години доби, дні тижня, календарні, святкові дні і ін.;

- розщеплення вихідного ряду на окремі компоненти, в тому числі і на компоненти сезонності, з наступною побудовою прогнозів для отриманих рядів;

- включення в модель ретроспективних даних - лагів послідовних або розподілених;

- комбінування перерахованих підходів.

У деяких роботах облік добової періодичності здійснюється побудовою прогнозу для 24 рядів цін.

Отже, багато дослідників включають в свої моделі прогнозу цін фіктивні змінні годин доби, днів тижня, календарних святкових днів, іноді місяців року і аналогічні їм. Включення лагів в моделі дозволяє вловити добову, тижневу, а також більш довгострокову періодичність. У деяких дослідженнях моделей прогнозування часових цін включені лаги до 504 значення.

3) Екзогенні змінні в моделях прогнозування.

Майже в половині робіт модель прогнозу ціни на е/е побудована тільки на її спостережуваних ретроспективних даних без включення екзогенних змінних. В інших роботах в модель прогнозу включені екзогенні змінні, які можуть враховувати: обсяг попиту (лагові історичні значення або прогнозні); еластичність попиту за ціною; вплив температурних або інших погодинних змінних (температура, довжина світлового дня і ін.), які зазвичай враховані в динаміці обсягу попиту, але як самостійні чинники спільно з об'ємом не розглядаються; ціни на паливо при короткострокових прогнозах як самостійний фактор теж не розглядаються.

Деякі дослідники звернули увагу на вплив технологічних особливостей ринку на рівень і динаміку цін на е/е - обсяг гідроенергії, накопичені в водосховищах обсяги води, є суттєвою екзогенної змінної при побудові прогнозів на ринках е/е з великими гідроелектростанціями. Параметри, що характеризують резерв генеруючої потужності, впливають на динаміку цін на е/е.

Отже, кожна модель прогнозування будується з урахуванням характеристик та особливостей рядів цін конкретного оптового ринку. Встановлено, що об'єднання інтегрованої моделі авторегресії - ковзного середнього (ARIMA) і моделі узагальненої авторегресійної умовної гетероскедастичності (GARCH) дозволяє вловлювати багато важливих особливостей рядів. Даний підхід широко поширений і успішно використовується. У ряді робіт зазначено, що вейвлет-перетворення в поєднанні із зазначеним підходом покращують точність прогнозу. У більшості робіт в якості екзогенних змінних використовувався обсяг попиту, рідше погодні змінні і ціна на паливо. Окремі роботи приділили увагу питанням впливу технологічних характеристик ринків, прояви ринкової сили виробниками і особливостей правил ринків на прогнозування ціни.

Однак, безумовних доказів переваги по точності прогнозування якої-небудь однієї моделі над іншими не виявлено.

В результаті аналізу робіт [5, 17-20] можна констатувати що, традиційно завдання прогнозу кількості споживаної енергії вирішується за допомогою регресійних моделей, але через те, що дані ряди споживання енергії не є стаціонарними, то регресійні моделі можуть призводити до зниження точності, якщо не виконувати процедуру приведення даних часового ряду до вимоги стаціонарності. Тому, для врахування такої особливості даних часового ряду в ряді робіт застосовуються нейросіткові моделі.

Так в роботі [21] обрана модель нейросітки для короткострокового прогнозування обсягу попиту і ціни на e/e , яка будується як однозмінна модель (з одним виходом) для погодинного прогнозу на наступну добу. Модель в якості регресорів (входів) використовує: історичні чинники - значення показника на 1 годину назад, на добу назад, на тиждень назад; сезонні фактори - годину доби, день тижня, ознаки приналежності поточного дня до вихідного, святкового, робочого дня; галузеві екзогенні фактори - графік завантаження ТЕЦ, ремонтні компанії, водність ГЕС, стратегії постачальників.

Аналізувалися різні варіанти структури моделі і встановлені наступні результати:

- найбільш точними є моделі, що включають обмежений набір вихідних екзогенних факторів. Внаслідок відсутності статистичних даних по таким специфічним параметрам, як навантаження електромережі, температура зовнішнього повітря, склад включеного генеруючого обладнання, водність річок, що відображають особливості функціонування ринку e/e та впливають на точність обліку сезонності, а також у зв'язку з неможливістю суворо детермінувати дані фактори на перспективу, відповідні показники не враховуються при формуванні моделі;

- підвищується точність прогнозування при обліку в моделі сезонних чинників;

- облік екзогенного системного фактора величини обсягу попиту в достатній мірі не впливає на точність прогнозування ціни і може бути виключений з моделі;

- в цілому більш висока точність досягається при прогнозуванні обсягів попиту на e/e , ніж при прогнозі ціни на неї через вплив на останній показник не тільки детермінованих факторів у перспективі.

В цілому, розглянута модель короткострокового прогнозування цін і обсягів споживання e/e на ринку на добу вперед на основі нейронних сіток дозволила сформувати з досить високим ступенем точності прогнозні значення показників в умовах волатильності і невизначеності в різні сезони року.

Таким чином, можна на підставі проведеного аналізу стверджувати, що процес створення моделі прогнозування цін та обсягів споживання e/e на оптовому дерегульованому ринку повинен пройти через певні етапи:

- аналіз характеристик часових рядів;
- первинне коригування рядів і врахування періодичності (сезонності);

- вибір типу моделі прогнозування, в тому числі часових параметрів (глибини використаних даних, горизонт прогнозу) та екзогенних змінних;
- оцінка точності моделі.

А в якості моделі прогнозування починають переважати інтелектуальні методи та гібридний підхід до застосування моделей, тобто створення комбінованих за принципом дії моделей прогнозування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Aggarwal S.K. Electricity price forecasting in deregulated markets: A review and evaluation / S.K. Aggarwal, L.M. Saini and A. Kumar // *International Journal of Electrical Power & Energy Systems*, 2009, Vol. 31, no. 1. - P. 13-22.
2. Bobinaite V. Theoretical model for electricity market price forecasting / V. Bobinaite, I. Konstantinavičiūtė, V. Lekavičius // *Economics and Management*, 2012, Vol.17, no 3. - P.944-951. (<https://doi.org/10.5755/j01.em.17.3.2119>)
3. Luo B. A Literature Survey on Electricity Price Forecasting in Deregulated Markets / B. Luo and S. Miao // 2019 IEEE Sustainable Power and Energy Conference (iSPEC), 2019. - P. 359-365. (<https://doi.org/10.1109/iSPEC48194.2019.8974939>)
4. Дробыш И.И. Статистические модели прогнозирования цен на оптовых рынках электроэнергии: российский и зарубежный опыт / И.И. Дробыш // *Вестник ЮУрГУ. Серия «Экономика и менеджмент»*. – 2017. – Т. 11, № 3. – С. 41–54. (doi: 10.14529/em170306)
5. Weron R. Electricity price forecasting: A review of the state-of-the-art with a look into the future / R. Weron // *International Journal of Forecasting*. - 2014, Vol. 30. - P. 1030–1081. (<http://dx.doi.org/10.1016/j.ijforecast.2014.08.008>)
17. Forecasting Models of Electricity Prices / Special Issue Editor J. Contreras // *Open access journal Energies*, Basel, Switzerland, MDPI, 2017. - 250 p.
18. Singh, S. Pattern Modelling in Time-Series Forecasting / S. Singh // *Cybernetics and Systems - An International Journal*, 2000, Vol. 31, no 1. – P. 49–65.
19. Чучуева, И.А. Модель экстраполяции временных рядов по выборке максимального подобию / И.А. Чучуева // *Информационные технологии*. – 2010. – № 12. – С. 43-47.
20. Смирнова Е.О. Прогнозирование рынка электроэнергии «на сутки вперед»: пример второй ценовой зоны / Е. О. Смирнова, А. Ю. Филатов // *Вестник ВГУ. Серия: Экономика и управление*. - 2018. - № 4. - С.149-159.
21. Золотова И.Ю. Краткосрочное прогнозирование цен на российском оптовом рынке электроэнергии на основе нейронных сетей / И.Ю. Золотова, В.В. Дворкин // *Проблемы прогнозирования*. - 2017. - №6. - С.47-57.

Владимирський Олександр Альбертович,
ІПМЕ ім. Г.Є. Пухова НАН України,
провідний науковий співробітник,
av1000000@ukr.net

Владимирський Ігор Альбертович,
ІПМЕ ім. Г.Є. Пухова НАН України,
старший науковий співробітник,
gosho2018@yahoo.com

ЗАСТОСУВАННЯ КОРЕЛЯЦІЙНИХ ПАРАМЕТРИЧНИХ МЕТОДІВ ПОШУКУ ВИТОКІВ ДЛЯ ПЕРІОДИЧНОГО МОНІТОРИНГУ ПІДЗЕМНИХ ТРУБОПРОВІДІВ СИСТЕМ ТЕХНІЧНОЇ ВОДИ ВІДПОВІДАЛЬНИХ СПОЖИВАЧІВ АЕС

Анотація. Пропонується застосування кореляційних параметричних методів пошуку витоків для проведення періодичного моніторингу прихованих під ґрунтом трубопроводних систем на територіях атомних електростанцій. Методи є розвитком широко застосовуваного для діагностики підземних трубопроводів кореляційного методу. Параметричні методи мають низку переваг, серед яких висока чутливість до акустично слабо виражених дефектів і наочність результатів діагностики.

Abstract. It is proposed to use correlation parametric leak detection methods for periodic monitoring of pipeline systems hidden under the ground in the territories of nuclear power plants. The methods are a development of the correlation method widely used for diagnostics of underground pipelines. Parametric methods have a number of advantages, including high sensitivity to acoustically weakly pronounced defects and clarity of diagnostic results.

Про важливість обстеження підземних трубопроводів АЕС йдеться, зокрема, у [1], де рекомендується використати досвід розробок із близьких областей. Доцільність цього підходу очевидна з огляду на високу відповідальність об'єктів АЕС, де мають застосовуватися лише добре перевірені методи діагностики. Зокрема, методи, які показали себе ефективними при діагностиці міських тепломереж. До таких методів відносяться кореляційні параметричні методи [2] через високу чутливість до дефектів на ранніх стадіях їх виникнення та чіткість результатів застосування [3]. Параметричні методи дозволяють подолати надмірність що міститься у взаємних кореляційних функціях (ВКФ) інформації щодо часто необхідних, інформативних домінуючих за потужністю сплесків у різних частотних смугах сигналів. Розроблений та реалізований у течешукачах сімейства К-10 метод аналізу заснований на суміщеному за частотою відображенні спектрів потужності, відношення сигнал-перешкода і координати для кожного домінуючого в окремій смузі частот сплеску ВКФ.

Число аналізованих таким способом частотних смуг практично є не обмеженим. Наочність і частотна повнота уявлення лише необхідних властивостей ВКФ полегшує їх просторовий аналіз. Такий аналіз часто необхідний через високу чутливість ВКФ до вибору місць реєстрації сигналів. Методи ефективні при інтерференційних спотвореннях, що виникають під час реєстрації когерентних сигналів зі складною хвильовою структурою [4]. Спектр відносин сигнал-перешкода вирішує завдання функції когерентності, проте з урахуванням корельованих перешкод та у зручній прив'язці до координати. Показано корисний практичний прояв та застосування параметричної структури, названої координатною полицкою у спектрі координат [2, 3, 4]. Наявність полицки швидко розпізнається на графіці і є хорошим індикатором наявності не випадкової кореляції на тлі випадкових осциляцій через статистичні похибки оцінки ВКФ. Подальший розвиток методу призводить до корисних параметрів неузгодженості параметричних спектрів потужності та відношення сигнал-перешкод при пошуку витоків [4]. Дані параметри добре орієнтовані на просторово-частотну селекцію ВКФ, яка сформована потужними хвилями гідравлічного удару з відомою швидкістю в умовах інтерференційних спотворень. Параметри неузгодженості можна використовувати для оцінки похибки координати пошкодження. Цю похибку зручно використовувати як критерій достатності вимірювань за різних положень датчиків. Метод пройшов апробацію при інтенсивному пошуку витоків у міських теплових мережах і може бути корисним у завданнях діагностики обладнання АЕС.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. В.В. Инюшев, А.И. Бережной, Э.А. Завизион, В.Н. Головкин, Е.И. Петропавловский. Обзор методов технического освидетельствования трубопроводов ответственных потребителей группы «А» на АЭС. Ядерная радиационная безопасность 3(59).2013.-С.10-15.
2. Владимирський О.А., Владимирський І.А. Кореляційні параметричні методи визначення координат витоків підземних трубопроводів // Електрон. моделювання, 2021, 43, № 3, с. 3—17.
3. Vladimirsky O, Vladimirovsky I., Dybach O. Parametric Analysis of Correlation Functions for Acoustic Monitoring and Assessment of Underground Piping at NPPs. Nuclear and Radiation Safety. 2022. No. 3(95). 64-70. doi: [https://doi.org/10.32918/nrs.2022.3\(95\).06](https://doi.org/10.32918/nrs.2022.3(95).06).
4. Владимирський О.А., Владимирський І.А. Параметричний кореляційний спосіб визначення координат витоків трубопроводів. Патент України № 144444. Публ. 25.09.2020р., Бюл. №18.

Цуркан Оксана Володимирівна,
ПІМЕ ім. Г. Є. Пухова НАН України,
молодший науковий співробітник,
otsurkan24@gmail.com

Герасимов Ростислав Павлович,
ПІМЕ ім. Г. Є. Пухова НАН України,
науковий співробітник,
gerasimov.rostislav@gmail.com

Клименко Тетяна Михайлівна,
ПІМЕ ім. Г. Є. Пухова НАН України,
Завідувачка науково-організаційного відділу,
klimenko-t@ukr.net

Яшенков Вадим Петрович,
ІЕ ім. Є. О. Патона НАН України,
науковий співробітник,
vadym.yashenkov@gmail.com

Коженьевський Сергій Романович,
ПІМЕ ім. Г. Є. Пухова НАН України,
кандидат технічних наук,
serhiikozhenevskyi@gmail.com

ФРЕЙМВОРК КІБЕРСОЦІАЛЬНОЇ ІНЖЕНЕРІЇ НА ОСНОВІ МОДЕЛІ KILL CHAIN

Анотація. Проаналізовано фреймворк кіберсоціальної інженерії на основі моделі Kill Chain. Встановлено особливості його використання, переваги та обмеження та узгодженість з базою знань MITRE ATT&CK.

