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

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

ПРИСВЯЧЕНА ДНЮ НАУКИ ТА РОКУ МАТЕМАТИКИ В УКРАЇНІ

Збірник тез конференції
15 травня 2020 р.

Київ – 2020

УДК 621.3 + 004 + 519.6 : 620.9

Рекомендовано до друку Вченою радою
Інституту проблем моделювання в енергетиці
ім. Г.Є. Пухова НАН України
(протокол №7 від 14 травня 2020 р.)

Відповідальні за випуск:
В.О. Артемчук, С.Ф. Гончар

Зб. тез XXXVIII науково-технічної конференції молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, м. Київ, 15 травня 2020 р. / ІПМЕ ім. Г.Є. Пухова НАН України. – 2020. – 147 с.

ЗМІСТ

V. Khaidurov

A MATHEMATICAL MODEL FOR DETERMINING THE VELOCITY OF SOUND WAVES PROPAGATION IN SOLIDS

To solve the applied problems of the control of the state of materials, ultrasonic analysis is widely used, by which defects of a material are determined, the material itself is determined by the characteristics of propagation and attenuation of sound waves and the like. During the examination of bodies by ultrasound, it is considered that the elastic deformation occurring in these bodies is insignificant compared to the size of the objects and systems under study [1]. The mathematical basis for the study of such processes is the wave equation of second order mathematical physics.

The equation in the field is considered $\Omega \subset \mathbb{R}^n$:

$$\frac{\partial^2 U(\bar{x},t)}{\partial t^2} = c^2 \sum_{i=1}^{n} \frac{\partial^2 U(\bar{x},t)}{\partial x_i^2} + f(\bar{x},t) \ on \ \Omega, \tag{1}$$

where

$\bar{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n, t \in [0, T_{fin}]$,

$x_i \in [a_i, b_i]$, $a_i \in \mathbb{R}$, $b_i \in \mathbb{R}$, $G = [a_1, b_1] \times [a_2, b_2] \times \ldots \times [a_n, b_n]$, $i = \overline{1,n}$.

Basic designations: x_i – spatial coordinate, n – the dimension of space, $\bar{x}$ – vector coordinates, t – time; U – the desired model solution, c – the speed of sound propagation in the environment, T_{fin} – the final time.

The initial conditions in (1) are as follows:

$$U(\bar{x},0) = g_1(\bar{x}), U_t(\bar{x},0) = g_2(\bar{x}). \tag{2}$$

The boundary conditions for (1)–(2) are set depending on the formulation of the problem corresponding to a particular physical process.

As an example of a wave propagation model that is performed by a point source, we consider the direct model described by the equation:

$$\partial^2 U / \partial t^2 = \partial^2 U / \partial x^2 + \partial^2 U / \partial y^2; (x, y) \in [0;1]^2; t \in [0;2]. \tag{3}$$

The initial conditions have the form:

$$U(x, y, 0) = U_t(x, y, 0) = 0. \tag{4}$$

Boundary conditions have the form:

$$\partial U / \partial \bar{n}\big|_{\Gamma} = 0, t > 0. \tag{5}$$

The internal condition has the form:

$$U(0,5;0,5;t) = 30^{-1} \sin 18\pi t, \ 0 < t < 0,2. \tag{6}$$

Internal condition (6) defines the harmonic oscillations that are made by a point source directly inside the object under study.

Figure 1 shows the solutions of the mathematical model (3)–(6).

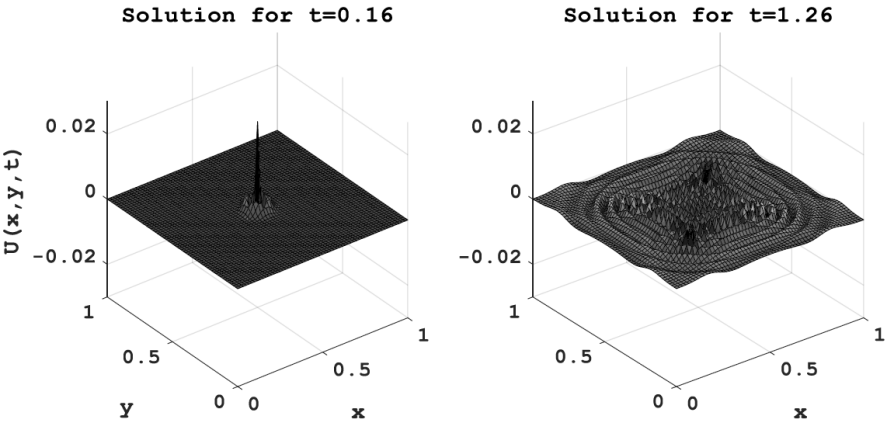


Figure 1 – Numerical solution of mathematical model (3)–(6) at different points in time

A mathematical model for determining sound wave propagation parameters in solids is an inverse model in which we need to find the global minimum of a quadratic function:

$$F(c)=\frac{1}{n}\sum_{i=1}^{n}\int_{\tau_i^{beg}}^{\tau_i^{end}}\left(s_i(c,t)-s_i^{experimental}(t)\right)^2 dt\to\min, \tag{7}$$

where c – the speed of propagation of sound waves in the medium, $s_i(c,t)=U\left(x_i^{sensor},y_i^{sensor},t\right)$; $0\le\tau_i^{beg}<\tau_i^{end}\le T, i=\overline{1,n}$, and the limitation to (7) is the wave equation, which describes the process of propagation of sound waves:

$$\partial^2U/\partial t^2=c^2\Delta U \; on\,\Omega,\; t\in[0;T]; \tag{8}$$

where $\Omega=(x,y)\in[a;b]\times[c;d], a,b,c,d\in\mathbb{R}$.

The initial conditions have the form:

$$U(x,y,0)=U_t(x,y,0)=0. \tag{9}$$

Boundary conditions have the form:

$$\partial U/\partial\bar{\boldsymbol{n}}\big|_{\Gamma}=0, t\in[0;T]. \tag{10}$$

The internal condition has the form:

$$U\left(x^{source},y^{source},t\right)=A\sin 2\pi ft. \tag{11}$$

Based on the model designation (7)–(11). n – total number of sensors, τ_i^{beg} – time of observation on the i-th sensor; τ_i^{beg} і τ_i^{beg} – the start and end time of the

observation on the i-th sensor, respectively, $s_i^{experimental}(t)$ – data of the i-th sensor in time $\left[\tau_i^{beg};\tau_i^{end}\right]$, T – total experiment time, Ω – calculation area, A, f – amplitude and frequency, $\left(x_i^{sensor}, y_i^{sensor}\right)$ – position of the i-th sensor, $\left(x^{source}, y^{source}\right)$ – source position. Figure 2 – inputs data of model (7)–(11).

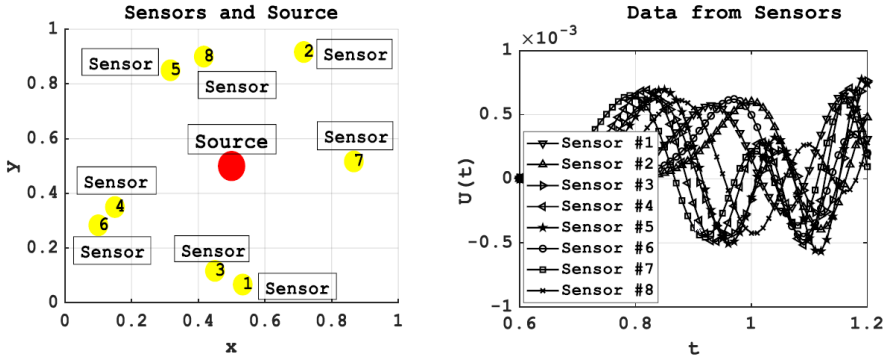


Figure 2 – Inputs for model (7)–(11): on the left – the position of the sensors in the object under study; on the right – the data received by the sensors

Table 1 contains the numerical results of the computational experiments of model (7)–(11) with the classical genetic algorithm. The number of bits to encode is 32, the total number of iterations of the genetic algorithm is 100. The velocity found for wave propagation is 1,0000193932, the real value is 1.

Table 1

Convergence (7) of model (7)–(11) with the classical genetic algorithm

Iteration	Value of (7)	Iteration	Value of (7)
1	4,05116296E-05	70	1,78558303E-13
5	2,43795886E-05	75	1,04036629E-13
10	1,39653308E-05	80	6,67451567E-14
15	7,86654197E-06	85	3,71148666E-14
20	4,37072926E-06	90	2,18322134E-14
25	2,78290865E-06	100	1,21550930E-14

Wave processes in any investigated objects have the property of attenuation, it is advisable instead of (1) to use:

$$\frac{\partial^2 U(\bar{x},t)}{\partial t^2} = c^2 \sum_{i=1}^{n} \frac{\partial^2 U(\bar{x},t)}{\partial x_i^2} + \gamma \sum_{i=1}^{n} \frac{\partial U(\bar{x},t)}{\partial x_i} + f(\bar{x},t), \qquad (12)$$

where γ – wave attenuation factor. In this case, in model (7)–(11), function (7) will depend on two variables c and γ.

[1] Yerofeyev V.A., Miller S.S. Ul'trazvukovoy monitoring mikrodefektov v metalle. Zhurnal “Izvestiya Tul'skogo gosudarstvennogo universiteta”, mashinostroyeniye i mashinovedeniye. 2014. S. 211–217.

К.Е. Дьомічев, О.Д. Петров

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ПСЕВДО-ПРУЖНЬО-ПЛАСТИЧНИХ ТІЛ З УРАХУВАННЯМ НЕЛІНІЙНОСТІ

В умовах сучасного науково-технічного прогресу в різних галузях науки та техніки знаходить застосування все більша кількість нових матеріалів.

Зростання виробництва застосування псевдо-пружно-пластичних матеріалів або матеріалів з пам’яттю форм та їх широке застосування, зумовлюють потребу створення нових математичних та комп’ютерних моделей і методів розрахунку з огляду на реально технологічні навантаження та властивості матеріалу.

Псевдо-пружно-пластичність - це здатність матеріалу при активному навантаженні накопичувати деформації певного значення в режимі більш високої температури, а потім після розвантаження (через петлю гістерезису) повертатися до початкового стану. Основним механізмом є зворотна мартенситна трансформація між фазами твердого тіла, яка може відбуватися при кімнатній температурі. Така трансформація може бути викликана зміною температури або за допомогою силових факторів. Матеріал також характеризується нелінійною механічною поведінкою, та великими деформаціями. Сплавами, які демонструють пам'ять форми та псевдо-пружно-пластичність, є такі: NiTiAuCd, CuAlNi, CuSn, CuZn, NiFeGa, NiTiNb, NiNiGa, NiFeGa, NiPi, NiPeGa, NiPiGi [1]. Такі характеристики роблять сплави з пам’яттю форм придатними для використання в різних пристроях або як складові частини в деяких передових композиційних матеріалах. Сплав NiTi лідирує в більшості таких застосувань завдяки своїм структурним властивостям.

За результатами аналізу встановлено, що в даний час існує цілий ряд моделей для опису термомеханічного поведінки сплавів з пам’яттю форми, псевдо-пружністю та псевдо-пружно-пластичністю. Більшість з них будуються на підставі класичних уявлень, тобто ставлять собі за мету безпосереднє описати експериментальні дані, отримані на різних зразках при простому і складному навантаженні. Однак, як встановлено в експериментальних дослідженнях поведінка матеріалу в точці тіла в загальному випадку відрізняється від поведінки зразка в цілому і при цьому можуть мати місце значні деформації.

Одним із аспектів числового розв’язання загальних нестаціонарних задач для не пружних тіл є вибір фізичних співвідношень між напруженням та деформацією. Цей вибір узгоджується з експериментами і тісно пов'язаний з процесами деформування, що відбуваються в матеріалі тіла. У загальному випадку величини деформації - це функції процесу напружень та перепадів температур, які визначаються характеристиками всього попереднього процесу змін фізичних факторів, а не лише поточними значеннями [2].

При побудові фізичних співвідношень передбачалося, що деформація в точці представлена як сума пружної складової, стрибка деформації при фазовому переході, пластична деформація та деформація, викликана перепадами температур.

Рівняння руху нескінченно малого об'ємного елемента суцільного середовища, що деформується, в ортогональній системі координат α^1, α^2, α^3 в представимо у вигляді:

$$\frac{\partial \upsilon_i}{\partial t} = \frac{1}{\rho} \cdot \frac{\partial \sigma_{ij}}{\partial \alpha^j} + B_i(\sigma_{mn}) \quad . \tag{1}$$

Де *i, j, n, m* =1, 2, 3, а ρ - густина. Величини $B_i(\sigma_{nm})$, які знаходяться в правій частині рівняння (1), наведені в [1,2] , а також:

$$v_i = \frac{\partial u_i}{\partial t} \quad , \; i = 1, 2, 3.$$

В загальному випадку ортогональної системи координат тензор деформації і складові вектора переміщень пов'язані такими нелінійними співвідношеннями [3]:

$$\varepsilon_{11} = e_{11} + \frac{1}{2}\left[e_{11}^2 + \left(\frac{e_{12}}{2} + \omega_3 \right)^2 + \left(\frac{e_{13}}{2} - \omega_2 \right)^2 \right];$$

$$\varepsilon_{12} = e_{12} + e_{11}\left(\frac{e_{12}}{2} - \omega_3 \right) + e_{22}\left(\frac{e_{12}}{2} + \omega_3 \right) + \left(\frac{e_{13}}{2} - \omega_2 \right)\left(\frac{e_{23}}{2} + \omega_1 \right); \tag{2}$$

Інші складові тензора деформацій отримуються з (1) шляхом циклічної перестановки індексів. У випадку використання ортогональної декартової системи координат:

$$e_{11} = \frac{\partial u_1}{\partial \alpha_1}; e_{22} = \frac{\partial u_2}{\partial \alpha_2}; e_{33} = \frac{\partial u_3}{\partial \alpha_3};$$

$$e_{12} = \frac{\partial u_2}{\partial \alpha_1} + \frac{\partial u_1}{\partial \alpha_2}; e_{23} = \frac{\partial u_3}{\partial \alpha_2} + \frac{\partial u_2}{\partial \alpha_3}; e_{31} = \frac{\partial u_1}{\partial \alpha_3} + \frac{\partial u_3}{\partial \alpha_1}; \tag{3}$$

$$2\omega_1 = \frac{\partial u_3}{\partial \alpha_2} - \frac{\partial u_2}{\partial \alpha_3}; 2\omega_2 = \frac{\partial u_1}{\partial \alpha_3} - \frac{\partial u_3}{\partial \alpha_1}; 2\omega_3 = \frac{\partial u_2}{\partial \alpha_1} - \frac{\partial u_1}{\partial \alpha_2};$$

З урахуванням цього після диференціювання за часом в геометрично нелінійному випадку для швидкостей деформацій можна записати:

$$\frac{\partial \varepsilon_{11}}{\partial t} = (1 + e_{11})\frac{\partial v_1}{\partial \alpha_1} + \left(\frac{e_{12}}{2} + \omega_3 \right)\frac{\partial v_2}{\partial \alpha_1} + \left(\frac{e_{13}}{2} - \omega_2 \right)\frac{\partial v_3}{\partial \alpha_1};$$

$$\frac{\partial \varepsilon_{22}}{\partial t} = \left(\frac{e_{21}}{2} - \omega_3 \right)\frac{\partial v_1}{\partial \alpha_2} + (1 + e_{22})\frac{\partial v_2}{\partial \alpha_2} + \left(\frac{e_{23}}{2} + \omega_1 \right)\frac{\partial v_3}{\partial \alpha_2};$$

$$\frac{\partial \varepsilon_{33}}{\partial t} = \left(\frac{e_{31}}{2} + \omega_2 \right)\frac{\partial v_1}{\partial \alpha_3} + \left(\frac{e_{32}}{2} - \omega_1 \right)\frac{\partial v_2}{\partial \alpha_3} + (1 + e_{33})\frac{\partial v_3}{\partial \alpha_3};$$

$$\frac{\partial \varepsilon_{12}}{\partial t}=\left(1+\frac{e_{11}}{2}+\frac{e_{22}}{2}\right)\left(\frac{\partial v_2}{\partial \alpha_1}+\frac{\partial v_1}{\partial \alpha_2}\right)+\left(\frac{e_{12}}{2}-\omega_3\right)\frac{\partial v_1}{\partial \alpha_1}+\left(\frac{e_{12}}{2}+\omega_3\right)\frac{\partial v_2}{\partial \alpha_2}+$$
$$+\frac{(e_{22}-e_{11})}{2}\left(\frac{\partial v_2}{\partial \alpha_1}-\frac{\partial v_1}{\partial \alpha_2}\right)+\left(\frac{e_{23}}{2}+\omega_1\right)\frac{\partial v_3}{\partial \alpha_1}+\left(\frac{e_{13}}{2}-\omega_2\right)\frac{\partial v_3}{\partial \alpha_2};$$
$$\frac{\partial \varepsilon_{23}}{\partial t}=\left(1+\frac{e_{22}}{2}+\frac{e_{33}}{2}\right)\left(\frac{\partial v_3}{\partial \alpha_2}+\frac{\partial v_2}{\partial \alpha_3}\right)+\left(\frac{e_{23}}{2}-\omega_1\right)\frac{\partial v_2}{\partial \alpha_2}+\left(\frac{e_{23}}{2}+\omega_1\right)\frac{\partial v_3}{\partial \alpha_3}+ \quad (4)$$
$$+\frac{(e_{33}-e_{22})}{2}\left(\frac{\partial v_3}{\partial \alpha_2}-\frac{\partial v_2}{\partial \alpha_3}\right)+\left(\frac{e_{31}}{2}+\omega_2\right)\frac{\partial v_1}{\partial \alpha_2}+\left(\frac{e_{21}}{2}-\omega_3\right)\frac{\partial v_1}{\partial \alpha_3};$$
$$\frac{\partial \varepsilon_{31}}{\partial t}=\left(1+\frac{e_{33}}{2}+\frac{e_{11}}{2}\right)\left(\frac{\partial v_1}{\partial \alpha_3}+\frac{\partial v_3}{\partial \alpha_1}\right)+\left(\frac{e_{31}}{2}-\omega_2\right)\frac{\partial v_3}{\partial \alpha_3}+\left(\frac{e_{31}}{2}+\omega_2\right)\frac{\partial v_1}{\partial \alpha_1}+$$
$$+\frac{(e_{11}-e_{33})}{2}\left(\frac{\partial v_1}{\partial \alpha_3}-\frac{\partial v_3}{\partial \alpha_1}\right)+\left(\frac{e_{12}}{2}+\omega_3\right)\frac{\partial v_2}{\partial \alpha_3}+\left(\frac{e_{32}}{2}-\omega_1\right)\frac{\partial v_2}{\partial \alpha_1},$$

Система рівнянь (1), (4) замикається фізичними співвідношеннями, що зв'язують напруги і деформації.

Авторами пропонується для моделювання поведінки псевдо-пружно-пластичних тіл використовувати співвідношення які пов’язують елементи тензора деформації і складові вектора переміщень у не лінійній постановці.

[1] Development of the method with enhanced accuracy for solving problems from the theory of thermo-psevdoelastic-plasticity / A.Petrov, Yu.Chernyakov, P.Steblyanko, K.Demichev, V.Haydurov // Eastern-European Journal of Enterprise Technologies. 2018. Vol. 4/7 (94). P. 25–33.

[2] Математичне моделювання термомеханічних процесів в пружно-пластичних циліндричних тілах / [К.Е.Дьомічев, П.О.Стеблянко, Ю.А.Черняков, О.Д.Петров]. – Київ, 2017. – 169 с.

[3] Теория упругости / [В.В.Новожилов]. – Ленинград, 1952. – 381 с.

В.В. Кучанський

РОЗРОБКА ШТУЧНОЇ НЕЙРОННОЇ МЕРЕЖІ ДЛЯ ДОСЛІДЖЕННЯ РЕЗОНАНСНИХ ПЕРЕНАПРУГ

Резонансні перенапруги в електричних мережах надвисокої напруги спостерігаються при відхиленнях значень параметрів електромагнітних процесів від характерних для нормального усталеного режиму. Даний вид перенапруг відрізняється від тих, що супроводжують нормальні операції під час експлуатації мережі і які безпосередньо враховуються при проектуванні електропередачі. Для моделювання за допомогою штучної нейронної мережі була прийнята гіпотеза про певний розвиток подій, яка потім знайшла підтвердження при порівнянні результатів досліджень з експериментальними даними. Необхідною умовою є відповідне резонансне налаштування лінії електропередачі надвисокої напруги [1, 2].

Важливу роль при моделюванні процесів з використанням штучної нейронної мережі відіграє попередня підготовка моделі, яка полягає у використанні програмного інструментарію для вибору, навчання, тестування і використання штучної нейронної мережі [3, 4]. Зокрема, для вирішення поставленої в роботі задачі множиною вхідних даних $Input$ є: значення напруги джерела живлення $U_{ДЖ}$, час замикання полюсів вимикача δ, ємність фази лінії електропередачі $C_{Ф}$, нахил кривої намагнічення трансформатора L_{sat} і залишковий магнітний потік Φ_0:

$$Input = \left\{\Phi_0, L_{sat}, C_{Ф}, \delta, U_{ДЖ}\right\}. \quad (1)$$

На рис. 1 приведена функціональна структурна схема підготовки вибірок даних з метою навчання штучної нейронної мережі. Для формування даних був спеціально розроблений програмний комплекс «Нейроген», який випадковим чином генерує значення вибірки вхідних параметрів, що впливають на характеристики для моделювання режиму включення ненавантаженого автотрансформатора.

В блоці 1 вибірка формується таким чином, що величини кута включення вимикача, потрапляють в області, які відповідають максимальним значенням струму (70°÷110°) і (250°÷290°). Як показує аналіз результатів отриманих при моделюванні і експлуатації, саме при цих значеннях спостерігаються максимальні значення перенапруг. Далі програмно організовується циклічне введення вибірки (1) Inp по блоку 2. На третьому блоці в схему комплексу вводяться ці ж самі п’ять параметрів в модель довгої лінії, що відтворює режим включення автотрансформатора. В четвертому блоці за результатами моделювання визначається масив кривої напруги:

$$Curve^{A,B,C} = (Curve^{A}, Curve^{B}, Curve^{C}) \quad (2)$$

де $Curve^{A}, Curve^{B}, Curve^{C}$ - масив значень напруги фаз A,B та C відповідно.

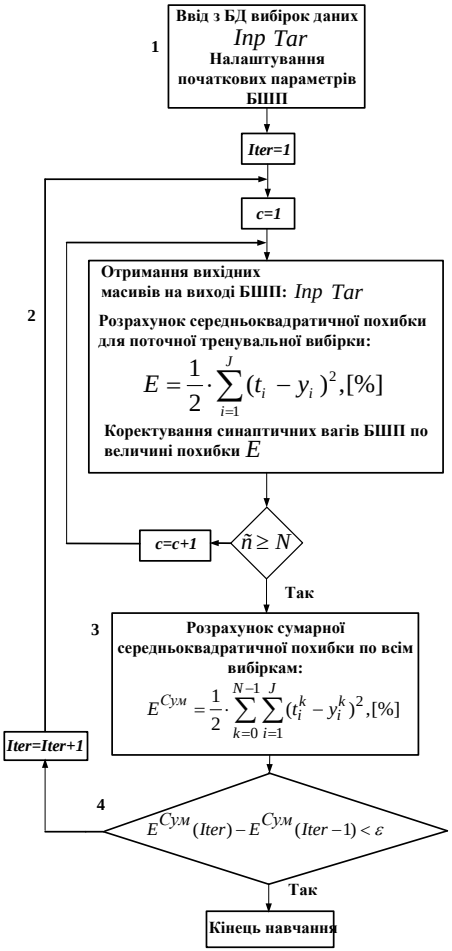


Рис. 1

Далі масив (2) $Curve^{A,B,C}$ потрапляє в ще один розроблений програмний «Нейрохар», який відповідає блоку 5 та визначає характеристики перенапруг: тривалість дії ($Dur^{A,B,C}$) і максимальні значення напруги ($U^{A,B,C}$), які і потрапляють в масив вихідних значень. Розробка «Нейрохар» зумовлена великим об'ємом масивів, що ускладнює неавтоматизовану обробку, а також складністю визначення $Dur^{A,B,C}$. Завдяки «Нейрохар» буде сформований

масив вихідних бажаних значень штучної нейронної мережі $U^{A,B,C}$ та $Dur^{A,B,C}$:

$$Tar = (U_A^{МДЛ}, U_B^{МДЛ}, U_C^{МДЛ}, Dur_A^{МДЛ}, Dur_B^{МДЛ}, Dur_C^{МДЛ}) \quad (3)$$

де $U_A^{МДЛ}, U_B^{МДЛ}, U_C^{МДЛ}$ - максимальні значення напруги та $Dur_A^{МДЛ}, Dur_B^{МДЛ}, Dur_C^{МДЛ}$ - тривалість дії напруги на ізоляцію устаткування.

Отримані в результаті роботи «Нейрохар» бажані вихідні сигнали (3) та вхідні сигнали (1-2), що згенеровані за допомогою «Нейроген», записуються в базу даних блоку 7.

Для дослідження перенапруг запропоновано використовувати штучної нейронної мережі з архітектурою багатошарового персептрона Як показує досвід, саме цей тип штучної нейронної мережі дозволяє успішно вирішувати завдання апроксимації, до яких відноситься й поставлена задача [3, 4]. Для навчання багатошарового персептрона використовується метод зворотного поширення помилки.

Вибірка даних (1) $Input$ і (2) Tar ділиться на навчальну і тестову. Як критерій навчання прийнята середньоквадратична похибка навчання, що розраховується:

$$E^{Сум} = \frac{1}{2} \cdot \sum_{k=0}^{N-1} \sum_{i=1}^{J} (t_i^k - y_i^k)^2, [\%] \quad (4)$$

де t^k – бажане значення $Dur^{A,B,C}$ та $U^{A,B,C}$; y^k – реальне значення виходу багатошарового персептрона $Dur^{A,B,C}$ та $U^{A,B,C}$; N – кількість поданих вибірок навчання, J – кількість вихідних шарів.

Резонансні перенапруги в електричних мережах можуть стати причиною розвитку важких аварій, тому що навіть при незначних амплітудних значеннях, мають порівняно велику тривалість та викликають відмову релейного захисту від підвищення напруги. Задача дослідження перенапруг парної кратності ускладнюється через врахування кореляції, яка існує між багатьма нечітко заданими параметрами.

[1] Кузнецов В.Г. Використання штучної нейронної мережі для визначення характеристик анормальних перенапруг / В.Г. Кузнецов, Ю.І. Тугай В.В. Кучанський // Праці Інституту електродинаміки НАН України. – К.: ІЕД НАНУ, 2012. – Вип. 31. – С. 8–14.

[2] V. Kuchanskyy, "The application of controlled switching device for prevention resonance overvoltages in nonsinusoidal modes," 2017 IEEE 37th International Conference on Electronics and Nanotechnology (ELNANO), Kiev, 2017, pp. 394-399.

[3] Аксенов С.В. Организация и использование нейронных сетей (методы и технологии) / С.В. Аксенов, В.Б. Новосельцев. – Томск.: Изд-во НТЛ, 2006. – 128 с.

[4] Галушкин А.И. Теория нейронных сетей. / А.И. Галушкин. [учеб. пособие для ВУЗов] – М.:ИПРЖР, 2010. – 496 с.

П.В. Шиманюк

АНАЛІЗ ТА ВИЗНАЧЕННЯ ТИПУ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ ДЛЯ РОЗВ'ЯЗАННЯ ЗАДАЧІ ПРОГНОЗУВАННЯ ВУЗЛОВОГО НАВАНТАЖЕННЯ

Штучні нейронні мережі (ШНМ) являють собою обчислювальні системи, які мають складну будову, подібну до біологічних нейронів у мозку людини чи тварини. Основою таких систем є вузли (нейрони), які об'єднані в шари і зв'язані між собою для передачі сигналів. З теорії машинного навчання відомо, що за допомогою ШНМ з одним прихованим шаром нейронів та нелінійною активаційною функцією можна апроксимувати будь-яку неперервну функцію з довільною точністю.

Завдяки розвитку обчислювальної техніки та сучасних графічних процесорів (GPU), методам та засобам на основі ШНМ вдалось досягти значних результатів у вирішенні різних задач, які в деяких випадках перевершують людські можливості. Все це дало поштовх для створення нейронних мереж більш складної архітектури і можливості для вдосконалення методів для їх навчання. На даний час ШНМ мають ряд напрямків застосування, відповідно до типу задач, зокрема: класифікації, прийняття рішень, кластеризації, прогнозування, стиснення даних та генерації нових даних.

Значне коло задач в галузі електроенергетики сьогодні розв'язуються з використанням штучних нейронних мереж, постійно розробляються нові та удосконалюються існуючі методи та моделі на базі ШНМ для розв'язання таких задач, а результати численних досліджень підтверджують ефективність використання ШНМ. Так, наприклад, в [1] описуються застосування гібридних систем на базі ШНМ та нечіткої логіки для короткострокового прогнозування попиту на електричну енергію та діагностики аварійних станів в електричних мережах.

Також до важливих задач, складові яких розв'язуються з використання ШНМ відносяться такі, як прогнозування електричного навантаження [2]; прогнозування режимних параметрів [8]; прогнозування перетоків потужності; прогнозування втрат електричного навантаження; прогнозування відпуску електричної енергії виробниками з відновлювальних джерел енергії [7]; пошук місць та виду пошкодження [5] в електричних мережах.

Вочевидь, що для різних задач використовуються різні типи та архітектури ШНМ. Однією з найпростіших архітектур серед ШНМ є перцептрон [4]. За рахунок своєї простоти та гнучкості таку мережу часто використовують як основу для гібридних моделей. Прикладом використання такої мережі є її застосування для визначення місць та видів [5] пошкоджень в електричних мережах, зокрема і лініях електропередавання.

Іншим прикладом є застосування нейронної мережі Кохенена для класифікації та діагностики електричного обладнання.

В свою чергу рекурентні мережі використовують для моделювання динамічних процесів, ідентифікації параметрів при наявності шумів, а також для оцінки стану електроенергетичної системи.

Ще одна архітектура нейронної мережі, під назвою Вольтері використовується для задач прогнозування нестаціонарних часових рядів, ідентифікації нелінійних об'єктів, а також для зменшення інтерференційних шумів у вхідних даних.

Для задач планування режимів автоматизованої системи диспетчерського управління, необхідними є графіки навантаження, які в свою чергу отримуються завдяки роз'язанню задач короткострокового прогнозування електричного навантаження. Для цієї задачі також використовуються різноманітні архітектури ШНМ. Наприклад, в [8] для даної задачі використана рекурентна нейронна мережа глибинного навчання типу LSTM [3]. Даний тип мережі досить широко застосовується в різних сферах, завдяки високій точності мережі і стабільності градієнту. Також, в [8] описано особливості використання даного типу нейронних мереж для прогнозування електричного навантаження.

Враховуючи, що в Україні почав функціонувати новий ринок електроенергії, прогнозування навантаження чи цін на електричну енергії є дуже актуальною задачею. Для прогнозування цін використовують такі типи ШНМ: багатошаровий перцептрон, рекурентні нейронні мережі, а також ШНМ радіально-базисної функції. В [6] описано особливості вирішення даної задачі на основі ШНМ радіально-базисної функції, яка за рахунок своєї архітектури, швидкої роботи і навчання, є досить ефективною, а також через відсутність проблем з локальними мінімумами, що можуть впливати на ефективність навчання. Використання точних прогнозних даних навантаження є важливим для роботи усіх учасників ринку. Так як виробники енергії з відновлюваних джерел енергії ВДЕ продають свою енергію гарантованому покупцеві, тому їм потрібно надавати точні дані відпуску електроенергії, для цього в статті [7] було проведення дослідження короткострокового інтегрального прогнозу сумарного відпуску електроенергії виробниками з відновлюваних джерел енергії (ВДЕ). Метою якого було отримання задовільних результатів прогнозу сумарного відпуску електроенергії, що дозволить зменшити плату за небаланс тим самим знизити ціну для кінцевих споживачів, а також дасть можливості продажу електроенергії на ринку «на добу наперед» для гарантованого покупця. У цьому дослідження було використано ШНМ глибинного навчання eResNet, яка була розроблена в Інституті електродинаміки НАН України. Дане дослідження показало, що похибка прогнозу з використанням ШНМ була врази меншою у порівнянні з прогнозами які надавали виробники з ВДЕ.

Однією з важливих сучасних задач, що потребує розв'язання є прогнозування вузлового навантаження, що є необхідним для вирішення задач планування та керування режимами енергосистеми. Аналіз різних типів та архітектур ШНМ дозволив виконати попередній вибір ШНМ для розв'язання цієї задачі. Зокрема запропоновано архітектуру штучної

нейронної мережі глибинного навчання для векторного прогнозування часових рядів, яка враховує взаємозв'язок між електричним навантаженням сумісних вузлів, оскільки нейронна мережа з більшою кількістю прихованих шарів здатна точніше апроксимувати складні функціональні залежності. Крім того, для однофакторного векторного прогнозування вузлового навантаження пропонується використовувати гібридну архітектуру, ключовими елементами якої є модуль довго- короткострокової пам'яті LSTM, ШНМ типу багатошаровий перцептрон та обхідні з'єднання

[1] Butkevych O.F., Pavlovskiy V.V. Hybrid system in power system problems solving. Tekhnichna elektrodynamika tematychnyi vypusk problemy suchasnoi enerhetyky Kiev 2002 .№ 4 Pp77-82.

[2] Gasparin A., Slobodan L., Alippi C. Deep learning for time series forecasting:the electric load case. 22 Jul 2019.

[3] Hochreiter S., Schmidhuber J. Long short-term memory. Neural Computation 9(8): 1997. Pp.1735-1780.

[4] Rosenblatt F. The perceptron: a probabilistic model for information storage and organization in the brain. Psychological Review Vol. 65, No. 6, 1958.

[5] Блинов И.В. Определение вида короткого замыкания ЛЭП на основе искусственных нейронных сетей. Тех. електродинаміка. Тем. дипуск: Силова електроніка та енергоефективність. 2007. С. 49-52.

[6] Блінов І.В., Корхмазов Г.С. Використання штучних нейронних мереж для розв'язання задачі короткострокового прогнозування оптових ринкових цін на електричну енергію. Праці інституту електродинаміки НАН України. Тем. вип.: Енергетичні ринки: перехід до нової моделі ринку двосторонніх контрактів і балансуючого ринку. 2009. С. 15 – 22.

[7] Блінов І.В., Мірошник В.О., Шиманюк П.В. Короткостроковий інтервальний прогноз сумарного відпуску електроенергії виробниками з відновлюваних джерел енергії. Праці інституту електродинаміки НАН України. 2019р. №54 С. 5-12.

[8] Черненко П.О., Мірошник В.О. Короткострокове прогнозування електричного навантаження електропостачальної компанії з використанням штучної нейронної мережі глибинного навчання. Праці інституту електродинаміки НАН України. 2018р. № 50. С. 5-11.

А.В. Ониськова, С.Ф. Гончар, М.Ю. Комаров, В.В. Ткаченко, С.М. Сергєєв

АНАЛІЗ СТАНДАРТІВ ПО ЗАБЕЗПЕЧЕННЮ КІБЕРБЕЗПЕКИ ІНТЕЛЕКТУАЛЬНИХ МЕРЕЖ SMART GRID

Поява, існування та актуальність проблеми кібербезпеки новітніх і перспективних електроенергетичних систем, у тому числі із застосуванням інтелектуальних мереж Smart Grid визнається сучасною світовою енергетичною спільнотою. Дослідженню і розв'язанню цієї проблеми приділяється все більше уваги в багатьох передових країнах світу. Впровадження технології інтелектуальних мереж з одного боку спрощує і прискорює управління, але з іншого боку відкриває доступ до можливих кібератак і неправомірного використанню даних.