Abstract. The cyber social engineering framework based on the Kill Chain model is analyzed. Features of its use, advantages, limitations and consistency with the MITER ATT&CK knowledge base are established.

Фреймворк кіберсоціальної інженерії орієнтований на моделювання атак упродовж різних стадій її використання [1]. За основу підходу взято модель Kill Chain. Насамперед це стосується спонукання людини до поведінки в інтересах кіберсоціального інженера. Демонстрування таких проявів досягається використанням бази знань MITRE ATT&CK. Водночас поза увагою залишено врахування психологічних станів людини при формуванні «бажаної» поведінки.

Отже, встановлено особливості використання, переваги та обмеження фреймворку кіберсоціальної інженерії на основі моделі Kill Chain. Як окрему перевагу показано узгодженість з базою знань MITRE ATT&CK.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Montañez Rodriguez, R., Xu, S. Cyber Social Engineering Kill Chain. Science of Cyber Security / C. Su, K. Sakurai, F. Liu. Cham, Switzerland : Springer, 2022. Vol. 13580. P. 487–504. DOI: https://doi.org/10.1007/978-3-031-17551-0_32.

Мохор Володимир Володимирович,
ПІМЕ ім. Г.С. Пухова НАН України,
член-кореспондент НАН України, доктор технічних наук, професор,
v.mokhor@gmail.com

Бакалинський Олександр Олегович,
ПІМЕ ім. Г.С. Пухова НАН України,
кандидат технічних наук, старший дослідник,
baov@meta.ua

Дорогий Ярослав Юрійович,
КПІ ім. Ігоря Сікорського,
доктор технічних наук, доцент,
argusyk@gmail.com

Цуркан Василь Васильович,
КПІ ім. Ігоря Сікорського, ПІМЕ ім. Г.С. Пухова НАН України,
кандидат технічних наук, доцент,
v.v.tsurkan@gmail.com

ТЕНДЕНЦІЇ РОЗВИТКУ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ СФЕРИ ЕНЕРГЕТИКИ

Анотація. Проаналізовано тенденції розвитку систем управління інформаційною безпекою об'єктів критичної інфраструктури сфери енергетики. При цьому враховано зміни 2022 року до міжнародних стандартів ISO/IEC 27k.

Abstract. The trends in the development of information security management systems of critical infrastructure facilities in the energy sector are analyzed. And the 2022 changes to the ISO/IEC 27k international standards are taken into account.

Тendenції розвитку систем управління інформаційною безпекою об'єктів критичної інфраструктури сфери енергетики обумовлюються оновленнями міжнародних стандартів ISO/IEC 27001:2022, ISO/IEC 27002:2022 та ISO/IEC 27005:2022. Перш за все вони характеризуються орієнтованістю на сценарії ризику, розширення та категорювання заходів. До того ж як визначення їх впливу на ризик, так і узгодження з діяльністю забезпечення кібербезпеки.

Отже, проаналізовано тенденції розвитку систем управління інформаційною безпекою. Показано їх орієнтованість на сценарії ризику та забезпечення кібербезпеки об'єктів критичної інфраструктури сфери енергетики.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO/IEC 27001 and related standards Information security management. URL: <https://www.iso.org/isoiec-27001-information-security.html> (accessed on: 14.11.2022).

Гільгурт Сергій Якович,
ІПМЕ ім. Г.Є. Пухова НАН України,
старший науковий співробітник, доктор технічних наук,
старший науковий співробітник,
hilgurt@ukr.net

Кіслов Олексій Геннадійович,
ІПМЕ ім. Г.Є. Пухова НАН України,
молодший науковий співробітник,
kislov@ipme.kiev.ua

Попова Валентина Миколаївна,
ІПМЕ ім. Г.Є. Пухова НАН України,
інженер першої категорії,
popovavn@ukr.net

ВИКОРИСТАННЯ ТРІЙКОВОЇ АСОЦІАТИВНОЇ ПАМ'ЯТІ НА РЕКОНФІГУРОВНІЙ ПЛАТФОРМІ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ

Анотація. Розглянуті питання використання трійкової асоціативної пам'яті на реконфігуровній платформі для вирішення задач захисту інформації в комп'ютерних системах і мережах. Наведено приклади готових рішень для застосування даної технології у вигляді IP-ядер.

Abstract. The issues of using ternary content-addressable memory on a reconfigurable platform to solve problems of information security in computer systems and networks are considered. Examples of ready-made solutions for the application of this technology in the form of IP-cores are given.

В монографії [1] проведено порівняльний аналіз апаратних платформ для прискорення задачі множинного розпізнавання патернів, яка є найбільш ресурсноємною в обчислювальному сенсі процедурою, що виконується в сигнатурних системах захисту інформації. В результаті порівняння таких напрямів, як спеціалізовані сопроцесори, мережеві процесори, трійкова асоціативна пам'ять, прискорювачі на базі багатоядерних процесорів, графічні акселератори та реконфігуровні обчислювачі на базі ПЛІС було з'ясовано, що саме реконфігуровна технологія якнайкраще відповідає складній та динамічній природі задач захисту інформації, а також випереджає конкуруючі технології за економічністю та гнучкістю, а уніфіковані обчислювачі на базі ПЛІС є найбільш придатною платформою для використання в системах захисту інформації.

Подальший аналіз підходів до побудови схем розпізнавання, вже на реконфігуровній платформі, також проведений в [1], виявив в якості одного з

найперспективніших напрямів технологію асоціативної пам'яті – Content-Addressable Memory (CAM) на базі цифрових компараторів.

Одним з різновидів технології асоціативної пам'яті є так звана трійкова асоціативна пам'ять – Ternary Content-Addressable Memory (TCAM), в якій на відміну від бінарної пам'яті, що має лише два стани: "0" або "1", кожна комірка може приймати також додатковий стан "?" (неважливо) [2]. Ця властивість дозволяє TCAM, не втрачаючи безпрецедентної швидкодії традиційної CAM, виконувати певні функції гнучкого розпізнавання [3], за рахунок чого, теоретично, мала б являти ще більший інтерес для розробників реконфігуровних засобів захисту інформації сигнатурного типу.

Але традиційне використання TCAM у вигляді інтегральних мікросхем, як було відмічено в [1], суттєво звужує можливості її застосування. Чинниками цього обмеження є жорстка архітектура та замалий об'єм словнику патернів. Тому в минулі роки технологія TCAM не отримала примітного розповсюдження при створенні засобів захисту інформації [1]. Однак стрімкий розвиток реконфігуровних обчислювальних засобів, в тому числі – у сфері захисту інформації, надає сьогодні цьому напрямку шанс на відродження. Поєднання переваг програмованої логіки із гнучкістю TCAM знов привертає увагу розробників до технічних рішень на її основі.

Сприяють відродженню трійкової асоціативної пам'яті уніфіковані рішення на базі ПЛІС у вигляді IP-ядер. В якості прикладів можна навести недавно анонсовані фірмою Xilinx/AMD універсальний модуль Ternary CAM Search v2.4 [4] та засновану на подальшій модифікації TCAM розробку Semi-Ternary CAM Search v2.4 [5].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гільгурт С.Я., Чемерис О.А. Реконфігуровні сигнатурні засоби захисту інформації комп'ютерних систем. Київ, Академперіодика, 2022. 297 с. DOI: <https://doi.org/10.15407/akademperiodyka.458.297>.
2. Yu F., Katz R.H., Lakshman T.V. Gigabit rate packet pattern-matching using TCAM. 12th IEEE International Conference on Network Protocols. Proceedings Paper, 2004. P. 174-183. DOI: <https://doi.org/10.1109/icnp.2004.1348108>.
3. Xu C.C., Chen S.H., Su J.S., Yiu S.M., Hui L.C.K. A Survey on Regular Expression Matching for Deep Packet Inspection: Applications, Algorithms, and Hardware Platforms. IEEE Communications Surveys and Tutorials. Vol. 18, No. 4, 2016. P. 2991-3029. DOI: <https://doi.org/10.1109/comst.2016.2566669>.
4. Ternary CAM Search v2.4. LogiCORE IP Product Guide. Vivado Design Suite. PG318 (v2.4) November 8, 2022. [Електронний ресурс] URL: https://www.xilinx.com/content/dam/xilinx/support/documents/ip_documentation/cam/v2_4/pg318-tcam.pdf. Дата звернення: 17.11.2022.
5. Semi-Ternary CAM Search v2.4. LogiCORE IP Product Guide. Vivado Design Suite. PG319 (v2.4) November 2, 2022. [Електронний ресурс] URL: https://www.xilinx.com/content/dam/xilinx/support/documents/ip_documentation/cam/v2_4/pg319-stcam.pdf. Дата звернення: 17.11.2022.

Коломієць Євген Анатолійович,
ПІМЕ ім. Г.С. Пухова НАН України,
науковий співробітник,
e.a.kolomiets@gmail.com

КОМП'ЮТЕРНІ ЗАСОБИ ОЦІНКИ БЕЗПЕКИ ЕКСПЛУАТАЦІЇ ЕНЕРГЕТИЧНИХ ПАЛИВНИХ СИСТЕМ ТРАНСПОРТНИХ ЛІТАКІВ

Анотація. Розроблено програмне забезпечення для оцінки займистості паливного бака на транспортних літаках методом Монте-Карло. Наведено опис, можливості та основні переваги нової комп'ютерної системи «Монте-Карло».

Abstract. Software has been developed for assessing the flammability of a fuel tank on transport aircraft using the Monte-Carlo method. Descriptions, possibilities and main advantages of the new Monte-Carlo computer program are presented.

Найважливіша вимога до повітряних суден – це забезпечення пожежо-вибухобезпеки компонентів енергетичних паливних систем – паливних баків. Вимоги щодо запобігання можливому займанню палива або його парів у надпаливному просторі паливних баків для літаків транспортної категорії викладено у документі FAR-25 [1]. Цей документ встановлює вимоги за межами займистості для конкретних типів баків: час незахищеності від займистості бака (час незахищеності у відсотках).

Для оцінки займистості паливного бака застосовується метод розроблений Федеральним управлінням цивільної авіації департаменту транспорту США (FAA) та представлений у документі “Метод оцінки займистості паливного бака. Посібник користувача” [2]. За допомогою обчислювальної моделі даного методу проводиться розрахунок великої кількості варіантів польотів, на формування умов яких використовується статистичний метод Монте-Карло. Для кожного польоту на підставі теплової моделі бака, що використовується, визначається час, протягом якого бак є займистим. Середня схильність до займання парком літаків є виражене у відсотках відношення сумарного часу, протягом якого незаповнений обсяг паливного бака здатний спалахнути, до сумарного часу для всіх проаналізованих польотів. Розрахунок тривалості пожежонебезпечного періоду для досить великої кількості рейсів у результаті дає статистично достовірні дані про тривалість пожежонебезпечного періоду. Час незахищеності від займання потім порівнюється з межами займистості, визначеними в нормах визначення відповідності. Цей метод є стандартизованим методом аналізу.

Обчислювальна модель методу представлена у документі FAA [2] у вигляді програми Visual Basic for Applications (VBA) та реалізована в Microsoft Excel як набір макросів та електронних таблиць. На основі цієї моделі розроблено нове програмне забезпечення: система оцінки займистості паливного бака на літаках методом Монте-Карло (система «Монте-Карло») [3].

Система «Монте-Карло» призначена для розрахунку методом Монте-Карло часу, протягом якого бак є займистим, у відсотках відносно загального часу польоту, аналізу та оцінки займистості паливного баку на транспортних літаках.

Система «Монте-Карло» дозволяє користувачу:

- Вводити в систему вихідні дані розрахунку:

- дані літака;
- дані польоту;
- робочі дані паливного бака;
- вихідні дані бака у корпусі літака;
- температурні дані паливного бака;
- дані, що визначають характер розрахунку та кількість розрахункових

випадків;

- дані про конструктивні характеристики засобів зниження займистості (далі FRM), необхідні для оцінки ефективності FRM.

- Запускати розрахунок для одиночного польоту або для декількох польотів.

- Контролювати процес розрахунку.

- Отримувати інформацію про помилки під час виконання розрахунків.

- Отримувати повну інформацію за результатами розрахунку у табличному та графічному вигляді: часу займистості паливного бака з урахуванням та без урахування FRM, загального та за фазами польоту, для поточного польоту та сумарного для всіх польотів.

- Аналізувати результати розрахунків та оцінювати займистість палива в баках на літаках відповідно вимогам FAR-25;

- Експортувати з системи результати розрахунків у вигляді текстових файлів та файлів електронних таблиць.

Система розроблена на мові програмування C# у середовищі Microsoft Visual Studio Community 2019, як додаток операційної системи Microsoft Windows (починаючи з версії 7) та збережена на десктопне використання. Система не потребує попередньої інсталяції у ОС Windows, але потребує наявності на комп'ютері користувача встановленої програмної платформи Microsoft .NET Framework версії не нижче 4.7.2.

Інтерфейс користувача системи реалізовано з використанням технології Windows Forms. Інтерфейс складається з наступних блоків:

- «Вихідні дані» – введення вихідних даних для розрахунку;
- «Результати по польотах» – перегляд результатів розрахунків виконаних для декількох польотів у табличній формі та у вигляді графіків;

- «Одиничний політ» - перегляд результатів розрахунку одиночного польоту в табличній формі та у вигляді графіків, результати одиночного польоту показані у двох різних графічних форматах: графіки на основі часу та висоти.