Дослідженню проблеми забезпечення кібербезпеки інформаційних систем об'єктів енергетичного сектору присвячено значну кількість наукових робіт, зокрема [1, 2]. Разом з тим, питання кібербезпеки сучасних електроенергетичних об'єктів з використанням інтелектуальних мереж Smart Grid, оснащених цифровими системами моніторингу, управління, релейного захисту та протиаварійної автоматики стають дуже актуальними, через новизну і недостатнє дослідження проблеми. Необхідно провести аналіз стандартів, які стосуються питання забезпечення кібербезпеки інтелектуальних мереж Smart Grid.

На традиційних підприємствах порушення кібербезпеки в більшості випадків призводить до фінансових втрат, тоді як інші, більш серйозні наслідки є досить рідкими, на відміну від інтелектуальних мереж Smart Grid. Забезпечення кібербезпеки інтелектуальних мереж Smart Grid вимагає нових, багатопрофільних підходів, що поєднують різні технології та включають управлінські, політичні, правові аспекти тощо.

Забезпечення кібербезпеки інтелектуальної мережі є необхідним для надійної роботи цієї нової форми електромережі. На думку експертів, у першу чергу слід застосовувати стандартизовані рішення та практику. В останні роки було опубліковано багато нових стандартів, пов'язаних із інтелектуальними мережами Smart Grid, що, призводить до певних труднощів у систематизації відповідної інформації.

Розглянемо деякі стандарти, які регламентують питання забезпечення кібербезпеки інтелектуальних мереж Smart Grid [3].

- NISTIR 7628 [4]. Цей документ являє собою аналітичну базу, яку організації можуть використовувати для розробки ефективних стратегій кібербезпеки Smart Grid з урахуванням їх конкретних особливостей, ризиків та уразливостей. Даний документ представляє методи для оцінки ризику, а також визначення та застосування відповідних вимог безпеки. У документі приводиться стратегія, архітектура та вимоги високого рівня Smart Grid, стратегія кібербезпеки включає довідкову інформацію про Smart Grid та важливість кібербезпеки для забезпечення надійності мережі та

конфіденційності конкретної інформації. Обговорюється стратегія кібербезпеки для Smart Grid та конкретні завдання в рамках цієї стратегії.

- ISO/IEC 27019 [5]. Область застосування ISO / IEC 27019 охоплює системи управління технологічними процесами, що використовуються енергетичною промисловістю для контролю та моніторингу генерації, передачі, зберігання та розподілу електроенергії, газу та тепла у поєднанні з керуванням допоміжними процесами.

- IEC 62443 [6]. Метою застосування стандартів 62443 серій є підвищення безпеки, доступності, цілісності та конфіденційності компонентів або систем, що використовуються для промислової автоматизації та управління, а також забезпечення критеріїв для придбання та впровадження безпечних систем промислової автоматизації та управління. Відповідність вимогам стандартів 62443 серій призначена для поліпшення електронної безпеки та сприяє виявленню і усуненню уразливостей, зменшуючи ризик порушити конфіденційну інформацію або спричинити вихід з ладу апаратне та програмне забезпечення. Серія стандартів 62443 заснована на встановлених стандартах безпеки систем інформаційних технологій загального призначення (наприклад, серії ISO / IEC 27000), ідентифікуючи та вирішуючи важливі відмінності, наявні в промислових автоматизованих системах управління.

- IEC 62351 [7]. Сімейство стандартів 62351 регламентує керування енергетичними системами та пов'язаний з ним інформаційний обмін, безпеку даних та комунікацій, зображує архітектуру захищеної системи живлення та стандартизує її протоколи і компоненти.

Таким чином, проведено аналіз стандартів, які стосуються питання забезпечення кібербезпеки інтелектуальних мереж Smart Grid. За результатами проведеного аналізу здійснено систематизацію, представлення та опис основних стандартів, які визначають вимоги до кібербезпеки, що застосовуються до інтелектуальних мереж Smart Grid.

[1] Mokhor V., Gonchar S. The Idea of the Construction of the Algebra of Risks on the Basis of the Theory of Complex Numbers. Electronic modeling, 2018, Vol.40, no. 4, pp. 107-111.

[2] Mokhor V., Gonchar S., Dybach O. Methods for the Total Risk Assessment of Cybersecurity of Critical Infrastructure Facilities. Nuclear and Radiation Safety, 2019, 2(82), pp. 4-8.

[3] R. Leszczyna. A Review of Standards with Cybersecurity Requirements for Smart Grid. // Computers & Security, 2018.

[4] Guidelines for Smart Grid Cyber Security: Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements.

[5] ISO/IEC 27019. Information technology — Security techniques — Information security controls for the energy utility industry.

[6] IEC 62443. Cyber Security for Industrial Automation and Control Systems (IACS).

[7] IEC 62351. Power systems management and associated information exchange - Data and communications security.

В.В. Шкарупило

ПРО ЗАСТОСУВАННЯ ПРАВИЛА КОМПОЗИЦІЇ ПРИ СИНТЕЗІ ФОРМАЛЬНИХ СПЕЦИФІКАЦІЙ

У наш час формальні методи є дієвим засобом забезпечення заданого рівня функціональної безпеки систем, зокрема систем критичного призначення, до яких відносяться і системи енергетичної галузі. Механізм названого забезпечення полягає у своєчасному виявленні та усуненні потенційно небезпечних умов у роботі електронних систем із програмною складовою [3]. Зокрема, у Наказі Державної інспекції ядерного регулювання України від 22.07.2015 № 140, із змінами, внесеними згідно з Наказом Державної інспекції ядерного регулювання № 508 від 25.11.2019, дається наступне визначення поняттю функціональної безпеки: «функціональна безпека – властивість системи (компонента) атомної станції, що полягає у здатності виконувати всі потрібні функції, важливі для безпеки, зберігати потрібні властивості та відповідати заданим характеристикам в усіх передбачених проектом режимах й умовах експлуатації» [7].

Демонстративними і різноплановими прикладами успішного застосування формальних методів, зокрема, методів перевірки на моделі, є програмна платформа хмарних сервісів Microsoft Azure [4], атомна енергетика Фінляндії [6] тощо.

Характерними ознаками методів перевірки на моделі є наступні: можливість автоматизації їх застосування; судження відносно властивості (властивостей) системи виноситься на основі відповідної моделі – формальної специфікації (ФС). Засоби опису ФС різняться як за виразними можливостями, так і за ступенем строгості.

У роботі розглядається формалізм TLA+ темпоральної логіки дій TLA (Temporal Logic of Actions) Л. Лемпорта як засіб створення математично строгих ФС, що, на відміну від альтернативних рішень, дозволяє виразити властивість (властивості) досліджуваної системи єдиною темпоральною формулою [5].

Компактність і строгість ФС розглядаються в роботі у якості чинників, що спрощують процес сприйняття і аналізу ФС розробником, а також стимулюють зниження впливу людського фактору на результати синтезу ФС. У якості засобів розвитку існуючих напрацювань в озвученому контексті розглядаються числення послідовних процесів, що взаємодіють, Ч. Хоара (CSP, Communicating Sequential Processes) [1], «трійки Хоара» і відповідні аксіоми (правила) [2].

У якості засобу «компактизації» ФС розглянемо правило композиції:

$$\frac{\{\varphi_0\}e_1\{\varphi_1\},\{\varphi_1\}e_2\{\varphi_2\},...,\{\varphi_{n-1}\}e_n\{\varphi_n\}}{\{\varphi_0\}e_1;e_2;...;e_n\{\varphi_n\}}, \qquad (1)$$

де $n \in N$, $e_j\left(j = 1,2,...,n\right)$ – j-а «подія», що відображає виконання фрагменту ФС, φ_{j-1} – передумова виникнення події, φ_j – пост-умова. При цьому φ_{j-1} і φ_j є специфікаціями станів системи переходів (СП) – автомату із кінцевим числом станів (структури Кріпке). Виникнення e_j інтерпретується як опрацювання відповідного фрагменту програми.

Чисельник виразу (1) представляє ФС фрагментовано – до застосування правила, знаменник – після. Ключова ідея роботи полягає у застосуванні у якості передумови виникнення e_j не ФС стану СП, а ФС попередньої події e_{j-1}.

Результати проведених експериментальних досліджень показали, що, на прикладі досліджуваного тестового набору, застосування правила композиції (1) дозволило зменшити розмір результуючої ФС на значення від 18 до 33 %. Такий ефект охарактеризовано як вагомий. При цьому показником розміру ФС виступила кількість рядків.

Отже, результати проведених досліджень показали, що застосування правила композиції на основі трійок Хоара є дієвим засобом компактизації формальної специфікації системи.

[1] Hoare C. A. R. Communicating sequential processes. Communications of the ACM. 1978. Vol. 21, No. 8. P. 666-677.

[2] Hoare C. A. R. An axiomatic basis for computer programming. Communications of the ACM. 1969. Vol. 12, No. 10. P. 576-583.

[3] IEC 61508 Edition 2.0. Functional safety of electrical/electronic/programmable electronic safety-related systems. [Approved: April 2010]. URL: https://www.iec.ch/functionalsafety/standards/page2.htm. (Accessed: 07.02.2020).

[4] Kuppe M. A., Lamport L., Ricketts D. The TLA+ Toolbox. Formal Integrated Development Environment, F-IDE 2019 : 5th Workshop (Porto, Portugal, October 7, 2019). EPTCS 310, 2019. P. 50-62. DOI: http://doi.org/10.4204/EPTCS.310.6

[5] Lamport L. Specifying systems: The TLA+ language and tools for hardware and software engineers. Boston : Addison-Wesley, 2002. 382 p.

[6] Pakonen A., Tahvonen T., Hartikainen M., Pihlanko M. Practical applications of model checking in the Finnish nuclear industry. Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies : Proc. 10th International Topical Meeting (San Francisco, CA, USA, 11-15 June 2017). P. 1342-1352.

[7] Про затвердження Вимог з ядерної та радіаційної безпеки до інформаційних та керуючих систем, важливих для безпеки атомних станцій: наказ Державної інспекції ядерного регулювання від 22.07.2015 № 140, із змінами, внесеними згідно з Наказом Державної інспекції ядерного регулювання № 508 від 25.11.2019. URL: https://zakon.rada.gov.ua/laws/term/34229 (дата звернення: 26.03.2020).

О.О. Огір

МЕТОДИ ТА ТЕХНОЛОГІЇ ОТРИМАННЯ І ОБРОБКИ ОПЕРАТИВНОЇ ІНФОРМАЦІЇ ПРИ ВИКОРИСТАННІ НЕЙРОННО-МЕРЕЖЕВОГО ПІДХОДУ ДО УЗ ЗОБРАЖЕНЬ ВНУТРІШНЬОЇ СТРУКТУРИ МАТЕРІАЛІВ

Актуальність даної тематика показана в [1, 2, 3].

Сучасні діагностичні зображення, що формуються в процесі обробки оперативної інформації, являють собою в більшості випадків результат реалізації тих чи інших алгоритмів цифрової реконструкції.

Завдання сегментації діагностичних зображень, тобто виділення на цих зображеннях зон цікавості, відповідних біотканинам з однаковими характеристиками, залишається одним з найактуальніших для розвитку сучасних діагностичних методів. Завдання даного класу відносяться до розробки програмних засобів розпізнавання образів і візуалізації.

Нейронно-мережевий підхід має переваги перед традиційними математичними методами, якщо розглянута задача не піддається адекватній формалізації, оскільки містить елементи невизначеності, що не формалізуються традиційними математичними методами або існуючий математичний апарат вирішення задачі не задовольняє вимогам отримання рішень по часу, розміру, якості та ін. У такій ситуації, щоб отримати потрібну якість виконання завдання, ефективним є нейронно-мережевий підхід.

При такому підході зведені до мінімуму спотворення, які викликані неточністю апаратури. Другий підхід до цієї проблеми заснований на методах обробки зображень з метою виділення на них деяких необхідних зон деталей або неоднорідностей, при цьому не суттєва інформація пригнічується. В результаті виходить зображення зручне для візуального аналізу або інтерпретації. Але в даному процесі отримання зображень також є різні спотворюючі чинники, які впливають на їх якість. Джерелом цих спотворень може бути як сам алгоритм отримання зображення (якщо зображення є результатом реалізації тих чи інших алгоритмів цифрової реконструкції), так і недосконаліть пристроїв введення-виведення, що мають часто нелінійні характеристики передачі рівня сигналу. Методи підвищення інформативності зображень усувають негативні спотворення, такі як недостатня контрастність, спотворені характеристики яскравості і висока зашумленість.

У даній роботі моделювання навмисно проводиться для випадку низько контрастних характеристик. Така постановка супроводжується характерною нелінійністю і виключається будь-яка можливість отримання задовільних оцінок з використанням ліанеризації підходів. Завдання інтерпретації діагностичних зображень вирішується в рамках обраної математичної моделі для кожного набору параметрів з навчальної множини.

Отож, якщо ідентифікуючим параметром є положення центру розподілу інтенсивності яскравості, для якого відомі його геометричні розміри і

гістограми, то підготовка вхідних даних для нейронної мережі зводиться до багаторазового обчислення амплітуд градієнтів інтенсивності яскравості для різних значень x – координати центру неоднорідності.

Якщо геометричні параметри неоднорідності і контрасти є фіксованими, то для рішення задачі необхідно визначити форми гістограмного розподілу яскравості. На рис. 1 представлені ексцесивна і багатовершинна гістограми. Ексцесивна гістограма має унімодальний характер з максимальним значенням інтенсивності яскравості і характеризується вузькою підставою і загостреною вершиною, що говорить про відсутність неоднорідностей в виділеній зоні. Багатовершинна гістограма, в межах якої відбувається перерозподіл значень яскравості, а також зміна значень їх максимумів, характерна для рентгенівських зображень краеутворюючої дуги серцево-судинної системи і свідчить про наявність множинних артефактів.

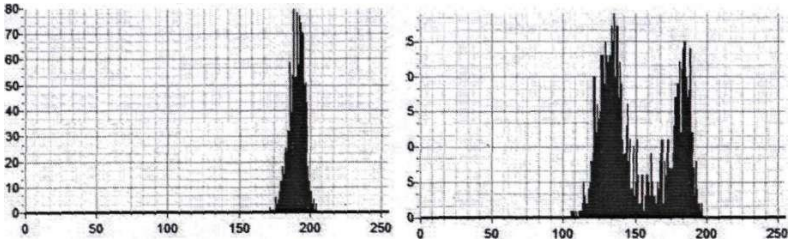


Рис. 1 Форми гістограмного розподілу яскравості

В результаті досліджень та тестування нейронна мережа була налаштована на ідентифікацію розподілу гістограм і поданням на її вхід 60 пар зображень «Характеристики розподілу – параметри неоднорідності». Нейромоделювання зводиться до численного експерименту з мережею, знаходженню її оптимальної архітектури, а також до вибору функцій активації, підбору зсувів і т.д., забезпечують найбільш швидке навчання мережі при вирішенні конкретної завдання ідентифікації променевих зображень.

При виборі архітектури мережі було проведено дослідження кількох конфігурацій з різною кількістю елементів. При цьому основним показником був обсяг навчальної множини і узагальнююча здатність мережі.

[1] Теория нейронных сетей. / [А.И. Галушкин] - М.: ИПРЖР, 2010. – 348 с.
[2] Перспективы распараллеливания программ нейросетевого анализа и обработки данных / [В.Г. Царегородцев] // Материалы конф. «Математика, информатика, управление – 2008». – Иркутск, 2014. – С. 110-117.
[3] Машинне навчання. / [Іван Гудфелов, Йоша Бенгіо, Арон Коурвілле] MIT Press, 2016. Режим доступу: http://www.deeplearningbook.org.

О.С. Огір

ДОСЛІДЖЕННЯ І ОПТИМІЗАЦІЯ МЕТОДІВ АНАЛІЗУ І ОБРОБКИ ДІАГНОСТИЧНИХ ЗОБРАЖЕНЬ

Мета роботи полягає у розробці спеціалізованих інтелектуальних технологій для розпізнавання й аналізу неоднорідностей на цифрових діагностичних зображеннях, зокрема у створенні нової технології, програм та апаратури для вимірювань та обробки оперативної інформації у вигляді фазових параметрів відбитого когерентного поля в сканованому об'ємі при застосуванні спеціалізованих нейронних мереж для розпізнавання новоутворень на діагностичних зображеннях, що дасть можливість сформувати нову діагностичну концепцію до розпізнавання захворювань на ранніх стадіях, а також виявлення найдрібніших дефектів матеріалів та середовищ. Варто зазначити, що досить складно забезпечити необхідний рівень адекватності інформації, реєстрованої з різних, послідовних точок синтезованої апертури для всіх точок дефекту, розташованого в сканованому шарі матеріалу. Теоретично, зондування повинно здійснюватися плоскою хвилею для всіх точок дефекту з синхронізацією процесу опромінення дефекту з різних точок синтезованої апертури. Оскільки при кожному зондуванні здійснюється тільки один вимір амплітуди і фази сигналу з заданого шару матеріалу (по часу затримки приходу сигналу) в такій системі якість зображення визначається обмеженнями амплітудної голографії, що є досить впливовими і можуть визначати лише зовнішні контури дефекту в досить розмитому (не сфокусованому) вигляді. Таким чином, до основних факторів, що впливають на якість та точність реконструкції діагностичних зображень можна віднести наступні:

- Недостатньо висока поперечна просторова розрізнювальна здатність, що визначається фізичними параметрами звукового променя.
- Низька точність відтворення інтенсивності сигналів фокусованих точок об'єкту, що є обмеженою внаслідок дії сигналів-завад реверберацiйної і нормальної природи.
- Погіршення поздовжньої та поперечної розрінювальної здатності за рахунок флуктуації тривалості та амплітуди сумарного ехосигналу. Ці флуктуації визначаються зміненням форми фронтів ехосигналів при розповсюдженні в досліджуваному середовищі.

В результаті буде створена нова технологія ефективного розпізнавання дефектів об'єктів на ранніх стадіях, а також виявлення найдрібніших дефектів матеріалів та середовищ. Спосіб ідентифікації характеристик гістограм, заснований на застосуванні спеціалізованих нейронних мереж. Зокрема, будуть розглянуті такі області застосування цього підходу в обробці цифрових зображень, як використання багатошарових персептронів для вирішення завдань інтерпретації даних і конструювання спеціалізованих нейронних мереж.

Є.В. Парус, О.Є. Парус

ВІДПОВІДАЛЬНІСТЬ ЗА НЕБАЛАНСИ ВИРОБНИКІВ З ВІДНОВЛЮВАЛЬНИХ ДЖЕРЕЛ У СТРУКТУРІ РИНКОВОЇ ВАРТОСТІ ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ

На момент впровадження нової моделі ринку електроенергії України [1, 5] доля відновлювальних джерел енергії (ВДЕ) у загальній структурі виробничих потужностей ОЕС України складала більше 5% (6.46% станом на вересень 2019 р.), а доля ВДЕ у структурі у вартості електроенергії вже перевищила 10%. В порівнянні з 2018 в 2019 році за перші 7 місяців частка виробництва станціями з ВДЕ виросла в 2 рази з 1,6% до 3,2% (згідно даних ДП «Енергоринок). При цьому лише за перше півріччя 2019 р. встановлена потужність об'єктів відновлювальної енергетики виросла на 71,6% з 2117,42 МВт до 3634,422 МВт (станом на 01.07.2019). За даними ДП «Гарантований покупець» на кінець 2019 року загальна встановлена потужність ВДЕ за укладеними договорами складала 4 803 МВт.

В новому ринку електричної енергії гарантований покупець (ГП) купує всю вироблену з ВДЕ (крім домогосподарств) та продає на РДН/ВДР та постачальникам універсальної послуги [2]. Згідно із чинним законодавством, ГП за покладеними на нього спеціальними обов'язками для забезпечення загальносуспільних інтересів (ПСО) [3] компенсує різницю між «зеленим» тарифом та ринковою вартістю електроенергії шляхом закупівлі необхідних обсягів електроенергії у ДП НАЕК «Енергоатом» та ПрАТ «Укргідроенерго» на спеціалізованих аукціонах із подальшим їх перепродажем на ринку на добу наперед (РДН) [7] та внутрішньодобового ринку (ВДР).

Для оцінки впливу ВДЕ на ринкову вартість електричної енергії розглянемо спрощену модель ціноутворення в організованих сегментах ринку електроенергії України з єдиним для всіх сегментів графіком пропозиції та фіксованим за обсягами нееластичним по ціні попитом в межах однієї години доби (рис. 1).

За умовою обов'язковості продажу всіх обсягів виробленої ВДЕ електроенергії, відповідна пропозиція розглядається на РДН першочергово, що призводить до зміщення інших пропозицій вправо по осі обсягів. Таке зміщення призводить до зменшення граничної ціни на погодинному аукціоні РДН – стійка тенденція за появи будь-якої додаткової пропозиції з мінімальним значенням ціни в сегменті РДН. Точка перетину графіків попиту та пропозиції в сегменті РДН також є початковою точкою графіка пропозиції для балансування на завантаження чи розвантаження енергоагрегатів електростанцій на балансуючому ринку (БР) [4, 8]. Для спрощення несуттєві по відношенню до повного балансу обсяги торгів у сегменті ВДР не враховуються на рис.1. Тому загальне зміщення графіка пропозиції по осі обсягів вправо за умови збільшення обсягів пропозиції ВДЕ призводитиме зо зменшення ціни у початковій точці (область 1 на рис.1) балансування та

загального зниження вартості як розвантаження (штрихована область 2 на рис.1), так і завантаження (штрихована область 3 на рис.1), з іншого боку ВДЕ призводять до появи додаткових небалансів електричної енергії на БР, як в частині розвантаження (штрихована область 4 на рис. 1), так і завантаження (штрихована область 5 на рис.1) .

Важливо, що згідно Закону для виробників, які входять в балансуючу групу ГП вводяться спеціальні механізми відповідальності за власні небаланси. До 31 грудня 2020 р. виробники з альтернативних джерел звільнені від відповідальності за власні небаланси, шляхом встановлення на рівні 0% частки відшкодування ГП вартості небалансів. Законом передбачено щорічне збільшення на 10% даного показника до рівня 100% з 1 січня 2030 р. Крім того для виробників з ВДЕ до 31 грудня 2029 р. встановлено значення допустимих відхилень, тобто відповідальність за небаланс настає при похибці прогнозу ВЕС більше 20%, СЕС більше 10% та малих ГЕС більше 5%. Проте при досягненні виробниками з ВДЕ частки в розмірі 5% і більше в річному балансі електричної енергії значення допустимих відхилень знижуються до 10% для ВЕС та 5% для СЕС.

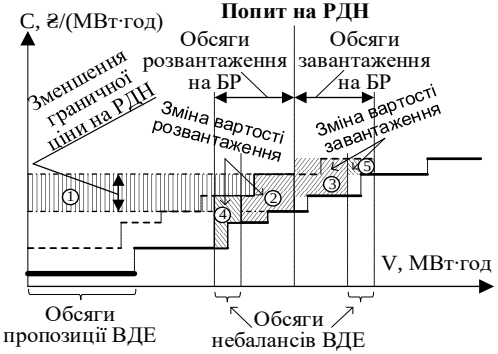


Рис.1

Окрім «зелених» тарифів, надбавок за використання вітчизняного обладнання, зниження оподаткування при імпорті обладнання та гарантованої купівлі та/або оплати заявлених обсягів відпуску навіть при відключенні електроустановок за диспетчерськими командами, звільнення від відповідальності за власні небаланси є засобом стимулювання збільшення встановленої потужності електростанцій з ВДЕ, але на відміну від інших такий механізм призводить до суттєвих проблем при балансуванні попиту і пропозиції в енергосистемі.

Наразі в ситуації, коли практично відсутня відповідальність за небаланси, похибка прогнозу відпуску електричної енергії «на добу» наперед» ВЕС та СЕС може досягати 60% в окремі години доби, що суттєво ускладнює балансування енергосистеми та знижує надійність її роботи. Розглянемо прийнятий механізм відповідальності за небаланси виробників з ВДЕ більш детально. Згідно затвердженого Порядку [2] величина врахованого відхилення фактичного обсягу відпущеної електричної енергії від прогнозного для кожної генеруючої одиниці (u) виробника (p) розраховується за формулами:

$$APE_t^{up} = \frac{\left|W_t^{up} - PR_t^{up}\right|}{PR_t^{up}} \cdot 100\ \%, \qquad (1)$$

$$\varepsilon_t^{up} = \begin{cases} \left(W_t^{up} - PR_t^{up}\right) \cdot \dfrac{a^u}{100}, & \text{якщо } APE > K^u \\ 0, & \text{якщо } APE \le K^u \end{cases},$$

$$\varepsilon_t^p = \sum\nolimits_{u \in p} \varepsilon_t^{up}$$

де W_t^{up} – фактичний обсяг відпуску електричної енергії в годину *t*, МВт·год;
PR_t^{up} - прогнозний обсяг відпуску електричної енергії в годину *t*, МВт·год;
APE_t^{up} – величина абсолютного відхилення у відсотках;
K^u – допустиме відхилення (для ВЕС – 20%, ГЕС – 5%, СЕС – 10%);
a^u – частка відшкодування гарантованому покупцю, визначена в перехідних положеннях Закону України «Про ринок електричної енергії»;
ε_t^{up} – величина врахованого відхилення для генеруючої одиниці *u* виробника *p;*
ε_t^p – сумарне враховане відхилення всіх генеруючих одиниць виробника *p*.

Винесення в знаменник формули (1) прогнозних значень викликано необхідністю уникнути ділення на 0 в години доби, коли станція фактично не відпускала електроенергію. Наприклад, в нічні години для СЕС та при силі вітру, що перевищує технічні можливості роботи ВЕС. Але при використанні зазначеної формули у виробників виникає можливість зменшувати свої виплати, завищуючи прогнозні значення. Наприклад, при фактичному значенні в 100 одиниць прогноз в 90 одиниць дає похибку 11,1%, а при прогнозі в 110 похибка складає 9,1%, що для СЕС є допустимим відхиленням і відповідальність за небаланс не настає при тому самому абсолютному відхиленні в 10 одиниць.

Критерій використання прогнозу наведений в Порядку дещо обмежує можливість зловживань станціями, але відкриває можливість для маніпуляцій гарантованому покупцю, як збільшувати так і зменшувати платежі виробників. Згідно даного пункту Порядку гарантований покупець повинен використовувати власний прогноз відпуску для станцій виробників, якщо середньоквадратична похибка його прогнозу нижче середньоквадратичної похибки виробника 9 днів з 14.

Для уникнення такої можливості необхідно в знаменнику формули (1) використовувати значення незалежно від дій виробника (при експлуатації електростанції). Такою величиною може бути встановлена потужність електростанції. Обсяг відшкодування виробником за «зеленим» тарифом гарантованому покупцю частки вартості врегулювання небалансу у розрахунковий період (IMC_t^p) розраховується за формулою:

$$CIEQ_t^p = \begin{cases} \frac{\varepsilon_t^p}{S_t^\varepsilon} \cdot \varepsilon_t^{sum} \cdot (P_t^{DAM} - P_t^{IMSP}), \varepsilon_t^{sum} > 0 \wedge \varepsilon_t^p > 0 \wedge P_t^{IMSP} < P_t^{DAM} \\ \frac{\varepsilon_t^p}{S_t^\varepsilon} \cdot \varepsilon_t^{sum} \cdot (P_t^{DAM} - P_t^{IMSP}), \varepsilon_t^{sum} < 0 \wedge \varepsilon_t^p < 0 \wedge P_t^{IMSP} > P_t^{DAM} \\ 0, \end{cases}, (2)$$

де ε_t^p – враховане відхилення виробника p в годину t;
ε_t^{sum} – сумарний небаланс балансуючої групи гарантованого покупця;
P_t^{DAM} – ціна на електричну енергію яка склалась на ринку «на добу наперед» для години t;
P_t^{IMSP} – ціна небалансів сформована за результатами торгів на балансуючому ринку для години t;
S_t^ε – сумарне відхилення учасників балансуючої групи, відхилення фактичного споживання від прогнозного яких співпадає за знаком з небалансом всієї балансуючої групи:

$$S_t^\varepsilon = \sum\nolimits_p \left\{ \varepsilon_t^{sp} | \varepsilon_t^{sp} \cdot \varepsilon_t^{sum} > 0 \right\}.$$

Для розрахунку S_t^ε використовуються фактичні відхилення $\varepsilon_t^{sp} = \sum_{u \in p} (W_t^{up} - PR_t^{up})$, а не враховані.

Формула (2) відображає логіку пропорційного розподілу витрат на покриття небалансів між його «винуватцями». З неї випливає, що відшкодовують вартість небалансів тільки ті виробники, відхилення яких збігаються за знаком з загальним відхиленням всієї балансуючої групи, що додатково ослаблює стимули до прогнозування та встановлення систем накопичення електричної енергії. Застосування формули (2) додатково суттєво знижує імовірність плати виробників ВДЕ за небаланс. В той же час відповідальність за небаланс учасників ринку які оперують напряму на оптовому ринку електричної енергії (постачальники, трейдери тощо) розраховується для кожного учасника ринку окремо.

Враховуючи суттєву нерівномірність розподілу встановленої потужності, більше 1500 МВт (29%) встановленої потужності припадає на 20 станцій (3,6%), у великих виробників з'являється можливість маніпулювати виплатами інших учасників ринку, що може ускладнювати розвиток малої розосередженої генерації. В таких умовах оптимальною стратегією для великих виробників може виявитись не підвищення точності прогнозу, а маніпуляція їх значенням. Враховуючи, що «зелений» тариф є формою субсидіювання виробників з ВДЕ за рахунок кінцевих споживачів, метою якої є зниження забруднення навколишнього середовища, цілком виправданим було б посилення відповідальності за небаланси виробників з ВДЕ.

Одним із шляхів подолання такої ситуації є стимулювання розвитку ВДЕ на основі «зелених» аукціонів за якими переможець може розраховувати на гарантований викуп відпущеної електроенергії протягом 20 років. При

цьому максимально можливою ціною є поточний «зелений» тариф. Це дасть змогу знизити фінансове навантаження на інших учасників ринку та кінцевих споживачів. В рамках даного механізму для переможців аукціону повна відповідальність за власний небаланс настає після визнання внутрішньодобового ринку ліквідним, але не пізніше ніж з 1 січня 2024 р.

Іншим напрямком зменшення негативного впливу ВДЕ на ринкові та технологічні процеси функціонування ОЕС України є впровадження систем прогнозування, що може дати суттєвий економічний ефект. За результатами виконаних досліджень [6] та виконаних розрахунків, впровадження системи прогнозування сумарного відпуску електричної енергії виробниками, що входять в балансуючу групу гарантованого покупця, з використанням розробленої в Інституті електродинаміки НАН України нейронної мережі eResNet, дає можливість ввести в експлуатацію додатково від 900 до 2000 МВт встановленої потужності електростанцій з ВДЕ при поточній кількості маневрових потужностей. Впровадження та подальше вдосконалення таких систем за рахунок включення метеорологічної інформації та збільшення кількості доступних для навчання даних дасть можливість підвищити допустимі значення встановленої потужності ВДЕ за рахунок підвищення точності прогнозу відпуску електроенергії такими виробниками.

[1] Закон України «Про ринок електричної енергії» від 13.04.2017 №2019-VIII.

[2] Порядок купівлі гарантованим покупцем електричної енергії, виробленої з альтернативних джерел енергії. Постанова НКРЕКП 26 квітня 2019 року N 641 у редакції постанови НКРЕКП 13 грудня 2019 року N 2802.

[3] Постанова Кабінету Міністрів України від 5 червня 2019 р. № 483 в редакції постанови Кабінету Міністрів України від 9 грудня 2019 р. № 1003.

[4] Блінов І.В., Парус Є.В., Іванов Г.А. Імітаційне моделювання функціонування балансуючого ринку електроенергії з урахування системних обмежень на параметри ОЕС України // Технічна електродинаміка. 2017. №6. С.72 – 79.

[5] Блінов І.В., Попович В.І. Гармонізована рольова модель європейського ринку електроенергії. Проблеми загальної енергетики. 2011. № 3(26). С. 5 – 11.

[6] Блінов І.В., Мірошник В.О., Шиманюк П.В. Короткостроковий інтервальний прогноз сумарного відпуску електроенергії виробниками з відновлювальних джерел енергії // Праці Інституту електродинаміки НАН України. Вип. 54: 5-12, 2019.

[7] Кириленко О.В., Блінов І.В., Парус Е.В. Визначення результатів аукціону з купівлі-продажу електричної енергії. Проблеми загальної енергетики. 2010. № 3. С. 5 – 12.

[8] Blinov I.V., Parus E.V., Ivanov G.A. Complex calculation model of the day-ahead and balancing market of Ukraine // Promelectro – 2016. – No 4-5. – С. 8 – 12.

М.Ю. Комаров, А.В. Ониськова, С.Ф. Гончар, В.В. Ткаченко, С.М. Сергєєв

РОЗРОБКА БАЗИ ДАНИХ КІБЕРЗАГРОЗ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Загальна картина, що характеризує порушників та зловмисників в області комп'ютерної безпеки, змінюється з часом, але загальні категорії загроз та небезпек залишаються незмінними [1]. Для того щоб зірвати плани атакуючих зловмисників проводяться відповідні дослідження, тому завжди важливо правильно класифікувати різні типи реально існуючих атак [2].

База даних кіберзагроз об'єктів критичної інформаційної інфраструктури (далі – БД) призначена для використання в автоматизованій системі розпізнавання несанкціонованого впливу на режими роботи об'єктів критичної інфраструктури. Кластерна структура бази даних орієнтована на зберігання параметрів елементів та об'єктів об'єднаної енергосистеми, розрахункових параметрів режиму і інформації, отриманої від SCADA (існуючі системи управління і збору інформації) і EMS (Energy Management System) в реальному часі.

Запропонована модель бази даних побудована на основі СУБД ORACLE з використанням її системи управління доступом [3] та механізмів безпеки [4].

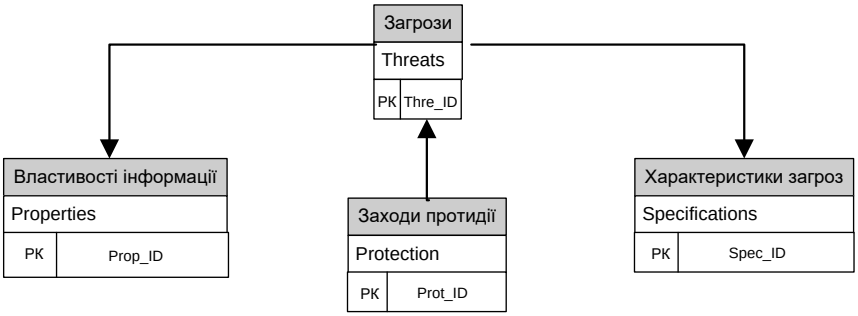
Нижче наведені приклади суттєвостей таблиць бази даних.

Тип	Кіберзагроза
Threat	Spoofing
Specifications	Кількість виявлених IP-адрес у спам-базах
Specifications	Кількість спам-слів у темі
Specifications	Кількість спам-слів в повідомленні
Properties	Цілісність
Properties	Доступність
Properties	Спостережність
Protection	Налаштування управління доступом
Protection	Додаткова автентифікація (одноразовий пароль, криптографічна автентифікація)

Тип	Кіберзагроза
Threat	Denial-of-Service, DoS
Specifications	Кількість одночасних підключень до серверу
Specifications	Кількість пакетів з однаковою адресою відправника та отримувача
Specifications	Швидкість обробки запитів
Specifications	Затримка між запитами від одного користувача
Properties	Доступність

Properties	Спостережність
Protection	Аналіз трафіку
Protection	Блокування шкідливих IP-адрес
Protection	Фільтрація трафіку
Protection	Адекватні апаратні потужності та канали зв'язку

Структура бази даних кіберзагроз об'єктів критичної інформаційної інфраструктури наведена нижче.