- «FRM» - надається інформація про займистість на кожному з етапів польоту (на землі, при наборі висоти, на кожному етапі польоту, при

зниженні та вирулюванні) без застосування та із застосуванням засобів FRM, а також загальний час польоту. Окремо представлені дані для польотів, при яких температура навколишнього середовища на землі перевищує 26.7°C.

- «Р.Д.1», «Р.Д.2» - перегляд результатів розрахунків для аналізу та оцінки займистості паливного баку.

Загальні переваги системи «Монте-Карло»:

- Забезпечує однакову точність й відповідність отримуваних результатів з додатком VBA в Microsoft Excel, як для одиничного польоту та й для довільного числа польотів.

- Дозволяє виконувати розрахунки з підвищеною швидкістю: порівняно з макросами Microsoft Excel швидкість основних розрахункових алгоритмів програми зросла мінімум у два рази.

- Не потребує наявності на комп'ютері користувача додатків Microsoft Office.

- Реалізована можливість інтеграції у систему власної програмної теплової моделі паливного баку транспортного літака, яка має бути розроблена у середовищі Microsoft Visual Studio з використанням мов програмування, що підтримуються середовищем.

- Система може бути використана для підтримки прийняття рішень при автоматизованому проектуванні, супроводі випробувань та дослідній експлуатації бортових авіаційних паливних систем сучасних українських транспортних літаків.

- Практичне використання системи дозволяє зменшити обсяги необхідних експериментальних досліджень та льотних випробувань, які потребують залучення значних державних коштів.

- Реалізовані у системі методи і засоби можуть бути використані для міжнародної сертифікації паливних систем літаків, без успішного проходження якої неможливо реалізовувати українські транспортні літаки на зовнішніх світових ринках.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Advisory Circular № 25.981-2A «Fuel Tank System Flammability Reduction Means».

2. U.S. Department of Transportation FAA DOT/FAA/AR-05/8 - Fuel Tank Flammability Assessment Method. User's Manual. [Електронний ресурс] URL: <http://www.fire.tc.faa.gov/systems/fuel tank/FTFAM.stm>

3. Комп'ютерна програма «Система оцінки займистості паливного бака на літаках методом Монте-Карло» («Монте-Карло»); Коломієць Євген Анатолійович; Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова Національної академії наук України. Свідоцтво про реєстрацію права на твір №113038, ДП «Український інститут інтелектуальної власності», 23 травня 2022.

Костенко Ганна Петрівна,
ІЗЕ НАН України,
інженер

Згуровець Олександр Васильович,
ІЗЕ НАН України,
провідний науковий співробітник, кандидат технічних наук,
старший дослідник,
oleks.zgur@gmail.com

ПЕРСПЕКТИВИ РЕГУЛЮВАННЯ ЕЛЕКТРИЧНОГО НАВАНТАЖЕННЯ В ЕНЕРГОСИСТЕМІ ЗА ДОПОМОГОЮ ЕЛЕКТРОМОБІЛІВ

Анотація. Надійне функціонування електроенергетичної системи неможливе без дотримання балансу генерації та споживання електричної енергії. Нерівномірність споживання викликає необхідність утримання достатніх обсягів регулюючої генерації. Істотна зношеність наявних теплових електростанцій (ТЕС) обмежує можливості з їх використання у якості регуляторів. Задача балансування додатково ускладнюється завдяки зростанню частки вітрової та сонячної генерації, а також пошкодженням енергетичної інфраструктури у наслідок військових дій. Одним зі шляхів вирішення цього питання може стати залучення електромобілів до процесу регулювання електричного навантаження енергосистеми України, що дозволить покращити як ефективність, так і безпеку її функціонування.

Abstracts. Reliable functioning of the electric power system is impossible without maintaining a balance of electricity generation and consumption. The unevenness of consumption causes the need to maintain sufficient volumes of regulating generation. Significant wear of existing thermal power plants (TPPs) limits the possibilities of utilizing them as regulators. The balancing task is further complicated by the growing share of wind and solar generation, as well as damage to the energy infrastructure as a result of military operations. One of the ways to solve this issue may be the involvement of electric vehicles in the process of regulating the electric load of the Ukrainian power system, which will improve both the efficiency and safety of its functioning.

В ОЕС України зберігається тенденція щодо значної нерівномірності добового графіка електричного навантаження (ГЕН), особливо в осінньо-зимовий період. Конфігурація добового ГЕН в цілому по Україні характеризується піком навантаження в години вечірнього максимуму, провалом навантаження в години нічної зони доби та відносно рівномірним споживанням електричної енергії протягом годин ранкового максимуму та напівпікової зони. При цьому нерівномірність добового графіка навантаження ОЕС України становить від 4500 МВт у літній період до 6500 МВт у зимовий [1].

Генеруючі джерела фактично знаходяться на стадії вичерпання фізичних можливостей для забезпечення добового регулювання і раціональних режимів роботи електростанцій. З цієї причини вже найближчим часом необхідна їх повна або часткова модернізація, а також введення в роботу нових високоманеврових потужностей, що вимагає значних інвестицій. Тому впровадження та використання системи децентралізованих споживачів-регуляторів на основі електромобілів для регулювання електричного навантаження є потенційно ефективним для пом'якшення негативних наслідків проблеми нерівномірності ГЕН енергосистеми України за рахунок виключення відповідних потужностей ТЕС з роботи в маневреному режимі.

Збільшення кількості електричних транспортних засобів, яке спостерігається протягом кількох останніх років, робить їх важливою складовою системи електропостачання як на регіональному рівні, так і на рівні всієї країни. Розвиток електричних мереж з інтегрованими електромобілями, розробка і використання технологій Smart Grid, а саме Vehicle-to-Grid (V2G), для них здійснюється з урахуванням додаткових вимог і обмежень відносно режимів заряду тягових батарей автомобілів з метою забезпечення їх ефективної інтеграції в систему електропостачання [2].

На сьогодні реалізовано можливість інтеграції електричних транспортних засобів в електричну мережу при використанні їх для регулювання навантаження енергосистеми, яка полягає в тому, щоб заряд акумуляторів транспортних засобів здійснювати під час мінімуму навантаження енергосистеми, а в пікові періоди часу – генерувати енергію від акумулятора в мережу [2,3]. Масове використання електромобілів в такому режимі дозволить знизити попит на електроенергію в пікові періоди, що, у свою чергу, знижує потребу в пікових електростанціях і допомагає зменшити шкідливі викиди, оскільки такі генеруючі джерела більш екологічні й ефективні порівняно з електростанціями, що забезпечують базове навантаження. Ця задача актуальна як для багатьох європейських країн, так і для України.

Для впровадження такого підходу використання електромобілів необхідно вирішити наступні задачі: проаналізувати графіки навантажень енергосистеми України для оцінки доцільності регулювання навантажень за допомогою електротранспорту, оцінити економічну привабливість регулювання з погляду власників електромобілів, розробити технічні засоби для передачі електроенергії в мережу, її обліку і програмне забезпечення для управління процесами заряду-розряду, розробити топологію розташування точок генерації енергії і визначити можливі зміни електричної мережі.

Застосування технології V2G має ряд переваг та недоліків.

Переваги:

- Концепція дозволяє автомобілям із технологією V2G допомогти балансувати добові графіки навантаження, заряджаючи автомобіль уночі при низькому попиті та продаючи енергію назад у мережу, коли попит високий.

- При диференційованих тарифах на електроенергію власники транспортних засобів з V2G можуть споживати енергію в години з дешевшим тарифом, а продавати в мережу за вищим.

- У майбутньому ця технологія може забезпечити зберігання енергії, отриманої від ВДЕ, таких як енергія вітру та сонця. Наприклад, споживаючи надмірну енергію, що виробляється у вітряні періоди, і віддаючи її назад у мережу у періоди високого навантаження, транспортний засіб з технологією V2G може ефективно стабілізувати мінливість генерації ВДЕ.

- Технологія дозволяє компенсувати витрати на заміну акумуляторної батареї та необхідне обладнання для підключення до технології V2G, а також несе в собі нове джерело економічної вигоди для учасників концепції.

Недоліки:

- Батареї мають кінцеву кількість циклів зарядки, а також термін придатності, тому використання транспортних засобів як накопичувача в мережах може вплинути на довговічність батареї. Дослідження, в яких відбувається цикл батарей два або більше разів на день, показують значне зниження ємності та скорочення терміну служби.

В сучасних умовах розвитку децентралізованих систем енергозабезпечення для України існує значний потенціал залучення електротранспорту та використання технології V2G. Реалізація типових або індивідуальних шаблонів використання технології V2G та залишкової ємності відпрацьованої батареї дозволяє мати економічний ефект автовласнику разом з компенсацією її прискореного зносу. Головною складністю практичного застосування технології V2G є відсутність розробленої нормативної документації, правил участі на ринку електроенергії та затверджених законодавчих актів з відповідними вимогами та умовами до впровадження цієї технології.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Khatskevych Yu.V., Lutsenko I.M., Rukhlov A.V. Perspectives of load management in energy system with help of electric cars. Scientific Bulletin of the National Mining University. 2017. Vol. 5, pp. 82–88.
2. Mets, K., Verschueren, T., Turck, F. and Develder, C., 2011. Exploiting V2G to optimize residential energy consumption with electrical vehicle (dis)charging. In: 2011 IEEE First International Workshop on Smart Grid Modeling and Simulation (SGMS), 17 October 2011.
3. Kara, E.C., Macdonald, J.S., Black, D., Bérges, M., Hug, G. and Kiliccote, S., 2015. Estimating the Benefits of Electric Vehicle Smart Charging at Non-Residential Locations: A Data-Driven Approach. Applied Energy, 155, pp. 515–525.

Криворучко Ігор Петрович,
ПІМЕ ім. Г.Є. Пухова НАН України,
аспірант,
uhmi_igorkr@ukr.net

КУСКОВО-ЛІНІЙНА АПРОКСИМАЦІЯ ГЛАДКИХ, ПЛОСКИХ КРИВИХ МЕТОДОМ СІЧНИХ

Анотація. Для спрощення реалізації руху каретки віброкалібрувального комплексу пропонується апроксимація синусоїди кусково-лінійною функцією. Запропонований раніше алгоритм розбиття аналітично заданої функції методом «хорд» модифікований у алгоритм розбиття методом «січних», який має переваги по ступеню подібності з вихідною кривою, зменшенню кількості лінійних елементів. Детально описується алгоритм розбиття вихідної функції. Наводяться дані щодо порівняння обох методів розбиття.

Abstract. In order to simplify the implementation of the movement of the carriage of the vibro-calibration complex, the approximation of the sinusoid by a piecewise linear function is proposed. The previously proposed algorithm for piecewise linear partition an analytically given function using the "chord" method has been modified into a piecewise linear partition algorithm using the "secant" method, which has advantages in the degree of similarity with the original curve and the reduction of the number of linear elements. The algorithm for splitting the original function is described in detail. Data on the comparison of both partitioning methods are given.

Апаратно-програмний віброкалібрувальний комплекс складається із системи приводу руху каретки з датчиками параметрів руху (акселерометри) та вимірювального блоку [1]. Відповідно до ТЗ потрібно забезпечити періодичний рух каретки з досить високими показниками якості руху. Передбачений у якості приводу кроковий двигун (КД) має, як і всі КД, ступінчастий характер обертання якоря. Обертальний рух якоря за допомогою спеціального пристрою - актуатора перетворюється на послідовне ступінчасте переміщення каретки.

Одним із основних типів коливань каретки – синусоїдальний рух. Реалізація синусоїдального руху каретки вимагає розрахунку моментів здійснення чергового кроку згідно з формулою наведеною в [2].

Апроксимація гладких ліній кусково-лінійною функцією актуальна в багатьох застосуваннях, де це представлення може значно спростити технологічний процес без суттєвого програшу у якісних показниках. Наприклад, запис даних кусково-лінійної апроксимуючої функції вимагає значно меншого об'єму пам'яті, в порівнянні з апроксимованою.

Іншим варіантом реалізації синусоїдального руху є представлення його кінцевим числом послідовно з'єднаних прямолінійних відрізків. Перевага такого представлення - рівність часових інтервалів кожного кроку в межах окремого відрізка. У такому разі розмір пам'яті для зберігання

величин інтервалів зменшується у сотні разів. Заміна руху по синусоїді рухом по ламаній полілінії супроводжуватиметься збільшенням нелінійних спотворень у порівнянні з еталонним. Метод апроксимації плоскої кривої представленої в явній формі відрізками прямих ліній було розглянуто в роботах [3,4].

Запропоновано метод розбиття чи представлення гладкої кривої кусково-лінійною функцією, який в порівнянні з розбиттям методом «хорд» зменшує ступінь відмінності апроксимованої і апроксимуючої кривих для вибраного числа сегментів.

Очевидно, що зі збільшенням числа відрізків, що використовуються для представлення синусоїди, зменшується ступінь відмінності двох графіків. Для оцінювання рівня відмінності можна використовувати кілька оцінок: коефіцієнт кореляції, Евклідова відстань, різницю площ двох графіків, сума квадратів відхилень у заданих точках (квадратичне наближення), а також максимум модуля різниці та ін. Оцінка K_n , отже, і величини гармонійних складових дуже важлива. Запропонований новий метод кусково-лінійної апроксимації розглядається нижче.

На Рис.1. наведено графічне пояснення принципу модернізованого алгоритму кусково-лінійної апроксимації плоскої кривої деякої гладкої функції $F(x)$.

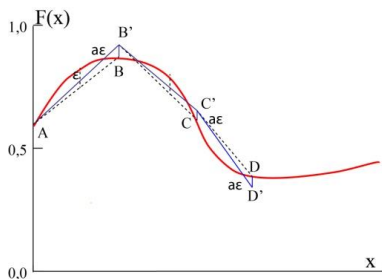


Рис.1

Перша точка першого відрізка відповідає крайній точці **A** на графіку. Послідовно перебираючи наступні точки лінії у якості другої точки відрізка і будуючи тимчасові відрізки розраховуємо максимальне відхилення від точок відрізка і відповідних точок на кривій. Якщо це значення відхилення досягає величини ϵ з установленим допуском, то ця точка **B** вибирається як друга точка відрізка **AB**. Наступним кроком відбувається коригування положення точки **B**. Для цього до ординати т.**B** додаємо величину $a\epsilon$, де a — коефіцієнт такий що $a \in \{0,1\}$. Причому, знак при a залежить від того, чи опукла крива в точці **B**. Якщо опукла, то знак при a вибирається додатний, якщо вгнута — від'ємний. Таким чином, другою крайньою точкою першого відрізка стає **B'**. Далі процес повторюється до перебору всіх точок гладкої кривої. Послідовно сполучуючи точки **A, B', C', D'**, отримуємо ламану криву. Для кінцевої точки останнього відрізка її зміщення по ординаті не проводиться.

У якості прикладу кусково-лінійної апроксимації на Рис. 2 наведено графіки відповідно апроксимованої функції $F(\varphi)=\text{Cos}(\varphi)$ (синій колір) та її

наближення - кусково-лінійну функцію (червоний колір), яка містить 4 лінійних відрізка методом «хорд» (а) та модифікованим методом - «січних» (в).

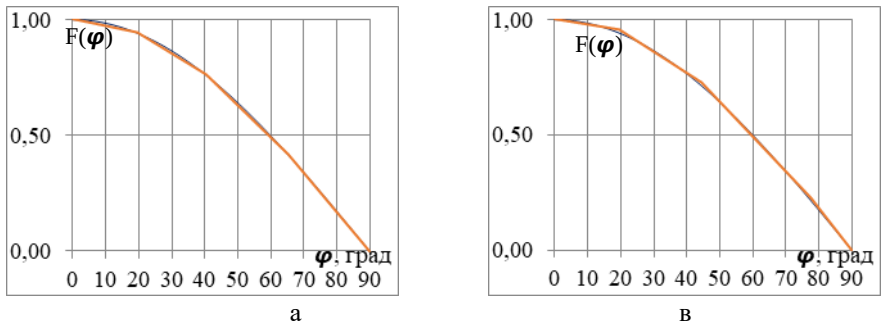


Рис 2.

У цьому випадку як і в наступних розрахунки проводилися для періодичної функції $F(\varphi) = \text{Cos}(\varphi)$ і частоти коливачь $F=5$ Гц. Результати розрахунків з апроксимації цієї функції методом «хорд» та «січних» (жовтий фон) наведені у таблиці 1.

Таблиця 1

Параметр	Величина відхилення ϵ							
	0,1	0,05	0,025	0,012	0,006	0,003	0,0015	0,001
N_{seg}	2	3	3	5	6	8	12	14
	2	2	3	4	5	7	10	13
R	0,9964	0,9989	0,9998	0,9999	1	1	1	1
	0,9947	0,9987	0,9997	0,9999	1	1	1	1
$K_r, \%$	3,71	2,68	0,98	0,63	0,16	0,05	0,05	0,03
	4,96	2,61	1,13	0,54	0,25	0,09	0,05	0,02
ρ_{ev}^m	0,054	0,034	0,015	0,0083	0,004	0,002	0,001	0,0007
	0,04	0,023	0,0097	0,0047	0,0027	0,0013	0,0007	0,0005
Fr	0,096	0,048	0,024	0,012	0,0058	0,003	0,0015	0,001
	0,08	0,04	0,02	0,0096	0,0048	0,0024	0,0012	0,0008

В залежності від заданої величини відхилення ϵ частина косинусоїди, що зображена на Рис.3 апроксимується різною кількістю сегментів N_{seg} . Порівняння даних наведених у таблиці 1 доцільно робити за окремими параметрами.

Зі зменшенням допустимого відхилення ϵ число відрізків апроксимуючої лінії N_{seg} зростає від 2 до 14. Однак у випадку «січних» спостерігається зменшення цієї величини по відношенню до «хорд». Тобто

забезпечення тієї ж величини відхилення ε можливе меншим числом відрізків.

Аналіз поводження коефіцієнта кореляції Пірсона R показує його недостатню інформативність для цього випадку, адже діапазон його зміни дуже невеликий і починаючи з деякого значення ε стає рівним 1. Найкращим серед наведених у таблицях параметром подібності апроксимованої і її представлення є Евклідова відстань ρ_{ev}^m добре корелює з ε . Інший показник подібності кривих - відстань Фреше має схожий до ρ_{ev}^m хід і порядок величини, але дещо складніший для розрахунків.

Якщо порівнювати між собою обидва методи, то ρ_{ev}^m для методу «хорд» на 35÷76% перевищує відповідне значення для методу «січних». Останній з наведених у таблицях коефіцієнт гармонік K_g використовується для оцінювання якості періодичної функції. Оскільки основним режимом коливач каретки віброкалібрувальної системи є періодичний синусоїдальний рух реалізований як рух кусково-лінійною траєкторією, оцінка якості такого руху є актуальною. Але використання цього параметру має певні особливості.

Слід відзначити достатньо високу якість апроксимуючої лінії для малих ε . Наприклад, розрахунковий рівень $K_g=0,02\%$ можна отримати апроксимацією $\frac{1}{4}$ косинусоїди 13-ма відрізками.

Також була проаналізована можливість кусково-лінійної апроксимації не лише графіка функції $F(\varphi)=\text{Cos}(\varphi)$, але і функції $F(\varphi)=\text{Cos}(3\varphi)+1.2$, яка на інтервалі $\varphi \in \{0, \pi/2\}$ має кривизну різних знаків.

Порівняльні розрахунки показали зростання міри подібності апроксимованої функції і її кусково-лінійного представлення цим методом у порівнянні з апроксимацією методом «хорд». Запропонований підхід може бути застосований також і для плоских кривих заданих таблично.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Владимирський О.А., Владимирський І.А., Івашенко А.П., Криворучко І.П. Розробка структури низькочастотної автоматизованої вібро-калібрувальної установки НАВКУ-3. Моделювання та інформаційні технології. Збірник наукових праць. Інститут проблем моделювання в енергетиці НАН України. Вип. 89, Київ, 2019р.-с.45-49.
2. Криворучко І.П. Методика розрахунку параметрів управління крокових двигунів для моделювання руху довільного характеру, Моделювання та інформаційні технології. Збірник наукових праць. Інститут проблем моделювання в енергетиці НАН України. Вип. 91, Київ, 2020 р.
3. Stone H. Approximation of curves by line segments// Mathematics of computation. 1961, vol. 15, № 73, p. 40-47.
4. Ленчук И.Г., Павленко Ю.С., Залевский В.И., Павлов А.В. Кусочно-линейная аппроксимация контуров деталей швейных изделий с заданным допуском// Известия вузов. Технология легкой промышленности, 1977, № 4, с.109-116.

Левкін Дмитро Артурович,
*Державний біотехнологічний університет,
доцент кафедри фізики та математики,
кандидат технічних наук, доцент,
dimalevkin23@gmail.com*

Макаров Олександр Анатолійович,
*Харківський національний університет імені В.Н. Каразіна,
доцент кафедри прикладної математики,
кандидат фізико-математичних наук, доцент,
makarovifamily07@gmail.com*

ЗАСТОСУВАННЯ МАТЕМАТИЧНИХ МЕТОДІВ ДЛЯ КОНТРОЛІНГУ ЕНЕРГЕТИЧНИХ ВИТРАТ В ТЕХНОЛОГІЧНИХ ПРОЦЕСАХ

Анотація. В роботі запропоновані математичні моделі і методи для підвищення точності контролінгу енергетичних витрат в технологічних процесах.

Abstract. The study proposes mathematical models and methods for increasing the accuracy of controlling energy costs in technological processes.

В роботі досліджені деякі аспекти розв'язання задачі підвищення ефективності контролінгу енергетичних витрат в технологічних процесах. Актуальність наведених досліджень підтверджена в роботах багатьох вчених, серед яких виокремимо наукові публікації [1, 2]. Підвищення точності контролінгу енергетичних витрат досягається завдяки збільшенню кількості врахованих факторів при реалізації розрахункових і прикладних оптимізаційних математичних моделей [3]. Однак, збільшення деталізації модельованих систем ускладнить реалізацію математичних моделей.

Коли необхідно забезпечити контролінг енергетичних витрат для багатошарового матеріалу під дією джерел термічної дії, то для обґрунтування коректності розрахункових математичних моделей автори пропонують розбити диференціальний символ основного диференціального рівняння з крайової задачі на суму двох символів. Для цих символів потрібно перевірити виконання умов експоненціально-коректних поліномів сталої сили та підлеглості. Якщо зазначені умови виконані, то крайова задача буде коректною в функціональних просторах.

Побудуємо рівномірну сіткову модель оптимізації технічних параметрів (потужність і час) термічної дії. Для значень потужності та часу, які характерні вузлам сіткової моделі, розв'яжемо крайові задачі і знайдемо значення функції мети. Розрахуємо пошкодження матеріалу у вузлових точках сіткової моделі. З метою збільшення точності контролінгу

енергетичних витрат здійснено подрібнення кроків сіткової моделі і розрахуємо пошкодження матеріалу під термічною дією з величинами потужності та часовими витратами, які характерні для вузлів подрібненої рівномірної сітки. Процес подрібнення кроків сіткової моделі та аналізу пошкодження матеріалу в вузлових точках продовжиться доти не буде вичерпаний час, відведений на оптимізацію параметрів, або не буде досягнуто необхідної точності контролінгу енергетичних витрат.

Результати наведених досліджень доцільно застосувати для розрахунку і оптимізації довільних параметрів технологічних процесів. Підвищення ефективності контролінгу енергетичних витрат модельованих процесів досягається завдяки збільшення точності реалізації розрахункових математичних моделей (крайових задач) в технологічних процесах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Згуровець О.В., Костенко Г.П. Ефективні методи управління споживанням електричної енергії. *Проблеми загальної енергетики*. Київ, 2007. № 2(16). С. 75–80.

2. Stanytsina V., Artemchuk V., Bogoslavskaya O., Zaporozhets A., Kalinichenko A., Stebila J., Havrysh V., Suszanowicz D. Fossil Fuel and Biofuel Boilers in Ukraine: Trends of Changes in Levelized Cost of Heat. *Energies*. 2022. Vol. 15. Issue. 19. 7215. <https://doi.org/10.3390/en15197215>

3. Kravtsov A., Suska A., Biekirov A., Levkin D. Development of a rheological model of stress relaxation in the structure of an oil film on the friction surface with fullerene additives. *Eastern-European Journal of Enterprise Technologies*. 2021. Vol. 3. No. 7 (111): Applied mechanics. Pp. 93–99: <https://doi.org/10.15587/1729-4061.2021.235468>

Лепатьєв Антон Олександрович,
ІПМЕ ім. Г.Є. Пухова НАН України,
аспірант, провідний інженер,
antonlepatiev@gmail.com

ТРИ ЦИКЛИ ПО МАСИВУ КОМПОНЕНТІВ МНЕМОСХЕМИ У АВТОМАТИЧНІЙ ПІДГОТОВЦІ ДАНИХ ДЛЯ РОЗРАХУНКУ РЕЖИМУ

Анотація. у даних тезах описується процес підготовки структурних параметрів і посилань при автоматичній підготовці даних для розрахунку режиму. Подається опис кожного з трьох циклів по масиву компонентів мнемосхеми.

Abstract. these theses describe the process of preparing structural parameters and references during automatic data preparation for mode calculation. The description of each of the three cycles through the array of mnemonic components is presented.

Під час розроблення тренажерного завдання розробник, при ручній підготовці даних для розрахунку режиму, структурні параметри(номера компонентів, індекси гілок) вводить їх вручну. Головним недоліком даного методу підготовки даних є можливість помилки при вводі структурних даних. Ці помилки можуть виникнути, якщо скопіювати компонент у редакторі, вставити новий компонент, проте забути змінити значення структурних параметрів. Відповідно декілька компонентів можуть мати однаковий номер або індекс і через це розрахунок режимів некоректний. Пошук на якому саме компоненті невірно записані структурні параметри займає багато часу. Дана проблема вирішується за допомогою автоматичної підготовки даних моделі режиму. На відміну від ручної підготовки даних моделі режиму електричної мережі, в автоматичній підготовці даних структурні параметри заносяться автоматично(без участі розробника тренажерного заняття), тим самим нівелюється можливість помилки під час присвоєння структурних параметрів. Процес підготовки структурних параметрів і посилань відбувається під час трьох циклів по масиву компонентів мнемосхеми.

Перед початком проходження циклів, розробник тренажерного завдання перетягує з бібліотеки компонентів у робоче поле графічного редактору необхідний йому компонент. Після перетягування розробник задає технологічні параметри(коефіцієнт трансформації, провідність і так далі). Після додавання усіх компонентів і заповнення усіх технологічних параметрів необхідно запустити програму. Після запуску відбувається перший цикл по масиву компонентів.

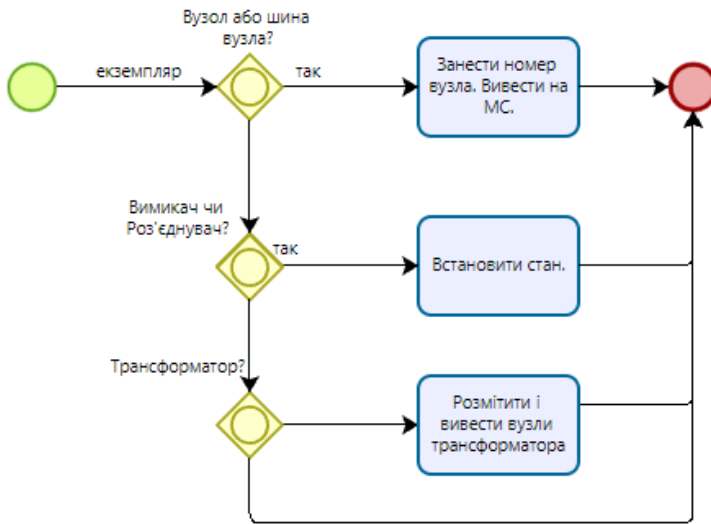


Рисунок 1. Перший цикл по екземплярам компонентів

Під час першого циклу, компоненти “Вузол” та “Трансформаторний вузол” отримують свій номер в залежності від порядку додавання у графічному редакторі Flash(вузол котрий додали першим отримує номер 0, вузол котрий додали другим номер 1 і т.д.). Задля зручності розробника тренажерного завдання та персоналу, який буде проходити завдання, номери вузлів та трансформаторних вузлів виводяться на мнемосхему. Також, у першому циклі по масиву компонентів встановлюється стан вимикачів та роз’єднувачів(увімкнений чи ввімкнутий).