Фізичні характеристики логічних атрибутів

№	Назва атрибуту	Фіз. формат	Переклад назви атрибуту
1.	Threats	TXT	Назва загрози
2.	Properties	TXT	Властивості інформації
3.	Protection	TXT	Заходи протидії
4.	Specifications	TXT	Назва типу документу
5.	Thre_ID	BINARY	Ідентифікатор загрози
6.	Prop_ID	BINARY	Ідентифікатор властивості інформації
7.	Prot_ID	BINARY	Ідентифікатор заходу протидії
8.	Spec_ID	BINARY	Ідентифікатор характеристики загрози

[1] Чио К., Фримен Д. Машинное обучение и безопасность / пер. с анг. А.В. Снастина. – М.: ДМК Пресс, 2020, 388 с.
[2] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view.
[3] М. Комаров, «Підсистема управління доступом системи управління базами даних ORACLE DATABASE 12C ENTERPRISE EDITION», Моделювання та інформаційні технології, №84, С. 87-96, 2018.
[4] М. Комаров, С. Гончар, «Аналіз механізмів безпеки системи управління базами даних Oracle Database 12C enterprise Edition», Моделювання та інформаційні технології, №85, С. 107-116, 2018.

І.С. Зінов'єва, Н.В. Ситник

ПІДХОДИ ДО ІНТЕГРАЦІЇ РОЗПОДІЛЕНИХ ДАНИХ НА БАЗІ POLYSTORE

Сучасні інформаційні системи в енергетичній сфері є досить складними (з архітектурної, технологічної, онтологічної та інших точок зору) системами, що не в останню чергу, обумовлено складністю й варіативністю оброблюваних даних. На даний час електроенергетичні системи в більшості країн світу реалізовані шляхом глибокої інтеграції електроенергетичних мереж та комп'ютерних й телекомунікаційних мереж та використання високопродуктивних розподілених середовищ (грід-систем, хмарних платформ). У цих системах у режимі реального часу продукується неймовірно великий обсяг інформації різнорідної за своїм змістом, формою, семантикою, рівнем структурованості, ступенем значущості. Зазначене призводить до того, що навіть в межах однієї інформаційної системи доводиться для зберігання даних і вирішення різних завдань по їх обробці використовувати кілька різних систем управління базами даних (скорочено – СУБД), кожна з яких підтримує свою модель даних. Детальний огляд наявних моделей даних та СКБД можна знайти у працях [1-2].

Проблема оброблення сукупності структурованої та неструктурованої інформації у великих розподілених інформаційних системах полягає у пошуку варіантів спільного використання різних типів баз даних та моделей їх представлення. Тобто, завдання полягає у створенні певного єдиного середовища, яке б створювало умови для спільного доступу до розподілених баз даних, що функціонують на базі різних моделей представлення даних. У закордонній літературі підхід, згідно з яким забезпечується використання кількох різноманітних баз даних в рамках єдиної інформаційної системи отримало назву «polyglot persistence» [3], а сукупність різнорідних баз даних, що підтримують обрані моделі представлення даних у межах єдиного цифрового середовища – мультисховищ (polystore databases, hybrid databases).

У першому наближенні можна виділити два ключові підходи до розв'язання проблеми спільного використання різнорідних даних:

1) підхід «зверху вниз» передбачає створення єдиних платформ для інтеграції розподілених даних із різних типів баз даних. Тут можна виділити наступні способи: розробка та використання інтегрованих платформ для спільного використання даних різного типу (наприклад, Apache Hadoop, хмарні платформи); використання багатомодельного підходу (multi-model databases), в рамках якого використовується єдиний інтегрований сервер, який забезпечує підтримку кількох типів моделей даних (наприклад, Oracle Berkeley DB або Microsoft Azure Cosmos DB); використання спеціальних архітектурних рішень, у т.ч. – сервіс-орієнтованої архітектури (SOA);

2) підхід «знизу вгору» передбачає використання певного проміжного програмного забезпечення, зокрема: посередників (mediators) – для

семантичної інтеграції даних шляхом уніфікування метаописів джерел даних; адаптерів (wrappers) із використанням технологій CORBA, які забезпечують зв'язок із включеними базами даних через процедуру віддаленого виклику (RPC); ORM- та ODM-бібліотек; конверторів даних (наприклад, у формати XML, JSON).

Кожен із цих підходів має як сильні, так і слабкі сторони. Наприклад, досить перспективним для інтеграції розподілених даних із різних типів баз даних видається використання SOA, в межах якої доступ до даних відбувається через інтерфейс відповідного сервісу, а сама інформаційна система розбивається на окремі більш-менш незалежні модулі. Однак, цей підхід вимагає значних матеріальних витрат на організацію взаємодії між сервісами, а тому доцільність його використання у невеликих проектах та малорентабельному бізнесі – сумнівна. Для «згладжування» різниць між базами даних та інтеграції даних можна створити рівень абстракції, який забезпечить переоформлення запитів до бази даних та уніфікує інтерфейс доступу до різнотипних даних. Існує ряд готових рішень та підходів для об'єктно-реляційного (Object-Relation Mapping – ORM) та об'єктно-документального представлення (Object-Document Mapping – ODM), які забезпечують управління життєвим циклом об'єктів, високий рівень абстракції від «батьківських» баз даних, виконання запитів в уніфікованих термінах. Однак, використання ORM- та ODM-бібліотек є малоефективним в розподілених інформаційних системах, оскільки істотно знижує продуктивність та швидкість обробки даних.

Проведений аналіз показав, що не існує універсального інструментарію для інтеграції розподілених даних із різних типів баз даних, кожен підхід та спосіб має свої обмеження. Однак, обирати в якості ядра інформаційної системи якусь конкретну СКБД із підтримкою певної моделі представлення даних також не варто, потрібно обирати такий інструментарій інтеграції даних, який би забезпечив розв'язання поставлених задач з урахуванням конкретних обстави та наявних ресурсів. Разом із тим, можемо говорити, що на даний час більш гнучким та поширеним у сфері інтеграції даних із різних типів баз даних у єдиному цифровому середовищі є підхід знизу вгору» і використання різного роду проміжного програмного забезпечення.

[1] І.С. Зінов'єва, В.О. Артемчук, «Сучасні підходи до подальшої еволюції концепції баз даних», in III International scientific and practical conference «Dynamics of the development of world science», Canada, 2019, pp. 34–44.

[2] N.V. Sytnyk, I.S. Zinovieva, «Evolution of the concept of database organization in the context of the digitalization of society», на II Національній науково-методичній конференції «Цифрова економіка», Київ, 2019, с. 150-153.

[3] Pramod J. Sadalage, Martin Fowler, «Introduction to Polyglot Persistence: Using Different Data Storage Technologies for Varying Data Storage Needs», InformIT, #5, 2012. [Online]. Available: https://www.informit.com /articles/article.aspx?p=1930511. Accessed on: April 21, 2020.

В.О. Артемчук[1,2], А.В. Яцишин[2], О.О. Попов[1,2], А.В. Яцишин[1,2]

ЗАСТОСУВАННЯ СПЕЦІАЛІЗОВАНИХ ГЕОІНФОРМАЦІЙНИХ СИСТЕМ ДЛЯ НАВЧАННЯ КОМП'ЮТЕРНОГО МОДЕЛЮВАННЯ МАЙБУТНІХ PhD

[1] Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Київ
[2] ДУ «Інститут геохімії і навколишнього середовища НАН України», Київ

Підвищення якості освіти є одним із важливих питань розвитку українського суспільства. Сучасний світ еволюціонує та змінюється швидкими темпами, відбувається оновлення та удосконалення інформаційних технологій, а тому вітчизняна система вищої освіти не встигає із адаптацією навчальних програм та планів до вимог ринку та цифрового суспільства. Актуальною ця проблема є у сфері підготовки майбутніх PhD за спеціальностями: 101 «Екологія», 103 «Науки про Землю», 122 «Комп'ютерні науки», 183 «Технології захисту навколишнього середовища».

Для України питання розробки та впровадження геоінформаційних систем (ГІС) є актуальним, про що наголошено в ряді нормативно-правових документів. Також, нині від закладів вищої освіти та наукових установ вимагається посилення геоінформаційного вектору навчання своїх студентів і аспірантів, зокрема, використання в навчальній практиці сучасних ГІС та програмного забезпечення, що максимально задовольняло б навчальним цілям та формуванню професійних компетентностей фахівців. Проте, нині обґрунтованість використання конкретного програмного забезпечення в навчальному процесі обумовлюється знаннями та досвідом викладача, який викладає навчальні дисципліни із застосуванням ГІС. Тому, важливим у навчальному процесі є формування навичок роботи у майбутніх PhD як з пропрієтарними, так і з відкритими й спеціалізованими ГІС. Це значно збагатить їх практичний досвід та дасть змогу зрозуміти механізм перетворень геопросторових даних незалежно від виду чи типу ГІС.

ГІС-спеціалісти мають володіти системними знаннями і навичками роботи в області проектування, експлуатації та розвитку ГІС. ГІС-освіта спрямована на: комплексне вирішення природно-економічних і соціальних задач; засвоєння нових методів і засобів обробки даних, які забезпечують високу наочність відображення різнорідної інформації, обробки та аналізу просторової інформації; використання сучасних засобів оперативного вирішення задач управління, оцінки і контролю оточуючих процесів [7].

Дослідниками [6] наголошено, що ГІС являють собою вікно в минуле, теперішнє та майбутнє, полегшуючи доступ до інформації, що стосується природних, соціальних та культурних аспектів. Таким чином ГІС стають незамінними, коли мова йде про пізнання, вивчення та якість довкілля. Описано використання Google Earth у екологічній освіті за допомогою

створення дидактичних маршрутів, зроблених студентами Університету Кордови (Іспанія).

Сучасні ГІС мають достатньо широкий комплекс можливостей, але з постійним розвитком технологій та зростанням вимог до інформаційних комплексів завжди є потреба вдосконалювати та ускладнювати геоінформаційні системи, тим самим ускладнюючи розрахунки, збільшуючи кількість операцій на одиницю часу, отримуючи тим самим більшу точність та достовірність результатів. Більшість сучасних ГІС здійснюють комплексну обробку інформації, використовуючи такі функції: введення і редагування даних, підтримка моделей просторових даних, зберігання інформації, перетворення систем координат і трансформація картографічних проекцій, растрово-векторні операції, вимірювальні операції, полігональні операції, операції просторового аналізу, різні види просторового моделювання, цифрове моделювання рельєфу та аналіз поверхонь, подання результатів у різних формах, а також багато різних специфічних, залежно від призначення системи, функцій моделювання. Визначення максимального переліку вимог до ГІС сьогодні є одним із найважливіших кроків у моделюванні таких систем. Геообробка – це ключове середовище для моделювання та аналізу геоданих. За допомогою цього середовища можна синтезувати дані, які неможливо отримати із тих чи інших джерел [10].

Геоінформаційне моделювання – це високотехнологічний процес створення моделі місцевості певної території в середовищі геоінформаційних систем. Створена модель візуалізує кількісні та якісні параметри модельованої місцевості, відображає інтенсивність протікання процесів (наприклад гідрологічних, технологічних), дає об'єктивну оцінку стану об'єкта (міського середовища, окремих компонентів природного довкілля, господарської діяльності людини тощо). Зазвичай геоінформаційне моделювання виступає інструментом прийняття рішення при розробці рекомендації щодо оптимізації природокористування, містобудівної діяльності, зменшення деструктивних антропогенних впливів на довкілля, попередження виникнення техногенних інцидентів та розвитку небезпечних явищ і процесів [2].

Із застосуванням ГІС можливо інтегрувати, на просторових засадах різноманітні дані, необхідні в процесі прийняття рішень: характеристики викидів забруднювальних речовин (ЗР) у регіоні; регіональні географічні, соціально-економічні, екологічні та медико-епідеміологічні характеристики. Поширеним є використання ГІС для відображення та аналізу полів забруднення на електронних картах. З погляду візуалізації інформації геоінформаційні системи цікаві тим, що забезпечують візуальне зображення багатовимірної екологічної інформації. Це дуже зручно в ході оцінювання екологічних ризиків та інформування осіб, що ухвалюють рішення. Отже, можна виділити головні можливості ГІС, які використовують у задачах управління якістю довкілля: 1) підготовка даних для аналізу та моделювання. ГІС використовують як для одержання і систематизації інформації (стосовно джерел емісії ЗР, характеристик поверхні), так і для аналізу, трансформації з

залученням потужних інструментів відображення даних; 2) просторовий аналіз і моделювання розподілу або змін об'єктів і процесів, які вивчають; 3) публікація результатів, що, по суті, є процесом формування процедури, за якої результати розрахунків та аналітичних досліджень перетворюються у зрозумілі користувачеві тематичні карти, де виявлені в процесі аналізу закономірності відображені якнайкраще в доступній для особи формі, що приймає рішення [8].

Комп'ютерне моделювання в задачах екологічного моніторингу. Для того щоб продемонструвати приклади роботи ГІС необхідно підготовити ряд моніторингових даних. Застосовуючи ГІС у задачах екологічного моніторингу можна стежити за станом довкілля, моделювати та відображати рівні забруднення, прогнозувати виникнення надзвичайних екологічних ситуацій, визначати зони з найбільшими концентраціями і території ризиків для здоров'я населення, інформувати населення про поточний екологічний стан навколишнього середовища, динаміку його змін, джерела забруднення, розміщення відходів, характер впливу екологічних факторів на здоров'я людей, забезпечивши вільний доступ до екологічної інформації [3].

Для того щоб моніторингові дані знаходили практичне використання, вони мають бути представлені відповідним чином. Лише вузька група фахівців, які займаються моніторингом якості довкілля або модельними оцінками, здатна скористатись необробленими даними, а не особи, котрі ухвалюють рішення, або широка публіка. Інтерпретація просторово-часової мінливості забруднення в багато чому полегшується, якщо звичні цифрові дані представити у вигляді графіків, рисунків та карт [3]. Використання географічних карт значно полегшує процес представлення складніших порівняльних характеристик забруднення. Концентрації забруднення для різних пунктів спостереження можна продемонструвати простим способом.

Наразі, для вирішення завдань екологічного моніторингу приземного шару атмосфери, застосовують вітчизняні та закордонні інформаційні програмно-моделюючими системами, а саме: EOL-2000[h], «Повітря», EcoStat, «ÉPK ROSA», «ÉRA-Vozdukh», UPRZA «Ékoloh», «HYS – atmosfera», «Mahystral′-horod 2.3», «RADExpert», RODOS, RECASS, NOSTRADAMUS, JSPEEDI, ARGOS, MEPAS, NARAC та ін. [4].

Важливим практичним аспектом є використання для підготовки майбутніх PhD, розробленого авторами даної публікації, інформаційно-програмного забезпечення для вирішення задач моніторингу та контролю екологічного стану урбанізованих територій – системи AISEEM.

Система AISEEM включає блок статистичного аналізу й попередньої оцінки техногенних навантажень на атмосферне повітря; блок математичного моделювання та прогнозування рівнів забруднення атмосфери і ризиків для населення; блок візуалізації та побудови екологічних карт [1]. Оскільки дана система має в наявності блок побудови електронних карт та ряд засобів для роботи з ними, а також відповідає певним характеристикам до ГІС, тому можна вважати її спеціалізованою ГІС. Розроблене інформаційно-програмне забезпечення спрямоване на вирішення багатьох наукових та практичних

задач екологічного моніторингу приземного шару атмосфери, що описані в публікаціях [3], [9], [12]. Нині систему AISEEM впроваджено в різних організаціях та підприємствах, а також в кількох закладах вищої освіти.

До прикладу, систему AISEEM можливо застосувати для моделювання різних навчальних задач (Задача 1. Моделювання техногенних навантажень на атмосферу за тривалий період часу. Задача 2. Оцінювання ризиків для здоров'я населення за техногенним атмосферним фактором) під час підготовки майбутніх PhD за спеціальностями: 101 «Екологія», 103 «Науки про Землю», 122 «Комп'ютерні науки», 183 «Технології захисту навколишнього середовища».

Отже, проведене дослідження показало, що нині інформаційні матеріали, які створені на базі ГІС, а також геоінформаційні знання та навички стають все більш затребуваними. Однак, підготовка майбутніх фахівців нової технологічної ери залишається на рівні, що не повною мірою задовольняє потреби виробництва, наукової та управлінської сфери [5]. Наголосимо, що далеко не усі освітні програми закладів вищої освіти і наукових установ, які здійснюють підготовку майбутніх PhD включають вивчення ГІС. А це на думку авторів даної публікації, є значним недоліком, оскільки, вміння застосовувати ГІС має міждисциплінарний характер, зокрема, розвиває знання і навички з комп'ютерного моделювання різних процесів, що можуть виникати у подальшій професійній діяльності.

[1] Andrii Iatsyshyn, Anna Iatsyshyn, Volodymyr Artemchuk, Iryna Kameneva, Valeriia Kovach and Oleksandr Popov. Software means for tasks of sustainable development of environmental problems: peculiarities of programming and implementation in the specialists` preparation. E3S Web of Conferences 166, 01001 (2020). https://doi.org/10.1051/e3sconf/202016601001.

[2] Geoinformation modeling. https://magneticonemt.com/en/geoinformation-modeling.

[3] Iatsyshyn, A.V., Popov, O.O., Kovach, V.O., Artemchuk, V.O.: The methodology of future specialists teaching in ecology using methods and means of environmental monitoring of the atmosphere's surface layer. Information Technologies and Learning Tools 66(4), 217–230 (2018). doi:10.33407/itlt.v66i4.2233

[4] Iatsyshyn, A.V., Popov, O.O., Kovach, V.O., Artemchuk, V.O.: The methodology of future specialists teaching in ecology using methods and means of environmental monitoring of the atmosphere's surface layer. Information Technologies and Learning Tools 66(4), 217–230 (2018). doi:10.33407/itlt.v66i4.2233.

[5] Iatsyshyn, Anna V., Kovach, V.O., Romanenko, Ye.O., Deinega, I.I., Iatsyshyn, Andrii V., Popov, O.O., Kutsan, Yu.G., Artemchuk, V.O., Burov, O.Yu., Lytvynova, S.H.: Application of augmented reality technologies for preparation of specialists of new technological era. In: Kiv, A.E., Shyshkina, M.P. (eds.) Proceedings of the 2nd International Workshop on Augmented Reality in Education (AREdu 2019), Kryvyi Rih, Ukraine, March 22, 2019, CEUR Workshop Proceedings 2547, 181–200. http://ceur-ws.org/Vol-2547/paper14.pdf (2020).