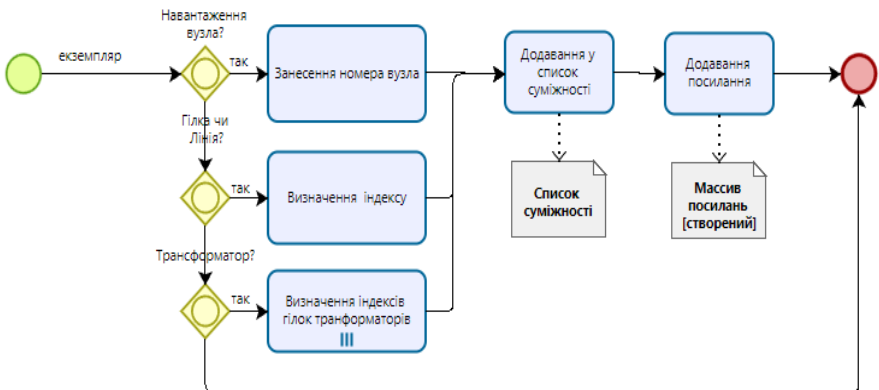


Рисунок 2. Другий цикл по екземплярам компонентів

У другому циклі по масиву компонентів гілкам, лініям та гілкам трансформаторів присвоюються структурний параметр індекс[2]. Компоненту навантаження вузла присвоюється номер. . Номер цього компонентів дублює номер вузла, до якого приєднано навантаження. Далі структурні параметри заносяться у список суміжності, а посилання на компоненти у масив посилань. Ці два масиви застосовуються у розрахунку режиму.

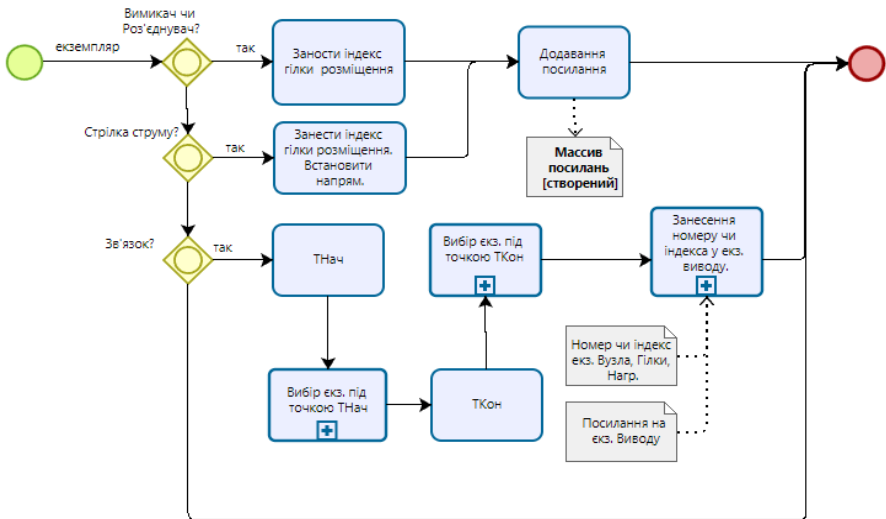


Рисунок 3. Третій цикл по екземплярам компонентів

Третій цикл по масиву компонентів починається з занесення індексів для вимикачів і роз'єднувачів. Індекс цих компонентів дублює індекс гілки розміщення. Стрілка струму таким самим чином отримують і свій індекс. Також автоматично встановлюється напрям стрілки. Напрямок стрілки залежить від руху токів. Після вище описаних дій, додається посилання на компоненти вимикача, роз'єднувач та стрілка струму. Посилання на дані компоненти додається у масив посилань. Останнім компонентом який проходить масив по компонентам є зв'язок, який виконує функцію переносу структурного параметру з одного компоненту до іншого. Для передачі структурного параметру необхідно Один кінець лінії зв'язку розмістити так, щоб він входив у вузол або гілку. Інший кінець лінії повинен входити у вивід. У разі не виконання цієї умови не відбувається передача індексу гілки або номеру вузла на вивід, і вивід буде показувати некоректні результати або взагалі не буде їх показувати[3]. Після завершення усіх трьох циклів у по масиву компонентів кожен компонент мнемосхеми має структурний параметр і модель має можливість почати розрахунок режиму.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Лепатьев А.О. Побудова мнемосхеми при автоматичній підготовці структурних даних моделі режиму. Київ, XL Науково-технічна конференція молодих вчених та спеціалістів інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України: матеріали, 11 травня 2022 р.
2. Лепатьев А.О. Триобмоткові трансформатори на мнемосхемі при автоматичній підготовці даних моделі режиму розподільчої мережі. Київ, X Всесвітній конгрес "Авіація у XXI столітті" – "Безпека в авіації та космічні технології") 28-30 вересня 2022 р.
3. Лепатьев А.О. Вивід значень струмів і напруг на мнемосхемі при автоматичній підготовці даних моделі режиму. Київ, Збірник тез XXXIX Науково-технічної конференції молодих вчених та спеціалістів інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України 12 травня 2021.

Митько Лідія Олексіївна,
ІПМЕ ім. Г.Є. Пухова НАН України,
кандидат фізико-математичних наук,
старший науковий співробітник,
lmitko@ukr.net

АНАЛІЗ ПРОПОЗИЦІЙ ЄВРОПЕЙСЬКИХ НАУКОВЦІВ ДЛЯ ЕНЕРГЕТИЧНОЇ ГАЛУЗІ З МЕТОЮ ЇХ АДАПТАЦІЇ В УКРАЇНІ, ВИКОРИСТОВУЮЧИ ЦИФРОВІЗАЦІЮ

Анотація. Ефективне управління енергетичною галуззю України дуже важливе не тільки нинішній ситуації, але і в середньостроковій та довгостроковій перспективі. Тому використання досвіду, пропозицій європейських вчених із залучення цифрових технологій сприятиме стійкості енергетичної безпеки Української держави.

Abstract. Effective management of Ukraine's energy industry is very important not only for the current situation, but also in the medium and long term. Therefore, the use of experience and proposals of European scientists on the involvement of digital technologies will contribute to the stability of the energy security of the Ukrainian state.

В період війни проблема забезпечення світлом та теплом населення, установи та підприємства України виводить енергетичну галузь на рівень забезпечення держави військовими ресурсами. А враховуючи, що енергетичні об'єкти стають першочерговими цілями для ворога, подальше використання багатьох механізмів управління енергетичними об'єктами і процедур їх функціонування, що були в довоєнний період, на сьогодні потребує нових підходів і законодавчого забезпечення. Враховуючи, що часу для розробки нових механізмів і підходів не має, то було б доцільним залучити досвід європейських країн в підходах до зменшення негативних явищ в енергетичній сфері у воєнний час.

Провідні світові науковці пропонують кроки [1], які повинні допомогти енергетичній галузі мати більш стабільне функціонування. Так першим кроком пропонується розробити програму по скороченню попиту на енергетичні ресурси паралельно з широким моніторингом споживання та фінансовими стимулами. Така програма в Україні не можлива без залучення широкомасштабної цифровізації споживання енергетичних ресурсів. В цій програмі повинна бути чітка лінія на обмеження використання електроенергії та енергоносіїв для неосновних послуг. Всі установи повинні мати максимальні зимові температури в приміщеннях, які будуть значно нижчими, ніж минулого року; мінімізувати нічне освітлення та більше

використовувати в роботу в час, який не потребує додаткового освітлення. Зниження попиту буде стимулювати зниження цін на енергоносії.

Другий аспект стосується імпорту енергоємних продуктів. Оскільки існує обмеженість наявності таких продуктів, бажано переглянути наявні енергетичні продукти з метою можливості продовження термінів їх служби. Одним із важливих факторів при цьому є заохочення використання наявних ресурсів для обігріву, освітлення і виробництв із заохоченням населення і промисловості використовувати або заряджати побутові пристрої і прилади в час, коли є зменшений попит на наявні ресурси.

Третє – це об'єднання зусиль населення, управлінських і законодавчих структур з метою створення активних програм консультацій та заходів з енергоефективності із заохочуванням населення вимикати пристрої, де це можливо, вдома та на роботі; зменшувати або вимикати радіатори в приміщеннях, де ніхто не перебуває. Паралельно потрібна винагорода та заохочення ефективного використання громадських місць для збереження тепла; місцеві органи влади також слід заохочувати до розблокування дозволів на планування для місцевих енергетичних схем, зменшити кількість бюрократичних заперечень щодо виробництва енергії.

Четвертим аспектом є розробка справедливих схем ціноутворення на енергетичні ресурси, які б також стимулювали енергозбереження. Одним із таких способів в європейських країнах пропонують запровадження зростаючого блокового тарифу зі знижкою для всіх побутових споживачів енергії. Це також є способом ефективного нормування енергії при збереженні доступності. Відповідно до зростаючого блоку, кожне домогосподарство може отримати нижчу ціну розподілу енергії, яка може бути визначена вимірними характеристиками домогосподарства за низькою ціною, а за використання більше, ніж визначено, зіткнутися із різким зростанням ціни. Тут може бути поєднання з винагородою за зменшення споживання енергії порівняно з минулорічним споживанням.

П'ятим пунктом є створення тимчасової системи ціноутворення, щоб уникнути спекуляцій в енергетичному секторі в ці виняткові часи. У воєнний час звичайні ринкові механізми для основних товарів і послуг призупиняються на користь адміністративних механізмів, призначених для збалансування потреби в ефективному виробництві товарів і послуг, та необхідності досягнення справедливого розподілу цих товарів і послуг. Приватна власність на виробництво може продовжуватись, але спекуляція на війні має бути обмежена, а прибутки суворо регламентовані. У воєнний час усіх потрібно заохочувати економити на використанні обмежених ресурсів, виробляти власні там, де це можливо і погоджуватися на незручні (але обов'язкові) обмеження на використання енергетичних ресурсів. При обговоренні питань забезпечення держави енергоресурсами, науковці [2] звертають увагу на рентабельне виробництво енергії або закупівлю джерел енергії при адекватному управлінні потоками енергії, тобто правильному

просторовому та часовому забезпеченню теплом та електроенергією споживачів.

Для стимулювання енергетичної безпеки країни необхідно поєднати підвищення ефективності, генерування відновлюваної енергії, зберігання енергії та використання відпрацьованого тепла. Практичне вирішення цих питань розглядається вже давно, але на сьогодні потребує швидких кроків з урахуванням обмеженого доступу до енергетичних ресурсів.

Ефективне управління енергетичною галуззю дуже важливе для забезпечення попиту не тільки нинішній ситуації, але і в середньостроковій та довгостроковій перспективі. А забезпечення енергетичними ресурсами України не можливе без широкого залучення цифрових технологій для моніторингу, аналізу і прийняття невідкладних управлінських рішень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Michael Pollitt. CERRE on the Energy Crisis: The Energy Market in Time of War. [Електронний ресурс] URL: <https://cerre.eu/news/cerre-on-the-energy-transition-the-energy-market-in-time-of-war/> Дата звернення: 15.09.2022
2. Harald Christ. Wir müssen uns aus der Energie-Krise herausmanagen! [Електронний ресурс] URL: <https://www.wiwo.de/politik/deutschland/energiewirtschaft-wir-muessen-uns-aus-der-energie-krise-herausmanagen/28750704.html>. Дата звернення: 20.10.2022

Грінченко Володимир Сергійович,
ІПМаш ім. А. М. Підгорного НАН України,
старший науковий співробітник,
vsgrinchenko@gmail.com

Ткаченко Олександр Олегович,
ІПМаш ім. А. М. Підгорного НАН України,
науковий співробітник,
oleksandr.tk7@gmail.com

КЛАСИФІКАЦІЯ СИСТЕМ КОНТУРНОГО ЕКРАНУВАННЯ МАГНІТНОГО ПОЛЯ ПІДЗЕМНИХ КАБЕЛЬНИХ ЛІНІЙ

Анотація. В роботі представлено класифікацію відомих систем контурного екранування, що можуть бути використані для нормалізації магнітного поля кабельних ліній високої напруги. В результаті проведеного огляду наукових публікацій визначено провідні наукові установи, що займаються розробками таких систем: дві установи з Італії та по одній з Іспанії та України. Розроблені ними системи контурного екранування мають свої особливості, проте можуть бути класифіковані за кількістю контурних екранів у системі. Відповідно, виділено такі три типи систем контурного екранування: одноелементні, двоелементні та багатоелементні. Найбільш доцільним визнано застосування одноелементних систем контурного екранування.

Abstract. The paper presents the classification of known passive loop systems used to normalize the magnetic field of high-voltage cable lines. As a result of the review of scientific papers, we identify the leading scientific institutions involved in the design of such systems, namely two institutions from Italy and one each from Spain and Ukraine. The passive loop systems designed by them have unique features, but they can be classified by the number of loops in the system. Accordingly we identify the following three types of passive loop systems: single-element, double-element, and multi-element ones. We find the single-element passive loop systems as the most appropriate.

Підземні кабельні лінії електропередавання (КЛ) є найбільш перспективним засобом передачі електричної енергії в містах, оскільки ширина їхньої охоронної зони на порядок менша за ширину охоронної зони повітряних ліній. Відповідно прокладання траси КЛ не вимагає відчуження значних міських земельних ділянок [1]. Якщо пропускна спроможність КЛ сягає 1000 А, то магнітне поле (МП) безпосередньо над трасою КЛ може в кілька разів перевищувати гранично допустимий рівень 10 мкТл, прийнятий в Україні для зони житлової забудови [2]. Традиційно для нормалізації МП КЛ використовують електромагнітні або магнітні екрани, проте перспективними засобами є системи контурного екранування. Наразі відомо

кілька різновидів таких систем, а метою представленої роботи є їхня класифікація.

Огляд робіт, присвячених методам та засобам екранування МП КЛ, показав, що провідні систем контурного екранування МП КЛ (рис. 1) розроблено в таких установах: *Politecnico di Torino* (Турін, Італія) [3]; Державна установа «Інститут технічних проблем магнетизму НАН України» (Харків, Україна) [1]; *Seville University* (Севілья, Іспанія) [4]; *Prysmian S.p.A.* (Мілан, Італія) [5]. Системи, розроблені в кожній з установ, мають свої особливості та можуть бути класифіковані за низкою ознак: кількість контурних екранів у системі екранування; форма контурних екранів, що використовуються в системі екранування; спосіб підвищення ефективності екранування МП КЛ. Ми пропонуємо проводити класифікацію систем контурного екранування за кількістю контурних екранів та виділяти, відповідно, одноелементні, двоелементні та багатоеlementні системи контурного екранування.

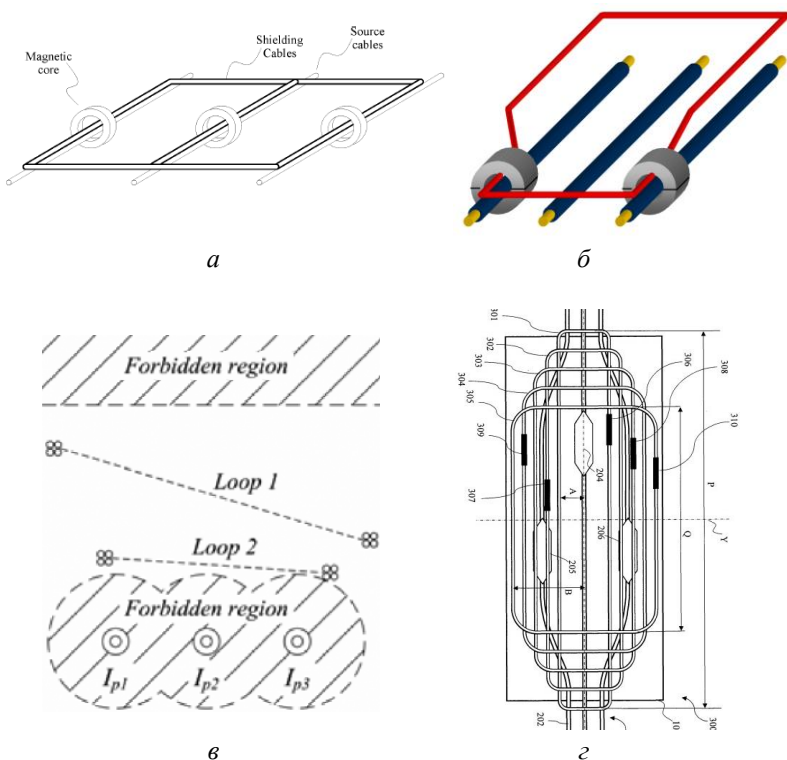


Рисунок 1 – Відомі системи контурного екранування магнітного поля кабельних ліній: а – [3], б – [1], в – [4], з – [5]

До одноелементних відносяться такі системи контурного екранування (рис. 1, а-б): *High Magnetic Coupling Passive Loop* [3] та одноконтурний екран з феромагнітними осердями та несиметричним магнітним зв'язком [1]. Обидві системи використовують феромагнітні осердя, що охоплюють силові кабелі, для підвищення ефективності екранування МП КЛ. Завдяки такому посиленню індуктивного зв'язку між системою екранування та КЛ, ефективність екранування МП КЛ може сягати 10 одиниць та більше.

Відомі двоелементні системи екранування складаються з прямокутних контурних екранів. Найбільша ефективність екранування МП КЛ досягається, коли один контурний екран розташовано поблизу КЛ, інший – між КЛ і поверхнею землі (рис. 1, в). Для підвищення ефективності екранування до контурів під'єднують допоміжні конденсатори. Вирішенню задачі оптимізації параметрів двоелементної системи присвячено [4]. Суттєвим недоліком таких систем є істотна залежність ефективності екранування від ємності допоміжних конденсаторів, причому відносно невелика зміна ємності може спричинити значне зменшення ефективності екранування.

Під багатоелементними ми розуміємо системи екранування, які складаються з більш ніж двох контурних екранів (рис. 1, г). Такі системи можуть містити до 16 контурних екранів та забезпечувати ефективність екранування МП КЛ понад 20 одиниць [5]. Проте це вимагає значного підвищення металоемності системи екранування.

Зважаючи на переваги та недоліки систем кожного з класів, можна стверджувати, що найбільш доцільним є використання одноелементних систем контурного екранування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Rozov V.Y., Grinchenko V.S., Yerisov A.V., Dobrodeyev P.N. Efficient shielding of three-phase cable line magnetic field by passive loop under limited thermal effect on power cables. *Electrical Engineering & Electromechanics*, 2019, no. 6, pp. 50-54.
2. Правила улаштування електроустановок. – Видання офіційне. – Міненерговугілля України. – Х.: Видавництво «Форт», 2017. 760 с.
3. Canova A., Bavastro D., Freschi F., Giaccone L., Repetto M. Magnetic shielding solutions for the junction zone of high voltage underground power lines. *Electric Power Systems Research*, 2012, vol. 89, pp. 109-115.
4. del-Pino-López J.C., Cruz-Romero P. The effectiveness of compensated passive loops for mitigating underground power cable magnetic fields. *IEEE Transactions on Power Delivery*, 2011, vol. 26, no. 2, pp. 674-683.
5. Maioli P., Zaccone E. Passive loops technique for electromagnetic fields mitigation: applications and theoretical considerations. *Jicable International Conference on Insulated Power Cables*, 2007, pp. 231-236.

Зубок Віталій Юрійович,
ІПМЕ ім. Г.Є. Пухова НАН України,
доктор технічних наук, старший дослідник,
vit@visti.net

Давидюк Андрій Вікторович,
ІПМЕ ім. Г.Є. Пухова НАН України,
аспірант,
andrey19941904@gmail.com

КОНЦЕПЦІЇ РІВНІВ ВПРОВАДЖЕННЯ ЗАХОДІВ КІБЕРЗАХИСТУ

Анотація. У дослідженні розглянуті підходи до оцінювання рівня впровадження заходів кіберзахисту та рівня зрілості процесів ІТ. За результатами їх порівняльного аналізу запропоновано застосовування рівнів впровадження заходів кіберзахисту та підхід для їх визначення.

Abstract. Approaches for assess the cybersecurity measures implementation level and the level of the IT processes maturity are considered in the research. According to the results of their comparative analysis, the application of the cybersecurity measures levels implementation and the approach for their determination are proposed.

Вступ. Рішення щодо впровадження заходів кіберзахисту формується на основі аналізу ризиків інформаційної та кібербезпеки. Водночас впровадження будь-яких заходів потребує оцінювання рівня такого впровадження для розуміння залишкових ризиків і потреби в їх обробці. Таким чином можна зробити висновок, що оцінювання впровадження є елементом процесу управління ризиками.

Для процесу оцінювання необхідним є визначення критеріїв оцінювання для предмету оцінювання та шкали оцінювання. З огляду на це термін «рівень впровадження» можемо визначити як інтегральну оцінку властивостей (характеристик) впровадженого заходу у відповідності до критеріїв оцінювання. Звідси під «критеріями оцінювання» будемо розуміти вимоги до властивостей (характеристик) впровадженого заходу.

Виклад основного матеріалу. Водночас можливість впровадження заходів кіберзахисту залежить від наявної ІТ інфраструктури та пов'язаних з нею процесів. Таким чином виникає залежність рівня впровадження заходів кіберзахисту від рівня зрілості ІТ процесів в організації. Така залежність є прямопропорційною, так як більш розвинута ІТ інфраструктура потребує більш складних технологій захисту.

Заходи кіберзахисту АСУ ТП є невід'ємною частиною кіберзахисту. Впровадження заходів кіберзахисту буде неефективним без врахування рівнів зрілості ІТ процесів. Пропонується використання відповідності рівнів впровадження заходів кіберзахисту рівням зрілості ІТ процесів, визначених

Методологією COBIT 5 [1], та рівнів захищеності згідно ISA 62443-1-1 [2], представленої в табл.1.

- 0. Incomplete process (Не існуючий)
- 1. Performed process (Початковий)
- 2. Managed process (Повторюваний але інтуїтивний)
- 3. Established process (Визначений)
- 4. Predictable process (Керований та вимірюваний)
- 5. Optimising process (Оптимізований)

Таблиця 1 – Відповідність рівнів впровадження заходів кіберзахисту рівням зрілості ІТ процесів

Рекомендації/NIST CSF	ISA 62443-1-1 (ISA 62443-3-3 Annex A)	COBIT 5
1.Частковий	0. Не має засобів захисту 1. Захищений від випадкового/ненавмисного порушення безпеки	0. Incomplete process (Не існуючий) 1. Performed process (Початковий)
2.Ризик-орієнтовний	2. Захищений від слабкого навмисного втручання (невеликі ресурси та знання низька мотивація, прості засоби)	2. Managed process (Повторюваний але інтуїтивний)
3.Повторюваний	3. Захищений від наполегливого навмисного втручання (здіяння суттєві ресурси, підключено професіоналів і спеціалізовані засоби, але атакуюча сторона має обмеження в можливостях та/або ресурсах та/або часі)	3. Established process (Визначений)
4.Адаптивний.	4. Захищений від цілеспрямованої наполегливої атаки (коли атакуюча сторона має ресурси на регулярні ворожі дії, постійно вдосконалює механізми атаки, вичікує, шукає нові вразливості).	4. Predictable process (Керований та вимірюваний) 5. Optimising process (Оптимізований)

Особливо актуальним таке співвіднесення є для автоматизованих систем управління технологічними процесами (далі – АСУ ТП) та операційних технологій (далі - ОТ) на об'єктах критичної інфраструктури (далі - OKI).

В Україні постановою Кабінету Міністрів України від 09.10.2020 № 1109 затверджено Методику категоризації об'єктів критичної інфраструктури, яка визначає критерії для віднесення OKI за рівнем неагативного впливу до тієї чи іншої категорії негативного впливу [3]. Рівні негативного впливу автоматизованих систем управління технологічними процесами відповідають рівням негативного впливу на надання основних послуг у разі знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури.

Відповідно до Наказу та NIST Framework for Improving Critical Infrastructure Cybersecurity (далі – NIST CSF) [4] визначено чотири ієрархічних рівні впровадження заходів кіберзахисту:

- 1.Частковий
- 2.Ризик-орієнтовний
- 3.Повторюваний
- 4.Адаптивний.

Основою для визначення рівнів впровадження згідно Наказу є процеси управління ризиками. Необхідний рівень впровадження залежить від рівня ризику для держави, який визначається з урахуванням рівня негативного впливу на надання основних послуг у разі знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури відповідно до Постанови Кабінету Міністрів України «Деякі питання об'єктів критичної інфраструктури» від 09.10.2020 №1109 [3].

Залежність необхідного рівня впровадження заходів кіберзахисту від наявного рівня ризику наведено в табл.2.

Таблиця 2 - залежність необхідного рівня впровадження від наявного рівня ризику

Рекомендації/ NIST CSF	СОВІТ 5	Низький ризик	Середній ризик	Високий ризик
1.Частковий	0. Incomplete process (Не існуючий) 1. Performed process (Початковий)			
2.Ризик-орієнтовний	2. Established process (Визначений)			
3.Повторюваний	3. Established process (Налагоджені)			
4.Адаптивний.	4. Predictable process (Керований та			

	вимірюваний) 5. Optimising process (Оптимізований)			
--	--	--	--	--

Таким чином, більший ризик матиме ОКІ з вищим рівнем можливого негативного впливу у разі порушення його функціонування

Водночас Наказом Адміністрації Держспецзв'язку від 06.10.2021 № 601 «Про затвердження методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури» (далі – Наказ) визначені категорії та підкатегорії заходів кіберзахисту [5].

Враховуючи таку класифікацію заходів кіберзахисту, резюмуємо, що зазначений в Наказі стандартний цільовий профіль кіберзахисту визначає мінімальний необхідний рівень впровадження для кожної підкатегорії заходів кіберзахисту ОТ/АСУ ТП відповідно до рівня небезпеки ОКІ.

Визначається п'ять рівнів впровадження заходів кіберзахисту:

0 - не впроваджено;

1 - впроваджено частково, не системно;

2 - переважно впроваджено, система контролю дотримання відсутня чи недостатня;

3 - переважно впроваджено і контролюється дотримання на поточному рівні;

4 - впроваджено в необхідному обсязі і працюють процедури контролю та актуалізації вимог.

Досягнення рівня впровадження заходів кіберзахисту визначається за повнотою виконання цих заходів з урахуванням поточної практики щодо реалізації заходів кіберзахисту та управління ризиками кібербезпеки на ОКІ, характеристики загроз кібербезпеки, законодавчі та нормативні вимоги, комерційні та стратегічні цілі ОКІ, вимоги до кібербезпеки в ланцюзі поставок програмного/апаратного забезпечення, організаційні та інші обмеження.

Враховуючи вищезазначене, пропонується застосовувати наступні рівні впровадження заходів кіберзахисту:

0 - підкатегорію заходів кіберзахисту не імплементовано;

1 - імплементовано частково, несистемно;

2 - переважно імплементовано, система контролю дотримання відсутня чи недостатня;

3 - переважно імплементовано, контролюється дотримання на поточному рівні;

4 - імплементовано в необхідному обсязі і працюють процедури контролю та актуалізації вимог

Стандартний цільовий профіль впровадження по категорії заходів кіберзахисту для кожної категорії заходів розраховується наступним чином:

$$CI_{кат} = \frac{\sum V_{субкат}}{N_{кат}},$$

де

$CI_{кат}$ - мінімальний середній рівень впровадження заходів;

$V_{субкат}$ - рівень впровадження заходів підкатегорії заходів, яка належить до категорії;

$N_{кат}$ - кількість підкатегорій заходів, що належать до категорії.