[6] Jorge Alcántara, Silvia Medina. Quintana The use of Educational Itineraries (GIS) in Environmental Education. Enseñanza de las ciencias, 37-2 (2019), 173-188 doi:10.5565/rev/ensciencias.2258

[7] Lyudmila Datsenko. Expansion of geographic information components in the educational programs of cartographers at Taras Shevchenko National University of Kyiv. The Problems of Continuous Geographical Education and Cartography, 2017, №. 25. С. 20-23. https://periodicals.karazin.ua/pbgok/article/view/9080/8603

[8] Nochvay V., Kryvakovska R., Ishchuk O. Use of GIS in the problems of air quality management. Electronics and information technologies. 2012. Issue 2. P. 154–163.

[9] Popov, O.O., Iatsyshyn, A.V., Kovach, V.O., Artemchuk, V.O., Kameneva, I.P., Taraduda, D.V., Sobyna, V.O., Sokolov, D.L., Dement, M.O., Yatsyshyn, T.M.: Risk Assessment for the Population of Kyiv, Ukraine as a Result of Atmospheric Air Pollution. Journal of Health and Pollution 10(25), 200303 (2020). doi:10.5696/2156-9614-10.25.200303.

[10] Жежнич, П.І., Осика, В.О. Функціональні та структурні вимоги до побудови сучасних географічних інформаційних систем. Інформаційні системи та мережі. 2011, №715, С. 104-113

[11] Підготовка докторів філософії (PhD) в умовах реформування вищої освіти: матеріали Всеукраїнської науково-практичної конференції (Запоріжжя, 5-6 жовтня 2017 р.). Запоріжжя: Запорізький національний університет, 2017. 216 с.

[12] Яцишин А.В., Куцан Ю.Г., Артемчук В.О., Каменева І.П., Попов О.О., Ковач В.О. Принципи та методи управління екологічною безпекою на основі інтелектуального аналізу даних мережі моніторингу атмосферного повітря // Електронне моделювання. 2019. № 4(41). С. 85-101.

А.О. Запорожець

БЕЗПІЛОТНІ ЛІТАЛЬНІ АПАРАТИ ДЛЯ СИСТЕМ МОНІТОРИНГУ В ЕНЕРГЕТИЦІ ТА ЕКОЛОГІЇ

Посилення негативного впливу людини на всі компоненти природного середовища вимагає застосування нових більш ефективних засобів і методів контролю [1]. При цьому разові спостереження не дають уявлення ні про інтенсивність процесів, що відбуваються, ні і про їх динаміку, а іноді і про сам факт негативного впливу. Саме тому останнім часом все більш актуальною стає реалізація систем моніторингу при оцінці стану природних і техногенних об'єктів [2]. Під моніторингом, в даному випадку, розуміють комплексну систему спостережень за станом навколишнього середовища (атмосфери, гідросфери, грунтово-рослинного покриву та ін.) та техногенних об'єктів з метою їх контролю та охорони. При цьому висока оперативність і ефективність контролю може бути забезпечена за рахунок застосування дистанційних методів досліджень, які виконуються на базі безпілотних літальних апаратів (квадрокоптерів) [3]. Своєчасно отримана в результаті систематичного моніторингу інформація, дозволяє приймати обґрунтовані управлінські рішення в області експлуатації природних і техногенних об'єктів.

На даному етапі розвитку безпілотних літальних апаратів (БПЛА) вже можна виділити окремий клас квадрокоптерів, що можуть бути використані для створення комплексних систем моніторингу енергетичних об’єктів. Це квадрокоптери серійного виробництва вартістю до 1000$ та вантажопідйомністю від 250 грам. Типовими задачами для таких квадрокоптерів є фото- та відеозйомка, а їх відмінною особливістю є наявність спеціального підвісу для камери, який може бути використаний для кріплення різних пристроїв і сенсорів. До таких квадрокоптерів можна віднести наступні: MJX X101, Syma X8HG, MJX BUGS 3, Cheerson CX-20, Hubsan X4 Pro H109S, Xiro Explorer G, 3DR Solo, GoPro Karma. Нижче приведено фото деяких моделей (рис. 1) та таблиця порівняння технічних характеристик представлених квадрокоптерів (табл. 1).

Квадрокоптери дозволяють ефективно підвищити рівень безпеки периметра електростанції і окремих об'єктів інфраструктури. Регулярний моніторинг із застосуванням безпілотників дозволяє контролювати проведення робіт на території електростанцій, дистанційно здійснювати розвідку місцевості і прилеглих територій, виявляти перебування сторонніх осіб і транспортних засобів. Квадрокоптери, оснащені блоком детектування гамма-випромінювання, дозволяють проводити розвідку радіаційного забруднення місцевості. Дані розвідки можуть передаватися з борта квадрокоптера на наземну станцію управління в режимі реального часу.

а) б)

Рис. 1. Зовнішній вигляд квадрокоптерів для створення систем моніторингу в енергетиці та екології: а) GoPro Karma; б) MJX BUGS 3

Таблиця 1. Порівняння технічних характеристик квадрокоптерів

Квадрокоптер	Час польоту, до хв	Дальність управління, до м	Підтримка висоти	Камера в комплекте	FPV	Ціна, від $
MJX X101	10	100	-	-	-	74
Syma X8HG	7-12	70	+	8Мп	-	120
MJX BUGS 3	8-19	500	-	-	-	119
Cheerson CX-20	15	1000	+	-	-	250
Hubsan X4 Pro H109S	25	1000	+	FHD	5,8 ГГц	390
Xiro Explorer G	25	800	+	-	5,8 ГГц (Wi-Fi)	237
3DR Solo	20	1000	+	-	3DR Link secure Wi-Fi network	399
GoPro Karma	20	3000	+	-	5,8 ГГц	1060

Моніторинг високовольтних ЛЕП з використанням квадрокоптерів дозволяє швидко і ефективно оцінювати технічний стан об'єктів у важкодоступних і віддалених місцях, стан опор та ізоляторів, рівня провисання проводів і висоти рослинності навколо ЛЕП, і дозволяє проводити раннє виявлення загроз та акти діяльності сторонніх осіб в охоронних зонах.

Тепловізіонная зйомка за допомогою БПЛА дозволяє виявляти зони витоку теплової енергії і погану ізоляцію.

Дані, отримані за допомогою квадрокоптерів дозволяють фахівцям оцінювати ризики і прогнозувати вплив природних факторів, обстежити нові маршрути прокладки ЛЕП і прилеглі до них території.

Також актуальним завданням є моніторинг забруднення повітря з

використанням квадрокоптера, що дозволяє оцінити якість повітря на різній висоті, спрогнозувати переміщення полів концентрації забруднюючих речовин та інше.

В роботі [4] наведено значення універсального якісного критерію ефективності (УЯКЕ) для кожного розглянутого квадрокоптера. Згідно з отриманими результатами, квадрокоптери можна розділити на 2 групи: з відносно низьким УЯКЕ (в межах від 6 до 7) і відносно високим УЯКЕ (в межах від 8 до 9). Максимальне значення УЯКЕ не має жоден з розглянутих квадрокоптерів. До групи з відносно низьким УЯКЕ потрапили такі моделі як: MJX X101, Syma X8HG, MJX BUGS 3, Cheerson CX-20. Дані квадрокоптери характеризуються відносно дешевою вартістю - від 75 до 250 $. До групи з відносно високим УЯКЕ потрапили такі моделі як: Hubson X4 Pro H109S, Xiro Explorer G, 3DR Solo, GoPro Karma. Дані квадрокоптера характеризуються відносно високою вартістю - від 250 до 1000 $.

Безумовно, для різних завдань моніторингу один з розглянутих параметрів може бути критично важливий [5]. В такому випадку, квадрокоптер з таким параметром повинен бути використаний. Однак, на підставі проведеного аналізу можна зробити висновок, що квадрокоптер MJX BUGS 3 має найвищу оцінку УЯКЕ серед розглянутих квадрокоптерів серед недорогого сегмента ринку. Його застосування для задач моніторингу в сфері енергетики та екології є обґрунтованим.

[1] Апаратно-програмне забезпечення моніторингу об’єктів генерування, транспортування та споживання теплової енергії / [В.П. Бабак, С.В. Бабак, В.С. Берегун та ін.; за ред. чл.-кор. НАН України В.П. Бабака]. – К., Ін-т технічної теплофізики НАН України, 2016. – 352 с.

[2] Теоретичні та прикладні основи економічного, екологічного та технологічного функціонування об’єктів енергетики / [В.О. Артемчук, Т.Р. Білан, І.В. Блінов та ін.; за ред. А.О. Запорожця, Т.Р. Білан]. – Київ, 2017. – 312 с.

[3] Солоха М.А. Використання безпілотників при вирішенні екологічних задач / М.А. Солоха // Вісник ХНУ імені В.Н. Каразіна. Серія «Екологія». – 2013. – №1070. – Вип. 9. – С. 84-90.

[4] Zaporozhets A.O. Review of quadrocopters for energy and ecological monitoring / A.O. Zaporozhets // Systems, Decision and Control in Energy I. Studies in Systems, Decision and Control. – 2020. – vol. 298.

[5] Popov O. Risk Assessment for the Population of Kyiv, Ukraine as a Result of Atmospheric Air Pollution / O. Popov, A. Iatsyshyn, V. Kovach, V. Artemchuk, I. Kameneva, D. Taraduda, V. Sobyna, D. Sokolov, M. Dement, T. Yatsyshyn // Journal of Health and Pollution. – 2020. – vol. 10. – №25. – 200303.

А.В. Малєй

ЗАСТОСУВАННЯ МЕТОДІВ ЕКСПЕРТНИХ ОЦІНОК ДЛЯ СИСТЕМ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ

Досить часто системи підтримки прийняття рішень для покращення якості діяльності потребують залучення певної групи компетентних спеціалістів, що володіють досвідом у необхідній галузі: управління, енергетика, промисловість, медицина [1].

Одним із вирішенням даної проблеми може бути застосування методів експертних оцінок.

Таким чином, метою роботи є проведення аналізу існуючих методів експертних оцінок, що можуть бути ефективно застосовані для систем підтримки прийняття рішень та інформаційно-аналітичних систем.

Експертне оцінювання – процес оцінки будь-чого, що базується на думках експертів, з метою подальшого прийняття рішення чи вибору[2].

Існує два типи експертних оцінок:

- індивідуальні оцінки, що базуються на використанні тверджень окремих експертів;
- колективні оцінки, що базуються на використанні колективних думок експертів.

В загальному випадку саме колективні оцінки демонструють більшу точність, ніж індивідуальні.

Розрізняють наступні методи експертних оцінок.

- Метод асоціацій. Базується на вивченні схожого за властивостями об'єкта з іншим об'єктом.
- Метод парних (бінарних) порівнянь. Базується на зіставленні експертом альтернативних варіантів, з яких треба вибрати ті, що найкраще підходять.
- Метод векторів переваг. Експерт аналізує весь набір альтернативних варіантів і обирає ті, що найкраще підходять.
- Метод фокальних об'єктів. Заснований на перенесення ознак випадково відібраних аналогів на досліджуваний об'єкт.
- Індивідуальний експертне опитування. Опитування у формі інтерв'ю або у вигляді аналізу експертних оцінок.
- Метод середньої точки. Створюються два альтернативних варіанти вирішення, один з яких менш вдалий. Після цього експерт повинен підібрати третій альтернативний варіант, оцінка якого розташована між значеннями першої і другої альтернативи.

Підхід з використанням експертних оцінок дозволяє вирішувати завдання, що не піддаються вирішенню звичайним аналітичним способом, зокрема:

- Вибір найкращого варіанта рішення серед наявних.
- Прогнозування розвитку процесу.

- Пошуку можливого рішення складних завдань.

Загальними вимогами для кількісних та якісних оцінок виступають:

1. Об’єктивність та достатність вихідної інформації.
2. Порівняльний характер оцінок.
3. Можливість класифікації характеру оцінки за декількома критеріями.
4. Визначення мінімальної та достатньої кількості критеріїв оцінки.

В роботі [3] наведено детальний опис предметного середовища, для якого можливе ефективне застосування підходів, описаних в даній статті.

[1] Карпов А.И. Психология групповых решений – М.: Юрист.2008.-55 с.
[2] Орлов А. И. Экспертные оценки. Учебное пособие. М.: ИВСТЭ, 2002
[3] В. З. Стецюк, А. В. Малєй, О. І. Лісовиченко, Н. О. Пічкур , Л. Ю. Бабінцева Особливості розроблення концептуальної математичної моделі процесу раннього діагностування спадкових орфанних захворювань ISSN 1996-1960. Медична інформатика та інженерія. 2018, No 2 -44 - 53 с

Є.В. Болтов

МЕХАНІЗМ НЕБЛОКУЮЧОГО ЗАПИСУ ТА ЗЧИТУВАННЯ ДАНИХ У ВБУДОВАНИХ СИСТЕМАХ З ВИКОРИСТАННЯМ РОЗПОДІЛЕНОЇ ПАМ'ЯТІ

Неблокуючі механізми синхронізації мають значні переваги в порівнянні з синхронізацією на основі блокувань, а саме: мають більшу відмовостійкість, усувають проблеми між синхронізацією та планувальником для систем реального часу, а також, само собою, не блокуються [1]. З поширенням автономних систем та модульного стилю написання програмного забезпечення, стає проблемою об'єднати все в єдиний компонент. Особливо сильно це стосується систем, де дані з датчиків повинні передаватися до багатьох компонентів системи за мінімальний час. Таким чином, було прийняте рішення спроектувати, реалізувати та протестувати на реальній системі власний механізм неблокуючого запису та зчитування даних з використанням розподіленої пам'яті (shared memory). Особливістю спроектованого механізму стала можливість одночасного неблокуючого зчитування даних декількома процесами, але з обмеженням на одночасний запис даних – не більше одного процесу.

При проектуванні механізму, перш за все, було визначено структуру даних. На рис. 1 представлена структурна схема даних, яка буде знаходитися у розподіленій пам'яті. Структура складається з первинного індексу A (далі префікс), вторинного індексу B (далі постфікс), індексу поточного запису INDEX, та записуваних даних DATA.

Рисунок 1. Ілюстрація структури буферу даних

Механізм використовує принцип кільцевого буфера (ring buffer), тому у розподіленій пам'яті зберігається декілька таких структур, їх кількість визначається емпірично, відповідно до швидкодії цільової платформи або специфічних вимог до навантаження. Префікс A та постфікс B використовуються для контролю цілісності даних, тобто захисту, що дана структура не записується у той самий час, коли зчитується. Індекс INDEX використовується для механізму захисту від неактуальної структури даних. Також у розподіленій пам'яті зберігається глобальний індекс поточного запису $INDEX_{global}$, а для задач зчитування відводиться локальний індекс поточного запису $INDEX_{local}$, який зберігається у програмах зчитування.

В роботі було спроектовано та реалізовано механізм, який дозволяє виконувати запис та зчитування даних у розподілену пам'ять, при якому операції запису та зчитування виконуються без блокуючих методів синхронізації. Спрощена імплементація алгоритму запису даних має

наступну послідовність дій (i – поточний буфер даних):

- запис унікального префіксу A_i
- запис індексу буфера $INDEX_i$
- запис даних $DATA_i$
- запис постфіксу B_i (B_i повинен дорівнювати A_i)
- нарощування та атомарний запис глобального індексу $INDEX_{global}$

Спрощена імплементація алгоритму зчитування даних має наступну послідовність дій (i – поточний буфер даних):

- атомарне зчитування глобального індексу $INDEX_{global}$
- перевірка, якщо $INDEX_{local}$ дорівнює $INDEX_{global}$, то нових даних немає
- зчитування префіксу A_i та постфіксу B_i
- перевірка, якщо A_i не дорівнює B_i, то дані ушкоджені
- зчитування індексу буфера $INDEX_i$
- перевірка, якщо $INDEX_i$ не дорівнює $INDEX_{local}$, то дані неактуальні
- зчитування даних $DATA_i$
- повторне зчитування префіксу A_i' та постфіксу B_i'
- перевірка, якщо A_i, B_i, A_i' та B_i', тотожно не рівні, то дані ушкоджені
- нарощування та запис локального індексу $INDEX_{local}$

Повний лістинг реалізованого механізму [3] та програми для тестування [4], доступні в репозиторіях GitHub.

У таблиці 1 надані результати тестування реалізованого механізму. Тестування проводилось на платформі NVIDIA Jetson Nano [2] (без модифікацій ядра). Програма запису даних виконувала запис 10000 буферів даних (оптимізація запису відсутня). Інтервал запису даних був незначно більшим, аніж інтервал зчитування. Це запроваджено для того, щоб програма зчитування даних мала можливість наздогнати програму запису, в випадках, коли було порушено інтервал, або виконувалась повторна спроба читання буферу даних. Усі програми тестування були запущені з використанням пріоритету реального часу (RR 99).

Як можна побачити з таблиці 1, при записі/зчитуванні даних більш ніж 100Кб, з'являються проблеми з перевищенням інтервалів та великою кількістю зайвих спроб читання. Це обумовлено тим, що розмір даних виходить за розміри кешу L2 [2], тому задача запису не встигає у відведений інтервал, а задача зчитування здійснює в цей час спроби читання. У тесті №7, задачі запису та зчитування були синхронізовані, тому зайві спроби зчитування відсутні. Кількість буферів даних обиралася емпірично таким чином, щоб не допустити втрату даних, коли задача запису випереджає задачу зчитування (в термінології кільцевого буфера – голова випереджує хвіст). Щодо середнього навантаження на ядро процесора, то воно прямолінійно залежить від розміру даних та відведеного інтервалу (за умови виходу за рамки кеша процесора).