Оцінюванні рівня ризику для АСУ ТП ОКІ здійснюється за стандартом ДСТУ ISO/IEC 27005, що є методичною основою для оцінювання ризиків на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури відповідно до Постанови Кабінету Міністрів України «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» від 19.06.2019 № 518 [6].

Після визначення рівня ризику для ОКІ, визначається рівень впровадження комплексу заходів кіберзахисту (цільового профілю).

Використовується шкала оцінювання відповідно до рекомендацій стандарту ДСТУ ISO/IEC 33004:2016 «Інформаційні технології. Оцінювання процесу. Вимоги до еталонної моделі процесу, моделі оцінювання процесу та моделі зрілості (ISO/IEC 33004:2015, IDT)» [7]:

«Повністю впроваджено»: рівень можливостей досягається понад 85 відсотків.

«Переважно впроваджено»: рівень можливостей досягається між 50 і 85 відсотками.

«Частково впроваджено»: рівень можливостей досягається між 15 і 50 відсотками.

«Не впроваджено»: рівень можливостей досягнуто менше ніж на 15 відсотків.

Рівень впровадження визначається на основі повноти базових атрибутів процесів:

- обізнаність і комунікація;
- політики, плани і процедури;
- інструменти та автоматизація;
- навички и знання;
- відповідальність і підзвітність;
- постановка цілей і вимірювання.

Базові атрибути повинні бути оцінені враховуючи цілі організації та результати процесів.

Базові атрибути визначаються для кожного заходу кіберзахисту відповідно до вимог законодавства, стандартів безпеки та політик організації.

Висновки. Розглянуто концепції рівнів впровадження заходів кібербезпеки, запропоновано застосовування рівнів впровадження заходів кіберзахисту та підхід для їх визначення:

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. COBIT 5 A business Framework for the Governance and Management of Enterprise IT.

2. IEC/TS 62443-1-1 Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models. Welcome to the IEC Webstore. URL: https://webstore.iec.ch/preview/info_iec62443-1-1%7Bed1.0%7Den.pdf (дата звернення: 11.11.2022).

3. Постанова Кабінету Міністрів України «Деякі питання об'єктів критичної інфраструктури» від 09.10.2020 № 1109

4. Cybersecurity Framework. NIST. URL: <https://www.nist.gov/cyberframework> (дата звернення: 11.11.2022).

5. Наказ Адміністрації Держспецзв'язку від 06 жовтня 2021 року № 601 Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури. <https://cip.gov.ua/>. URL: <https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-06-zhovtnya-2021-roku-601-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-pidvishennya-rivnya-kiberzakhistu-kritichnoyi-informacii-noyi-infrastrukturi> (дата звернення: 11.11.2022).

6. Постанова Кабінету Міністрів України «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» від 19.06.2019 № 518

7. ДСТУ ISO/IEC 33004:2016 «Інформаційні технології. Оцінювання процесу. Вимоги до еталонної моделі процесу, моделі оцінювання процесу та моделі зрілості (ISO/IEC 33004:2015, IDT)»

Мохор Володимир Володимирович,

ІПМЕ ім. Г.Є. Пухова НАН України,

член.-кореспондент НАН України, доктор технічних наук, професор,
v.mokhor@gmail.com

Зубок Віталій Юрійович,

ІПМЕ ім. Г.Є. Пухова НАН України,

доктор технічних наук, старший дослідник,
vitaly.zubok@gmail.com

Бакалинський Олександр Олегович,

ІПМЕ ім. Г.Є. Пухова НАН України,

кандидат технічних наук, старший дослідник,
baov@meta.ua

Дубинський Георгій Петрович,

Міністерство цифрової трансформації України,
pr@thedigital.gov.ua

Пазюк Андрій Валерійович

Навчально-науковий інститут міжнародних відносин КНУ імені Тараса Шевченка, доктор юридичних наук,
inet.media.law@gmail.com

ТОПОЛОГІЧНИЙ ПІДХІД ДО ОЦІНЮВАННЯ ТА ПІДВИЩЕННЯ ЦИФРОВОЇ РЕЗИЛЬЄНТНОСТІ

Анотація. Цифрова трансформація відбувається завдяки розвитку інформаційно-комунікаційних систем. Цифрова стійкість, або цифрова резильєнтність — здатність ефективно протистояти викликам будь-якого походження і характеру, адаптуватися до змін середовища, підтримувати стає функціонування, та відновлюватися на основі використання, застосування та розвитку цифрових технологій. Для аналізу цифрової резильєнтності пропонується розглянути цифрових суб'єктів, цифрові потреби, цифрові засоби і їхні залежності у вигляді топологічного простору, утвореного із структурованих підмножин зазначених елементів.

Abstract. Digital transformation happens through the development of information and communication systems. Digital resilience means the ability to effectively face challenges of any nature, adapt to environmental changes, maintain sustainable functioning, and recover based on the use, application and development of digital technologies. To analyze digital resilience, it is proposed to

consider digital individuals, digital needs, digital tools and their dependencies as a topological space formed from structured subsets of the specified elements.

Вступ. Цифрова трансформація - характерна риса цифрового суспільства, економіка якого базується на інформаційних технологіях і яке соціально трансформується з метою допомогти індивідам та спільнотам використовувати знання та ідеї, що допомагає людям втілити їх потенціал та реалізувати їх прагнення [1]. Семантичне поле цифрової трансформації включає в себе такі поняття, як цифрова економіка, цифрові навички, цифрові права, електронне урядування, цифрові інновації і багато іншого. Цифрова складова буття набуває значної цінності і стає об'єктом атаки. Здатність суб'єкта протистояти прямому чи опосередкованому негативному впливу на цифрову складову його буття відома як «цифрова стійкість».

Основний матеріал. Цифрова стійкість, або *цифрова резильєнтність* (digital resilience) — здатність/властивість держави, суспільства, підприємств, установ і організацій, спільнот і громадян ефективно протистояти викликам будь-якого походження і характеру, адаптуватися до змін середовища, підтримувати стале функціонування, швидко відновлюватися до бажаної рівноваги та еволюціонувати після кризових ситуацій на основі використання, застосування та розвитку цифрових технологій. Розвинення цифрової стійкості є важливим чинником і загальнонаціональної стійкості [2].

Цифрова трансформація відбувається завдяки розвитку *інформаційно-комунікаційних систем* (ІКС). Для функціонування звичайного бізнесу, наприклад мережі роздрібних магазинів, можуть бути задіяні місцеві ІКС кожного магазину, ІКС головного офісу, не менше одного ІКС оператора центру обробки даних (ЦОД), та ще кілька ІКС операторів електронних комунікацій. З ІКС нерозривно пов'язані усі види електронних комунікацій, засобів масової інформації, державні інформаційні послуги населенню. Важливо усвідомлювати також значення ІКС в спілкуванні та можливості бути на зв'язку. В цьому плані можна говорити про відкриту множину кібер-соціальних систем, функціонування яких забезпечує певну стійкість суспільства. Доступ до цифрових послуг користувач отримує у переважній більшості систем через Інтернет-доступ. Достатня зв'язність та пропускну спроможність глобальної мережі є найважливішим фактором стійкості ІКС, а отже – цифрової стійкості.

Для дослідження цифрової стійкості надзвичайно цінним є досвід України – держави, яка була серед лідерів цифрової трансформації до широкомасштабної війни з Росією. Безпрецедентні ракетні атаки на головні об'єкти електроенергетики призводять до масових аварійних відключень електроенергії, які контролюються величезними зусиллями операторів мережі. Бізнеси, оператори комунікацій та звичайне населення роблять спроби адаптуватися до рівня надання електроенергії, що безперервно знижується.

Наразі Україна готується до вимушеного переходу: замість планових відключень електроенергії на кілька годин на добу вводиться планові відключення на кілька годин на добу. Надалі очікуються багатоденні відключення. Кожен бізнес та кожне домогосподарство повинні постійно переглядати свої можливості виживання, що безпосередньо підводить нас до поняття резильєнтності. Наука має зробити свій внесок шляхом збору, аналізу, систематизації наявного досвіду (особливо секторального) задля зменшення у майбутньому кількості спроб і помилок при створенні резильєнтних ІКС в умовах обмежень та невизначеностей.

Для досягнення цієї мети необхідно вирішити наступні завдання:

1) дослідити найбільш чутливі інформаційні потреби цифрових суб'єктів;

2) провести аналіз кіберзагроз, які несуть із собою широкомасштабні несприятливі події і як вони впливають на найважливіші цифрові потреби;

3) провести аналіз архітектур мережі, типів комунікацій, топологій, та визначити які комбінації можуть підвищити стійкість ІКС, задіяних у наданні найбільш чутливих інформаційних потреб населення та бізнесу.

В результаті проведення аналізу будуть отримані множини цифрових суб'єктів – DS , цифрових потреб – DN , та цифрових засобів – DT (рис.1). Ці три множини утворюватимуть різноманітні кортежі з трьох елементів, $(ds \in DS, dn \in DN, dt \in DT)$, а також з двох елементів на основі наявних та доступних сполучень:

цифрового суб'єкта та його цифрових потреб

$(ds \in DS, (dn_1, dn_2, \dots, dn_{k-1}, dn_k) \in DN)$;

цифрового суб'єкта та доступних йому цифрових засобів

$(ds \in DS, (dt_1, dt_2, \dots, dt_{k-1}, dt_k) \in DT)$;

цифрових потреб та прийнятних засобів для їх задоволення

$(dn \in DN, (dt_1, dt_2, \dots, dt_{k-1}, dt_k) \in DT)$;

цифрових засобів та суб'єктів, які ними користуються

$(dn \in DN, (dt_1, dt_2, \dots, dt_{k-1}, dt_k) \in DT)$, і цей перелік не є вичерпним.

Нехай існує множина $\mathcal{D}$, така що $\forall ds \in \mathcal{D}, \forall dn \in \mathcal{D}, \forall dt \in \mathcal{D}$. Нехай існує система елементів цієї множини $\mathcal{T}$, до якої належать всі можливі комбінації цих елементів, об'єднання та перетини цих множин:

$\exists \mathcal{T}: \emptyset, \mathcal{D} \in \mathcal{T}; \forall \mathcal{D}', \mathcal{D}'' \in \mathcal{T}: \mathcal{D}' \cup \mathcal{D}'' \in \mathcal{T}; \mathcal{D}' \cap \mathcal{D}'' \in \mathcal{T}$.

Тоді $\mathcal{T}$ відповідає визначенню топології на множині $\mathcal{D}$, а пара $(\mathcal{D}, \mathcal{T})$ відповідає визначенню *топологічного простору*. Окремі елементи топології – мережеві структури [3], що можуть бути досліджені з використанням теорії графів, теорії складних мереж, теорії топологічних просторів для розроблення моделей і методів дослідження і підвищення цифрової резильєнтності.

Висновки. Представлення окремих компонентів цифрового світу у вигляді топологічного простору відкриває шлях до вивчення проблеми цифрової резильєнтності через дослідження групових властивостей, характеристик, динаміки великої кількості мережевих структур.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Okinawa Charter on Global Information Society [Електронний ресурс].
Доступно: <https://www.mofa.go.jp/policy/economy/summit/2000/documents/charter.html>. – Дата доступу: 11.11.2022
2. Резнікова О.О. Національна стійкість в умовах мінливого безпекового середовища : монографія. – Київ : НІСД, 2022. – 532 с. (дата звернення: 11.11.2022).
3. Зубок, В.Ю. Кібербезпека топології INTERNET : монографія / В. Ю. Зубок, В. В. Мохор. — Київ : ІПМЕ ім. Г.Є.Пухова, 2022. — 191 с. – ISBN 978-966-02-9929-0. – DOI:10.5281/zenodo.6795229

Потенко Олександр Сергійович,
ІПМЕ ім. Г.Є. Пухова НАН України,
науковий співробітник,
potenko@ipme.kiev.ua

Суліма Олександр Андрійович,
ІПМЕ ім. Г.Є. Пухова НАН України,
старший науковий співробітник,
rfitfo@gmail.com

АНАЛІЗ ДИНАМІКИ НАДХОДЖЕНЬ ПОПЕРЕДЖЕНЬ ВІД CSIRT ДЛЯ ЗАБЕЗПЕЧЕННЯ СТАБІЛЬНОСТІ КГ ГРІД САЙТУ

Анотація. Проведений аналіз загроз в таких розподілених комп'ютерних мережах як Ukrainian National Grid та European Grid Infrastructure.

Abstract. Conducting analysis of threats in such separate computer networks as Ukrainian National Grid and European Grid Infrastructure.

Грід -сайт Інституту проблем моделювання в енергетиці ім.Г.Є. Пухова був створений в рамках програми Державної цільової науково-технічної програми впровадження і застосування грід-технологій в 2007р. Грід-сайт був орієнтований на виконання задач навчання, підготовки та тестування грід задач перед їх виконанням в загальному грід середовищі. Він являється невід'ємною частиною українського національного грід середовища (UNG). Незважаючи на невисоку продуктивність, завдяки хорошему адмініструванню, грід-сайт мав високий коефіцієнт готовності 0.94-0.98. Завдяки чому на базі сайту було реалізовано 16 наукових проєктів, наприклад “Підтримка та розвиток грід-сайту Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАНУ та створення системи централізованого програмування реконфігурованих прискорювачів задач інформаційної безпеки в енергетичній галузі” . Одним з критичних аспектів являлись підвищені вимоги до безпеки грід-сайту. З одного боку, це викликано високою небезпекою порушення стабільності роботи сайту через помилки учнів. З іншого боку, великий потік нових користувачів збільшував ймовірність навмисних або випадкових пошкоджень за рахунок наявності стандартних вразливостей. Цей факт призвів до відпрацювання методології підтримки та швидкого відновлення працездатності грід вузла у рамках першої проблеми і необхідності моніторингу вразливостей, що знову відкриваються, по другій. У 2012 грід-вузол ІПМЕ ім. Г.Є. Пухова НАН

України був зареєстрований та сертифікований в європейському глід-співтоваристві European Grid Infrastructure (EGI). Після асоціації ГРІД вузла інституту в EGI стала доступна система попередження від Computer Security Incident Response Team (CSIRT).

Існує велика кількість баз даних, що містять опис вразливостей, нас цікавлять вразливості:

- CentOS,
- GRID NORDU,
- мережевих протоколів - обчислювального (Infiniband) і службового (Gigabit Ethernet) рівнів.

Найбільш поширеною є база даних загальновідомих уразливостей інформаційної безпеки CVE. Структура записи о вразливостях складається з наступних розділів: CVE ID, Reference, Description. CVE ID починається з префіксу CVE-і записується із зазначенням року, в якому було повідомлено про вразливість та номер, присвоєний CNA (CVE Numbering Authorities). Підтримкою CVE займається організація MITRE. MITRE Corporation – американська некомерційна організація, що спеціалізується у галузі системної інженерії. Організація підтримує проекти у різних галузях, таких як космічна безпека, інформатика у охороні здоров'я, кібербезпека та інших.

Національним інститутом стандартів і технологій США - National Institute of Standards and Technology (NIST) підтримується національна база даних вразливостей (National Vulnerability Database, NVD) яка є загальнодоступним сховищем даних про вразливості. Функціонування NVD опирається на роботу компанії MITRE та інших організацій. База даних NVD аналізує каталог відомих загроз безпеці CVE і кожній уразливості надає оцінку за загальною системою оцінки вразливостей - Common Vulnerability Scoring System (CVSS). CVSS є відкритим стандартом для оцінки вразливості. Згідно з CVSS, на основі набору показників та формул обчислюється оцінка небезпеки вразливості, яка може мати значення від 0 до 10.

Динаміка надходжень попереджень від CSIRT показана на рис. 1.

Статистика за 2022 рік поки не повна, 2021 рік в зв'язку з низкою причин не є характерним тому не розглядається. Критичні попередження вимагають негайного реагування команди підтримки глід сайту та інколи потребують зупинки роботи сайту. Що суттєво зніжує коефіцієнт готовності. Для його стабілізації необхідно резервувати робочий час команди підтримки глід сайту. При наявності відповідного резерву вдається забезпечити вчасне реагування та стабільний коефіцієнт готовності. Для щомісячного планування корисні графіки помісячного надходження попереджень від CSIRT які наведені на рис. 2.

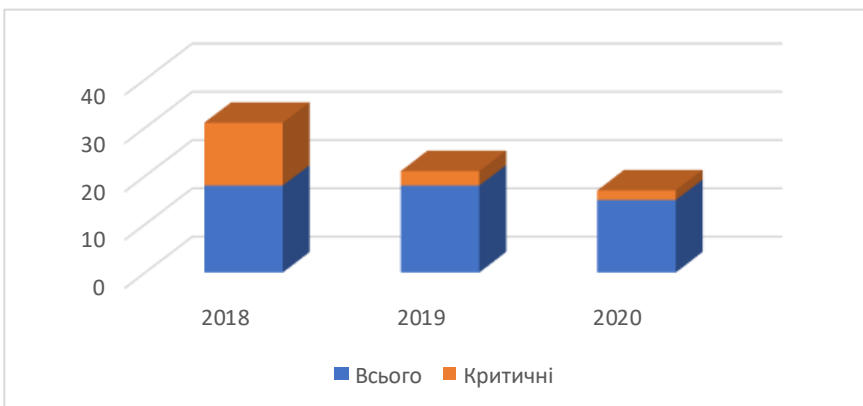


Рис. 1. Динаміка надходжень попереджень від CSIRT

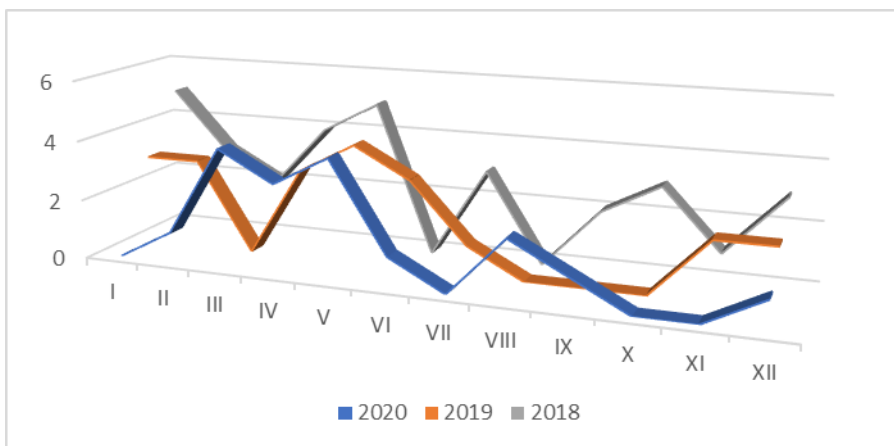


Рис. 2. Динаміка надходжень попереджень від CSIRT на протязі року

Аналіз графіку показує необхідність щомісячного резерву на відпрацювання трьох повідомлень, що при 24 денному навантаженні може складати до 25 відсотків робочого часу.

Висновки: Аналіз динаміки надходжень попереджень від CSIRT на протязі року показує необхідність 25 відсотків робочого часу команді підтримки грид сайту для забезпечення стабільності коефіцієнта готовності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Давиденко А.Н., Гильгурт С.Я., Анализ вопросов регистрации и сертификации вычислительных ресурсов в грид-инфраструктуре, Київ, Зб. наук. пр. ІПМЕ НАН України. – Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ ім. Г.Є. Пухова НАН України. – Київ, 2014. – Вип. 72. – С. 95-104.
2. Євдокимов В.Ф., А.М. Давиденко, С.Я. Гільгурт, Створення на базі грид-сайту іпме ім. г.є. пухова нану системи централізованого синтезу апаратних прискорювачів для вирішення задач інформаційної безпеки в енергетичній галузі, Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ ім. Г.Є. Пухова НАН України. – Київ, 2017. – Вип. 79. – С. 3-8.

ЗМІСТ

Dubovkina I., Myronchuk A. ENERGY SAVING TECHNOLOGY of HYDRODYNAMIC TREATMENT OF NUTRIENT SOLUTIONS.....	6
Ковальчук Л.В., Кучинська Н.В. ПЕРСПЕКТИВИ ВИКОРИСТАННЯ СМАРТ-КОНТРАКТІВ В ЕНЕРГЕТИЦІ ТА НАЯВНІ ВРАЗЛИВОСТІ, ЯКІ ПОТРІБНО ВРАХУВАТИ ДЛЯ МОЖЛИВОСТІ ЇХ ВИКОРИСТАННЯ.....	9
Сушко С.В., Чемерис О.А. АСПЕКТИ ВПЛИВУ ОПТИМІЗАЦІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА ЕНЕРГОСПОЖИВАННЯ ОБЧИСЛЮВАЛЬНИХ СИСТЕМ.....	19
Артемчук В.О., Каменева І.П., Попов О.О., Яцишин А.В., Кириленко Ю.О. ЗАСОБИ АНАЛІЗУ ДАНИХ В ЗАДАЧАХ ПІДТРИМКИ УПРАВЛІНСЬКИХ РІШЕНЬ В ГАЛУЗІ ЕКОЛОГІЧНОЇ БЕЗПЕКИ.....	22
Артемчук В.О. ПЕРСПЕКТИВИ РОЗРОБЛЕННЯ МЕТОДІВ І ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ РЕЗИЛЬЄНТНОСТІ ОБ'ЄКТІВ ЕНЕРГЕТИЧНОЇ ГАЛУЗІ УКРАЇНИ.....	30
Худинцев М.М. ЗАСТОСУВАННЯ ІНДЕКСІВ КІБЕРБЕЗПЕКИ ДЛЯ ОЦІНКИ СТАНУ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ.....	32
Чемерис О.А., Резнікова С.О. Р2Р РИНОК ЕЛЕКТРОЕНЕРГІЇ ДЛЯ МІКРОМЕРЕЖ.....	37
Чемерис О.А., Клименко Т.М. ПРОГРАМНІ ЗАСОБИ ДЛЯ ВИРІШЕННЯ МІР ЗАДАЧ.....	39
Борукаєв З.Х., Остапченко К.Б., Євдокімов В.А. ОСОБЛИВОСТІ ПОБУДОВИ МОДЕЛІ КОРОТКОСТРОКОВОГО ПРОГНОЗУВАННЯ ЕЛЕКТРОСПОЖИВАННЯ ПОСТАЧАЛЬНИКАМИ НА ОПТОВОМУ РИНКУ ЕЛЕКТРОЕНЕРГІЇ.....	41
Владимирський О.А., Владимирський І.А. ЗАСТОСУВАННЯ КОРРЕЛЯЦІЙНИХ ПАРАМЕТРИЧНИХ МЕТОДІВ ПОШУКУ ВИТОКІВ ДЛЯ ПЕРІОДИЧНОГО МОНІТОРИНГУ ПІДЗЕМНИХ ТРУБОПРОВІДІВ СИСТЕМ ТЕХНІЧНОЇ ВОДИ ВІДПОВІДАЛЬНИХ СПОЖИВАЧІВ АЕС.....	47

Цуркан О.В., Герасимов Р.П., Клименко Т.М., Яшенков В.П., Коженевський С.Р. ФРЕЙМВОРК КІБЕРСОЦІАЛЬНОЇ ІНЖЕНЕРІЇ НА ОСНОВІ МОДЕЛІ KILL CHAIN.....	49
Мохор В.В., Бакалинський О.О., Дорогий Я.Ю., Цуркан В.В. ТЕНДЕНЦІЇ РОЗВИТКУ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ СФЕРИ ЕНЕРГЕТИКИ.	51
Гільгурт С.Я., Кіслов О.Г., Попова В.М. ВИКОРИСТАННЯ ТРІЙКОВОЇ АСОЦІАТИВНОЇ ПАМ'ЯТІ НА РЕКОНФІГУРОВАНИЙ ПЛАТФОРМІ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ.....	52
Коломієць Є.А. КОМП'ЮТЕРНІ ЗАСОБИ ОЦІНКИ БЕЗПЕКИ ЕКСПЛУАТАЦІЇ ЕНЕРГЕТИЧНИХ ПАЛИВНИХ СИСТЕМ ТРАНСПОРТНИХ ЛІТАКІВ...	54
Костенко Г.П., Згуровець О.В. ПЕРСПЕКТИВИ РЕГУЛЮВАННЯ ЕЛЕКТРИЧНОГО НАВАНТАЖЕННЯ В ЕНЕРГОСИСТЕМІ ЗА ДОПОМОГОЮ ЕЛЕКТРОМОБІЛІВ.....	57
Криворучко І.П. КУСКОВО-ЛІНІЙНА АПРОКСИМАЦІЯ ГЛАДКИХ, ПЛОСКИХ КРИВИХ МЕТОДОМ СІЧНИХ.....	60
Левкін Д.А., Макаров О.А. ЗАСТОСУВАННЯ МАТЕМАТИЧНИХ МЕТОДІВ ДЛЯ КОНТРОЛІНГУ ЕНЕРГЕТИЧНИХ ВИТРАТ В ТЕХНОЛОГІЧНИХ ПРОЦЕСАХ.....	64
Лепатьєв А.О. ТРИ ЦИКЛИ ПО МАСИВУ КОМПОНЕНТІВ МНЕМОСХЕМИ У АВТОМАТИЧНІЙ ПІДГОТОВЦІ ДАНИХ ДЛЯ РОЗРАХУНКУ РЕЖИМУ...	66
Митько Л.О. АНАЛІЗ ПРОПОЗИЦІЙ ЄВРОПЕЙСЬКИХ НАУКОВЦІВ ДЛЯ ЕНЕРГЕТИЧНОЇ ГАЛУЗІ З МЕТОЮ ЇХ АДАПТАЦІЇ В УКРАЇНІ, ВИКОРИСТОВУЮЧИ ЦИФРОВІЗАЦІЮ.....	70
Грінченко В.С., Ткаченко О.О. КЛАСИФІКАЦІЯ СИСТЕМ КОНТУРНОГО ЕКРАНУВАННЯ МАГНІТНОГО ПОЛЯ ПІДЗЕМНИХ КАБЕЛЬНИХ ЛІНІЙ.....	73
Зубок В.Ю., Давидюк А.В. КОНЦЕПЦІЇ РІВНІВ ВПРОВАДЖЕННЯ ЗАХОДІВ КІБЕРЗАХИСТУ.....	76

Мохор В.В., Зубок В.Ю., Дубинський Г.П., Бакалинський О.О., Пазюк А.В. ТОПОЛОГІЧНИЙ ПІДХІД ДО ОЦІНЮВАННЯ ТА ПІДВИЩЕННЯ ЦИФРОВОЇ РЕЗИЛЬЄНТНОСТІ.....	82
Потенко О.С., Суліма О.А. АНАЛІЗ ДИНАМІКИ НАДХОДЖЕНЬ ПОПЕРЕДЖЕНЬ ВІД CSIRT ДЛЯ ЗАБЕЗПЕЧЕННЯ СТАБІЛЬНОСТІ КГ ГРІД САЙТУ.....	86

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

24 листопада 2022 року
м. Київ

Формат 60×90/16. Тираж 100.
Підписано до друку 28.10.2022. Заказ № 11

Інститут проблем моделювання в енергетиці
ім. Г.Є. Пухова Національної академії наук України,
Україна, 03164, Київ, вул. Генерала Наумова, 15,
тел.: +38 044 424 10 63
<https://ipme.kiev.ua/>, ipme@ipme.kiev.ua