Таблиця 1

Продуктивність механізму (пріоритет реального часу)

№	Всього спроб зчитування буфера	Інтервал, мкс	Кількість перевищень інтервалу	Розмір даних, байт	Кількість буферів даних	Середнє навантаження на 1 ядро
1	10006	5000	0	1K	10	1,6%
2	10013		0	10K	20	2,0%
3	10003		0	100K	50	5,6%
4	10191		4	1M	100	7,9%
5	10166		12	2.5M	100	16,4%
6	10003	1000	0	1K	10	4,3%
7	10000		0	10K	20	5,9%
8	10193		3	100K	50	8,5%
9	17658		40	1M	100	18,8%
10	42594		126	2.5M	100	19,5%

Перевагою використання запропонованого підходу є можливість зчитувати дані одночасно безліччю задач (обмежуючись продуктивністю цільової платформи), але при цьому накладається обмеження на запис - лише одна задача може записувати дані (декілька за умови використання додаткових підходів, таких як блокування або інші методи синхронізації). Представлений механізм підійде для організації міжпроцесної взаємодії в високонавантажених проектах реального часу, або «м'якого» реального часу.

[1] Blieberger, J., Burgstaller, B. (2018). Safe non-blocking synchronization in Ada2x. In A. Casimiro, & P. M. Ferreira (Eds.), Reliable Software Technologies – Ada-Europe 2018 - 23rd Ada-Europe International Conference on Reliable Software Technologies, Proceedings (pp. 53-69). (Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Vol. 10873 LNCS). Springer Verlag. https://doi.org/10.1007/978-3-319-92432-8_4.

[2] JETSON NANO [Електронний ресурс] // NVIDIA Corporation. – 2020. – Режим доступу до ресурсу: https://www.nvidia.com/ru-ru/autonomous-machines/embedded-systems/jetson-nano/.

[3] Shm non-blocking algorithm [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/exist009/Shm.

[4] Shm non-blocking algorithm performance test [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/exist009/Shm_test.

Ю.В. Маруня

МОДЕЛЮВАННЯ ІНДУКТИВНО-ЄМНІСНОГО ПЕРЕТВОРЮВАЧА З ОДНОФАЗНИМ МОСТОВИМ ВИПРЯМЛЯЧЕМ, АКТИВНИМ НАВАНТАЖЕННЯМ ТА ЄМНІСНИМ ФІЛЬТРОМ

Для нелінійних навантажень, в яких виникає необхідність підтримувати незмінним задане значення струму навантаження незалежно від змін його опору, використовуються індуктивно-ємнісні перетворювачі (ІЄП), в яких реактивні елементи налаштовані на резонанс частоти мережі живлення (рис.1). Актуальність даної тематики показано в [1-3]. В роботі [4] зокрема розглядався Т-подібний ІЄП, що має гарні енергетичні характеристики та покращує показники електромагнітної сумісності навантаження з мережею живлення. Методом математичної теорії планування експерименту був створений ортогональний план другого порядку, за яким проведено ряд експериментів Т-подібного ІЄП з мостовим випрямлячем та активним навантаженням з ємнісним фільтром [4].

Оскільки можливості фізичного макету обмежені у використанні широкого діапазону навантажень, було прийнято рішення створити комп'ютерні імітаційні моделі такої системи - «однофазний симетричний індуктивно-ємнісний перетворювач джерела напруги в джерело струму – мостовий випрямляч з активним навантаженням та ємнісним фільтром» в середовищах MatLab, MicroCap та в спеціалізованій програмі Omega, розробленій в Інституті електродинаміки НАН України.

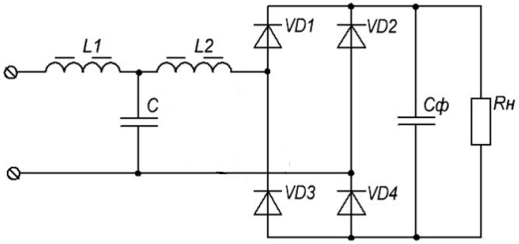


Рис.1

Метою роботи являється перевірити адекватність створених моделей для використання їх в наступних роботах на більших навантаженнях.

Згідно розробленого ортогонального плану в [4], функціями цілі Y_N для порівняння було обрано *THDi* (*Total Harmonic Distortion of input current* – коефіцієнт нелінійного спотворення вхідного струму), $I_н$ та $U_н$ (струм та напруга навантаження). За фактори, що варіюються, обрано: X_1 – відношення ємності $C_ф$ конденсатора фільтра (основний рівень *675 мкФ*, інтервал варіювання *225 мкФ*) до ємності *C* конденсатора *ІЄП* та X_2 – відношення опору навантаження R_H (основний рівень *67 Ом*, інтервал варіювання *43 Ом*) до опору реактора *ІЄП* $x_L = \omega L$, (де *L1=L2=L*). Експеримент проводився за схемою, зображеною на рис. 1, з наступними параметрами: напруга

живлення *230 В*, частота напруги *50 Гц*, потужність навантаження варіювалась від *0,25* до *1кВт*. *ІЄП* виконано по схемі *T1-LCL* з індуктивністю реакторів *L=184 мГн* і ємністю конденсатора *C=50мкФ*. Струм і напруга на виході випрямляча та *THDi* реєструвалися приладом *CA Power Quality Analyzez*. При виконанні імітаційних моделей враховувались також і наступні величини: активний опір, що враховує втрати в обмотках дроселів на нагрівання (*1,04 Ом*) та активний опір діодів в мостовому випрямлячеві (*0,075 Ом*).

Результати експериментальних вимірювань та дані імітаційних моделей, а також матрицю планування кодованих значень факторів (розділ x_i , в якому $x_3' = x_1^2 - 2/3$ та $x_4' = x_2^2 - 2/3$) наведено у таблиці.

На підставі реалізованого ортогонального плану другого порядку було визначено коефіцієнти поліномів b_i по формулі

$$b_i = (\sum_{N=1}^{9} x_{iN} Y_N)(\sum_{N=1}^{9} x_{iN}^2)^{-1}$$

і отримано наступні поліноми для потужності навантаження P_n:

$$P_n = 599{,}78 + 1{,}18x_1 + 308{,}72x_2 + 17{,}37x_1^2 - 44{,}01x_2^2 + 1{,}46x_1x_2 \quad (1)$$

$$P_{n\,Omega} = 676{,}21 + 0{,}25x_1 + 356{,}28x_2 - 2{,}21x_1^2 - 61{,}4x_2^2 + 0{,}97x_1x_2 \quad (2)$$

$$P_{n\,MicroCap} = 595{,}81 - 0{,}008x_1 + 294{,}68x_2 + 2{,}28x_1^2 - 66{,}83x_2^2 + 1{,}01x_1x_2 \quad (3)$$

$$P_{n\,MatLab} = 594{,}71 - 0{,}788x_1 + 294{,}83x_2 - 1{,}22x_1^2 - 64{,}57x_2^2 + 0{,}67x_1x_2 \quad (4)$$

На рис. 2 наведено поверхні відгуку *Pn* (розраховані за формулами 1-4), які дають більш повну картину залежності від факторів x_1 та x_2.

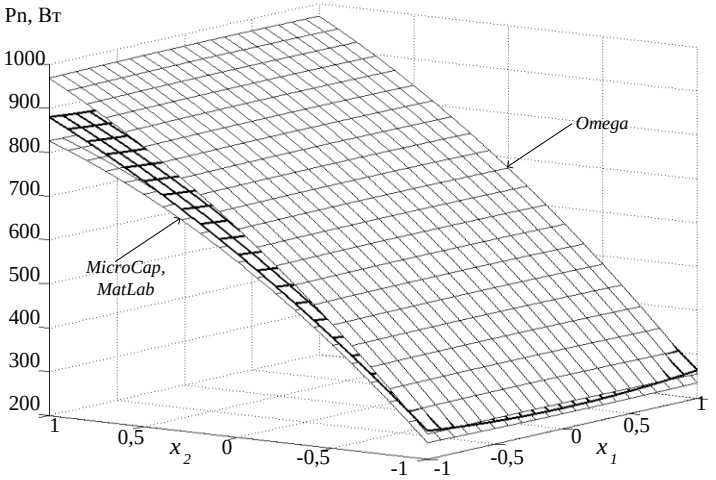


Рис. 2

Таблиця 1

N	x_i						Y_N			$Y_{N\ \text{Omega}}$			$Y_{N\ \text{MicroCap}}$			$Y_{N\ \text{MatLab}}$		
	x_0	x_1	x_2	x_3'	x_4'	$x_1 \cdot x_2$	*THDi*	$I_н$	$U_н$	*THDi*	$I_н$	$U_н$	*THDi*	$I_н$	$U_н$	*THDi*	$I_н$	$U_н$
1	+1	-1	-1	1/3	1/3	+1	2,7	3,33	78	2,28	3,45	74,53	1,9	3,15	75,68	1,89	3,143	75,44
2	+1	+1	-1	1/3	1/3	-1	2,7	3,33	78	2,59	3,452	74,456	2,458	3,13	75,14	1,98	3,121	74,9
3	+1	-1	+1	1/3	1/3	-1	1,4	2,93	304	2,74	3,34	289,31	2,064	2,82	293,1	2,11	2,812	292,48
4	+1	+1	+1	1/3	1/3	+1	1,4	2,93	306	2,10	3,347	289,83	2,115	2,82	293,4	2,13	2,811	292,34
5	+1	-1	0	1/3	-2/3	0	2,0	2,93	208	2,10	3,389	199,176	2,05	2,98	199,9	2,09	2,977	199,575
6	+1	+1	0	1/3	-2/3	0	2,0	2,95	207	2,55	3,39	198,479	2,08	2,99	200,0	2,09	2,976	199,404
7	+1	0	-1	-2/3	1/3	0	3,0	3,33	77	2,84	3,453	74,423	3,368	3,12	74,96	2,35	3,113	74,72
8	+1	0	+1	-2/3	1/3	0	1,5	2,87	293	2,06	3,349	290,388	2,028	2,81	292,4	2,10	2,822	293,5
9	+1	0	0	-2/3	-2/3	0	2,1	3,07	200	2,18	3,397	199,1	2,117	2,99	200,1	2,11	2,977	199,575

Поверхні відгуку *Pn*, дані для розрахунку яких отримано в середовищах *MatLab*, *MicroCap*, практично співпадають та мають меншу розбіжність з експериментальними (на рис. виділено темнішою поверхнею), чим отримані в *Omega*. Згідно [5] для однофазних систем повинно бути *THDi* < 8%, і оскільки варіювання цієї величини в отриманих значеннях (див. табл.) приведеними способами є невелике, то використання всіх імітаційних моделей для визначення коефіцієнту нелінійного спотворення вхідного струму є можливим.

Отже, проведені дослідження показали, що використані імітаційні моделі мають гарну збіжність з експериментальними даними і можуть використовуватися для подальших досліджень.

[1] Волков И.В. Принципы построения и оптимизация схем индуктивно-емкостных преобразователей / И.В. Волков, В.Н. Губаревич, В.Н. Исаков, В.П. Кабан // К: Наукова думка, 1981. 173 с.

[2] Архангельский Н.Л. Электропривод постоянного тока с импульсным преобразователем. /Архангельский Н.Л., Виноградов А.Б. // Учебн. пособ. Иваново: Изд-во Иван. гос. энерг. ун-т., 1995. 92 с.

[3] B. K. Bose. Modern Power Electronics and AC Drives / B. K. Bose. — Prentice Hall PTR, 2002. — 711 p.

[4] Спірін В.М. Якісні характеристики однофазного мостового випрямляча з активним навантаженням та ємнісним фільтром при живленні від джерела струму / Спірін В.М., Губаревич В.М., Маруня Ю.В., Салко С.В. // Технічна електродинаміка. 2020. Вип. 2. С. 23-27.

[5] ДСТУ EN 61000-3-12:2014 Електромагнітна сумісність. Частина 3-12. Норми. Норми на силу струму гармонік, створені обладнанням із номінальним вхідним струмом силою понад 16 А та до 75 А включно на фазу, підключеним до низьковольтних елекропостачальних систем загальної призначеності (EN 61000-3-12:2011, IDT)

А.Л. Березкін

МОДЕЛЬ ФОРМУВАННЯ ЕЛЕКТРОМАГНІТНОГО ПОЛЯ В УМОВАХ ЗАМКНУТОГО ПРОСТОРУ ТА АНАЛІЗ ФАКТОРІВ, ЩО ВПЛИВАЮТЬ НА ЙОГО ФОРМУВАННЯ

В сучасних радіотехнічних засобах досить широко використовують технології передачі та збору інформації на основі багатопроменевого випромінювання, наприклад, пристрої, засновані на радіотехнологіях WiFi, LTE (4G,5G), McWiLL, MIMO, LoRa.

Якщо розглядати більш вузькі аспекти застосування радіоприладів, наприклад у великих громадських будівлях, промислових об'єктах, шахтах, що можна охарактеризувати як замкнуті простори, то умови їх роботи є ще більш складними [1]-[3]. Це пов'язано з явищами багатопроменевого розповсюдження радіохвиль таких як інтерференція, рефракція і дифракція. Що, в свою чергу, призводить до появи інтермодуляційних завад, явища загасання радіосигналу.

Розглянемо математичну модель розповсюдження радіосигналів в умовах замкнутих просторів, що враховує особливості розповсюдження радіохвиль як на засадах оптичних моделей розповсюдження електромагнітних коливань, так і на засадах класичних моделей розповсюдження радіохвиль [4],[5]. На відміну від класичних моделей розповсюдження радіохвиль, які зазвичай базуються на уяві розповсюдження радіохвиль у вільному просторі та з урахуванням рельєфу місцевості у горизонтальній площині, розглянута модель повинна враховувати рельєф поверхні з усіх боків замкнутої поверхні та перешкоди всередині.

На основі моделі розповсюдження радіосигналів в умовах замкнутих просторів, запропонувати вирішення проблеми якісного прийому радіосигналу в цих умовах. На основі аналізу використання радіосистем в умовах промислових підприємств, зокрема шахтах та меткомбінатах, де радіосигнали розповсюджуються в умовах замкнутих просторів, було визначено особливості структури радіоканалів, та особливості прийому радіосигналів в умовах замкнутого простору. Сформовано характеристики радіоперешкод, можливих в умовах замкнутих просторів. Для підтвердження висновків аналізу було проведено декілька експериментів з розповсюдження радіохвиль частотою 868 МГц та 2300 МГц в умовах соляної шахти, конверторного цеху на підприємстві «Азовсталь», та штреках залізорудної шахти. Було встановлено, що електромагнітне поле в умовах замкнутих просторів є результатом багатопроменевого розповсюдження.

Це явище пов'язане з відображенням радіопроменів від навколишніх об'єктів. Ефект багатопроменевого поширення може приводити до ефекту завмирання сигналу або до зрушення частоти основного сигналу, що еквівалентно введенню допплерівської добавки в основний сигнал.

Це також призводить до погіршення якості прийому інформації, що

передається через зсув переданого сигналу щодо ширини смуги приймального фільтра.

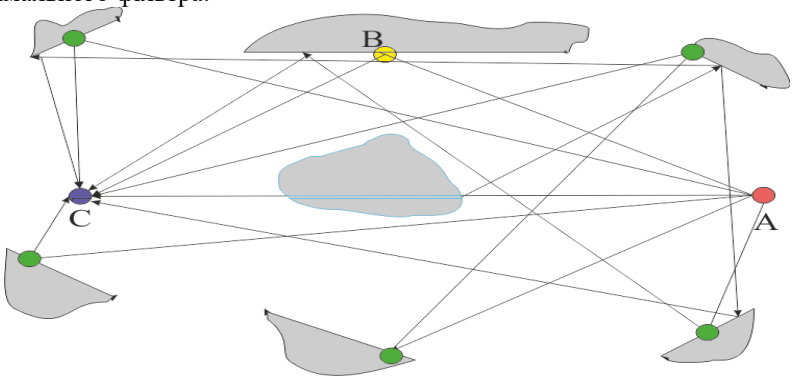


Рис. 1 Формування багатопроменевого розповсюдження радіосигналу.

На основі проведеного аналізу моделей формування електромагнітного поля в замкнутому просторі, запропоновано спиратися на наступні існуючі математичні моделі електромагнітного поля та розповсюдження електромагнітних хвиль:

- Електромагнітне поле $П_{пр}$ у будь який точці простору є результатом суперпозиції віртуальних джерел, рівномірно розповсюджених по сферичній поверхні, що знаходиться навколо джерела випромінювання.
- Електромагнітне поле на краях отвору $П_{отв}$ формується за принципом Гюйгенса.
- Електромагнітне поле дифракції $П_{діф}$.
- Електромагнітне поле дифракції $П_{дкр}$ на півплощині.
- Електромагнітне поле відображення $П_{дкр}$, яке формується областю суттєвою для відображення радіопроменя.
- Електромагнітне поле $П_{під}$, що формується як явище підсилення радіосигналу за перешкодою.

Таким чином встановлено, що результуюче електромагнітне поле є суперпозицією електромагнітних полів

$$П_{рез} = (К_{пр}П_{фр} + К_{отв}П_{отв} + К_{дкр}П_{дкр} + К_{під}П_{під} + К_{діф}П_{діф})N \quad (1)$$

де К -коефіцієнт, який характеризує внесок кожної складової у підсумкове поле і $0 \leq К \leq 1$, N - коефіцієнт проходження електромагнітної хвилі через середовище.

Природним способом підвищення якості прийому при багатопроменевому розповсюдженні радіосигналу є багатоканальний радіоприймач. Нажаль, він при класичному виконанні має великі розмірі. Для вирішення цієї задачі запропоновано використання панорамного радіоприймача на засадах SDR технології [6], що зображено на рисунку 2.

Прийнятий радіосигнал на широкому частотному діапазоні ΔF (ΔF

$\equiv [-\lambda_0/2; \lambda_0/2]$) з антено-фільтрового блоку подається на АЦП.

Після чого основний канал може бути поділено на декілька віртуальних радіоканалів обробки і подано на кінцевий пристрій обробки. Кількість віртуальних каналів залежить від потужності комп'ютерного обчислювача.

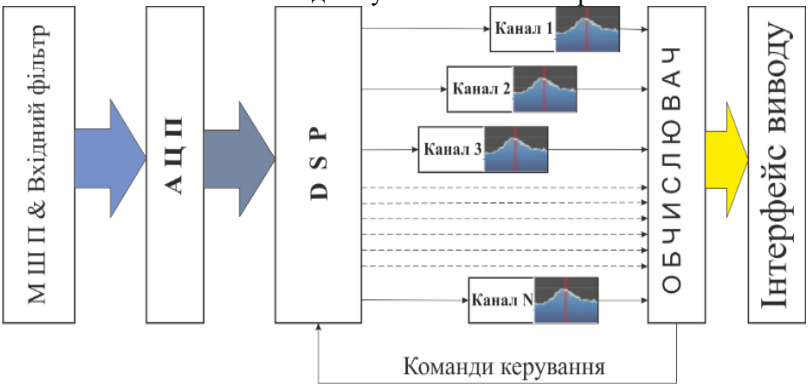


Рис. 2 Функціональна схема сучасної побудови панорамного SDR-приймача

Запропоновано математичну модель розповсюдження радіосигналів в умовах замкнутих просторів, що синтезує особливості розповсюдження радіохвиль як на засадах оптичних моделей розповсюдження електромагнітних коливань так і на засадах класичних моделей розповсюдження радіохвиль. На відміну від класичних моделей розповсюдження радіохвиль, які зазвичай базуються на уяві розповсюдження радіохвиль у вільному просторі та з урахуванням рельєфу місцевості у горизонтальній площині, запропонована модель враховує рельєф поверхні з чотирьох сторін та перешкоди всередині замкнутої поверхні.

Вирішена задача якісного радіосигналу в умовах багатопроменевого розповсюдження на основі багатоканального панорамного приймача на засадах SDR-технології.

[1] Ray-optical prediction of radio-wave propagation characteristics in tunnel environments/ [Y. P. Zhang, Y. Hwang, and R. G. Kouyoumjian] - Part 2: Analysis and measurements," IEEE Trans. Antennas Propag., vol. 46, no. 9, pp. 1337–1345, Sep. 1998.

[2] Radio Wave Characterization and Modeling in Underground Mine Tunnels/ [Mathieu Boutin, Ahmed Benzakour, Charles L. Despins]- IEEE Trans. Antennas Propag., vol. 23, no.2, pp. 540–549 Feb. 2008

[3] Strong Theory of the propagation of UHF radiowaves in coal mine tunnels/ [A. Emslie, R. Lagace] - IEEE Trans. Antennas Propag.,vol. 23, no. 2, pp. 192–205, Mar. 1975.

[4] Радиотехнические цепи и сигналі/ [И.С.Гоноровский] - М.: Радио и связь, 1986. – 512 с.

[5] Теоретические основы радиотехники/ [Б.Р. Левин] – М.: Радио и связь, 1989–656 с.

[6] Технология Software Defined Radio/[А.Силин] - Беспроводные технологии, №2, 2007-22 с.

В.В. Ткаченко, А.В. Ониськова, С.Ф. Гончар, М.Ю. Комаров, С.М. Сергєєв

АНАЛІЗ ЗАГРОЗ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В SMART GRID СИСТЕМАХ НА БАЗІ МЕТОДІВ SREP І CORAS

Однією з актуальних проблем в галузі створення «інтелектуальних мереж» є проблема забезпечення їх інформаційної безпеки. Дослідженню цієї проблеми присвячено значну кількість наукових робот [1 - 7].

У даному докладі пропонується розглянути можливі загрози системи захисту інформації для мережі Smart Grid.

Для розробки системи захисту Smart Grid систем пропонується проводити оцінку ризиків інформаційної безпеки з урахуванням наступних основних аспектів [6]: менеджмент - захист конфіденційної інформації з точки зору управління персоналом, розглядаються загрози, пов'язані з навмисними або випадковими діями співробітників Smart Grid; програми та бази даних - захист від загроз, що виникають на рівні додатків і баз даних; мережа - захист від загроз, які можуть виникнути в зв'язку з використанням LAN і WAN мереж, в тому числі загроз з мережі Інтернет; мобільні пристрої - захист від загроз, пов'язаних з використанням GSM-мереж і мобільних телефонів.

Для аналізу загроз і розробки заходів протидії виявленим загрозам були обрані два базових методи: SREP і CORAS, розроблених відповідно до міжнародного стандарту ISO / IEC 27001 [8].

SREP (Security Requirements Engineering Process) - метод, метою якого є розробка вимог до системи захисту інформації [9]. Реалізація методу включає:

1. Введення основних визначень;
2. Вибір критичних / вразливих джерел інформації;
3. Постановку цілей для системи захисту інформації;
4. Визначення загроз;
5. Визначення ризиків;
6. Розробку вимог до системи захисту;
7. Упорядкування вимог за важливістю;
8. Перевірку відповідності існуючої системи розробленим вимогам;
9. Розробку контрзаходів.

CORAS - метод проведення аналізу інформаційних ризиків [10]. Метод складається з:

1. Підготовки до проведення аналізу;
2. Вибору об'єктів захисту;
3. Опису об'єктів захисту за допомогою діаграм;
4. Постановки цілей;
5. Ідентифікації ризиків за допомогою діаграм загроз;
6. Визначення ризиків по діаграмах загроз;
7. Оцінки ризику з використанням діаграм ризиків;

8. Розробки контрзаходів з використанням діаграм контрзаходів.

Дані методи були обрані як найбільш підходящі для досягнення поставлених цілей. За допомогою CORAS здійснено аналіз ефективності системи захисту з точки зору додатків, баз даних і мережі. За допомогою SREP здійснено аналіз ефективності системи захисту з точки зору менеджменту та мобільних пристроїв.

Оцінка можливого ризику відбувалася відповідно до методології, запропонованої в стандарті ISO / IEC 27005 [11].

В результаті аналізу були виділені три види інформаційних ресурсів, що підлягають захисту: 1) Персональні дані користувачів Smart Grid; 2) Технічна інформація, яка надходить від клієнтів мережі; 3) Інформація про системні збої і помилки, які відбуваються при роботі мережі.

Таким чином, проведений аналіз дозволяє до вимог, які повинна реалізовувати система захисту віднести: запобігання неавторизованого розкриття інформації, що захищається (конфіденційність); забезпечення постійного доступу користувачів до інформації, що захищається (доступність); запобігання несанкціонованої зміни інформації, що захищається (цілісність).

[1] Енергетична стратегія України на період до 2030 року [Електронний ресурс] – http://www.niss.gov.ua/ public/File/2014_nauk_an_rozrobku/Energy %20Strategy %202035.pdf.

[2] Аналіз зарубіжної практики впровадження автоматизованих систем управління технологічними процесами в електроенергетиці [Електронний ресурс] - https://ua.energy/wp-content/uploads/2018/01/2.-SMART-GRID.pdf.

[3] European Smart Grid Technology Platform [Електронний ресурс] – http://ec.europa.eu/research/energy/pdf/smartgrids_en.pdf.

[4] Estimating the Costs and Benefits of the Smart Grid [Електронний ресурс] – http://www.rmi.org/Content/Files/EstimatingCostsSmartGRid.pdf.

[5] Гончар С.Ф. Оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури. Монографія – Київ: Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національна академія наук України, 2019. - 175с.

[6] Ткаченко В.В., Щебланін Ю.М. / Основні аспекти інформаційної безпеки в Smart Grid системах на основі стандартів ISO/IES 27001 та 27005: Сучасний захист інформації - № 3(39), 2019. - 36 - 41 с.

[7] Ткаченко В.В. / Основні аспекти кібербезпеки в Smart Grid системах: матеріали наук.-практ. конф. «Безпека енергетики в епоху цифрової трансформації» - Київ: Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національна академія наук України, 2019. – 21 с.

[8] ISO / IEC 27001: 2013 [Електронний ресурс] // - Режим доступу: https://www.iso.org/obp/ui/fr/#iso:std:iso-iec:27001:ed-2:v1:fr (18.10.2019).

[9] List of Known Meshlocals [Електронний ресурс] – https://docs.meshwith.me/meshlocals/existing/.

[10] Shifttstas. Hyperboria [Електронний ресурс] – https://habr.com/post/181862/.

[11] ISO/IEC 27005: 2018 [Електронний ресурс] - https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-3:v1:en.

В.Ю. Зубок

ВПЛИВ РИЗИКІВ, ПОВ'ЯЗАНИХ З ПРОГРАМНИМ ЗАБЕЗПЕЧЕННЯМ, НА ФУНКЦІОНУВАННЯ ГЛОБАЛЬНОЇ МАРШРУТИЗАЦІЇ В ІНТЕРНЕТІ

Атаки на глобальну маршрутизацію, зокрема викрадення та перехоплення маршрутів (route hijack та route leak), є однією з масштабних проблем кібербезпеки. Атаки використовуються для маніпуляцій з трафіком з метою дестабілізації мережі Інтернет, шпигунства, крадіжок, нанесення матеріальної шкоди. є можливими тому, що протокол прикордонного шлюзу (BGP) був запроваджений до того, як був усвідомлений його вплив на кібербезпеку. 30 років тому зловживання його незахищеністю були відсутні, а 20 років тому - не були такими поширеними, як сьогодні [1]. У оригінальній специфікації BGP не було визначено заходів безпеки для запобігання навмисних чи ненавмисних помилок конфігурації мережі. Відсутність вбудованих заходів безпеки робить BGP вразливим як до викрадення префікса, так і до витоків маршруту [2]. Викрадення префікса - це явище, при якому Автономна система (AS) нелегітимно оголошує себе як джерело префікса замість справжнього джерела. Витік маршруту означає, що AS нелегітимно, з порушеннм політики маршрутизації, пропонує маршрути до чужих префіксів. Ці нелегітимні маршрути забруднюють таблиці маршрутизації BGP, спотворюють шляхи проходження мережевого трафіку і впливають на конфіденційність, цілісність та доступність IP-комунікацій.

Однією з основних завдань системи розподілу адресного простору Інтернет є забезпечення унікальності розподілених ресурсів в глобальному масштабі. Використання в глобальному Інтернеті одного і того ж адресного простору кількома мережами призведе до порушення функціонування цих мереж, оскільки система маршрутизації Інтернет заснована на принципі, що кожний кінцевий пристрій має унікальну адресу. Для контролю за глобальним розподілом понад 20 років тому були введені в експлуатацію кілька баз даних Інтернет-маршрутів (Internet Routing Registry, IRR), за якими "доглядають" п'ять авторизованих регіональних реєстрів, що уповноважені виконувати розподіл IP-адрес і номерів автономних систем [3]. Структура взаємодії мереж в Інтернеті в багатьох випадках не є ієрархічною або не відповідає структурі розподілу адрес. Прикладом є пірингові взаємодії між мережами, або відносини клієнта з Інтернет сервіс-провайдером, в разі, коли клієнт має власний незалежний адресний простір. У всіх цих випадках провайдери покладаються на публічно доступні реєстраційні дані, які мали б міститись в IRR. Але якість інформації, що розміщена у цих джерелах, дуже сильно варіюється. Чим менше об'єкти реєстрації (мережі, маршрути і т.і.), та чим ближче вони до кінцевого користувача, тим менше довіри до того, що представлені дані дійсно відображають поточну політику маршрутизації суб'єктів, до яких ці дані мають відношення. Іншою проблемою є те, що

достовірність даних неочевидна для «третіх осіб». Найчастіше перевірка достовірності перетворюється в детективне розслідування з залученням різних джерел.

Для валідації джерел анонсів розроблено та адаптовано інфраструктуру публічних ключів для ресурсів (RPKI) [4]. RPKI вирішує питання авторизації внесення змін в IRR та валідації інформації про «належність» мережевих префіксів. Об'єктом валідації є запись про походження маршруту (Route Origin Authority - ROA). Нещодавній локальний інцидент у адміністратора реєстру призвів до масштабного збою в глобальный маршрутизації.

31 березня 2020 року в ході роботи з програмним забезпеченням реєстру з бази даних випадково видалили 4100 RPKI записів авторизації походження маршруту (ROA). Адміністратор реєстру - RIPE NCC - повідомив в середині дня 1 квітня 2020, що «це сталося під час технічного обслуговування нашого внутрішнього програмного забезпечення». Більш детальну інформацію було опубліковано у пост-фактумному звіті, з я кого зрозуміло тривалість і глобальність збоїв, що виникли в результаті проблем підчас оновлення програмного забезпечення [5].

Оновлення програмного забезпечення і видалення записів ROA трапилось в неробочий час, що призвело до невчасного детектування проблеми. повідомлення постраждалих кліїнтів були оброблені вже наступного ранку, 1 квітня 2020 року. Відновлення видалених записів не вдалося без втручання наших інженерів і загалом тривало до середини дня 2 квітня. Після того проводилось розслідування, чи страждали якісь IP-префікси підчас збою від route-leak чи route-hijack інцидентів (витоку чи перехоплення маршруту).

Масштаб описаний спеціалістами компанії QRATOR [6]. Відбувся витік машрутів до 8800 префіксів, які походять більш ніж з 200 автономних систем.

Викладені матеріли інциденту дають привід вважати, що з точки зору безпеки глобальної маршрутизації в Інтернеті, локальне програмне забезпечення інтернет-реєстру на сьогодні є новою єдиною точкою відмови (single point of failure - SPoF) саме завдяки розвитку механізму RPKI, що призваний захистити глобальну маршрутизацію. Це означає, що на етапі розробки, впровадження та супроводу підповідного програмного забезпечення було припущено помилок.

На сьогоднішній день безпека мережевого ПЗ впливає на все більше аспектів сучасності.

Без сумніву, незалежно від сфери застосування усі використовувані ресурси повинні бути захищеними. Проте далеко не в усіх випадках доречним буде правило «чим більше захисту, тим краще» – додатки різних сфер потребують різних підходів.

Забезпечення захищеності веб-додатків та веб-систем є комплексною задачею, та потребує уваги як у процесі їх розробки так і у ході експлуатації. Розробка програмного забезпечення - це діяльність, яка використовує різноманітні технологічні досягнення і вимагає високого рівня знань. Через ці

та інші фактори кожен проект розробки програмного забезпечення містить елементи невизначеності. Це відомо як проектний ризик. Управління ризиками включає такі завдання:

- визначення ризиків та їх тригерів;
- класифікування та визначення пріоритетів ризиків;
- розробка плану з усунення чи мінімізації наслідків кожного ризику;
- моніторинг стану триггерів ризику в ході проекта;
- в разі матеріалізації ризику - виконання плану з усунення чи мінімізації наслідків.

Невідомо, чи інцидент трапився через недоліки програмного коду, чи невдалої архітектури ПЗ. Роздивимось аспект моніторингу та мінімізації наслідків [7]. Інцидент розпочався підчас проведення планових робіт в час, а виявлено проблему було лише на ранок. Це брак моніторингу. Моніторинг включає:

- публікацію звітів про стан проекту включно з питаннями управління ризиками;
- перегляд планів ризику відповідно до будь-яких основних змін у графіку проекту;
- перегляд і репріоритізація ризиків;
- мозковий штурм щодо потенційно нових ризиків підчас планування змін в проекті.

Якщо виникає ризик, відповідна реакція на зменшення наслідків повинна бути взята із плану управління ризиками. Варіанти пом’якшення включають:

- прийняти: визнати, що ризик впливає на проект. Прийміть чітке рішення про прийняття ризику без будь-яких змін у проекті. Тут затвердження керівництва проекту є обов'язковим;
- уникнути: коригувати масштаби проекту, графік чи обмеження, щоб мінімізувати наслідки ризику;
- контроль: вживання заходів для мінімізації впливу або зменшення інтенсифікації ризику;
- передача: здійснити організаційну зміну відповідальності, відповідальності чи повноважень іншим зацікавленим сторонам, які приймуть ризик;
- продовжити моніторинг: часто підходить для ризиків із низьким впливом.

Протягом проекту важливо забезпечити ефективну комунікацію між усіма зацікавленими сторонами, менеджерами, розробниками, тестувальниками. Вочевидь, адміністратор реєстру не був готовий до швидкого відновлення даних. Попри значний вплив інциденту, його наслідки було усунуто більше ніж як за добу. Це означає відсутність чи недосконалість плану пом’якшення ризику.

Отже, питання поводження з ризиками в процесі розробки та експлуатації програмного забезпечення для реєстрів глобальної маршрутизації в Інтернеті потребують значно більшої уваги через те, що

впровадження нових технологій RPKI призвело до появи нової єдиної точки відмови.

[1] Pavlos Sermpezis, Vasileios Kotronis, Alberto Dainotti, and Xenofontas Dimitropoulos. A survey among network operators on BGP prefx hijacking. ACM SIGCOMM Computer Communication Review, 48(1):64–69, 2018.

[2] Andreas Reuter, Randy Bush, Italo Cunha, Ethan Katz-Bassett, Thomas C Schmidt, and Matthias Wählisch. Towards a rigorous methodology for measuring adoption of RPKI route validation and fltering. ACM SIGCOMM Computer Communication Review, 48(1):19–27, 2018.

[3] MERIT. List of Routing Registries. [Електронний ресурс] Режим доступу: http://www.irr.net/docs/list.html. Дата звернення: Апр.20, 2020.

[4] RIPE NCC. BGP Origin Validation. [Електронний ресурс] Режим доступу: https://www.ripe.net/manage-ips-and-asns/resource-management/certification/bgp-origin-validation. Дата звернення: Апр.20, 2020.

[5] RPKI ROA Deletion: Post-mortem [Електронний ресурс] Режим доступу: https://www.ripe.net/ripe/mail/archives/routing-wg/2020-April/004072.html. Дата звернення: Апр.21,2020.

[6] This is how you deal with route leaks. Qrator Labs corporate blog, Information Security, Network technologies [Електронний ресурс] Режим доступу: https://habr.com/en/company/qrator/blog/495260/. Дата звернення: Апр.21,2020.

[7] Risk Management in Software Development and Software Engineering Projects [Електронний ресурс] Режим доступу: https://www.castsoftware.com/research-labs/risk-management-in-software-development-and-software-engineering-projects. Дата звернення: Апр.22,2020.

В.С. Грінченко, О.О. Ткаченко, К.В. Чуніхін

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ЕКРАНУВАННЯ МАГНІТНОГО ПОЛЯ ЛІНІЙ ЕЛЕКТРОПЕРЕДАЧІ ҐРАТЧАСТИМИ ЕКРАНАМИ ПРИ ЗМІНІ МЕТАЛОЄМНОСТІ

Дослідження, що виконуються під патронатом Всесвітньої організації охорони здоров'я в рамках «The International EMF Project» [6], свідчать про високий ризик для здоров'я людини магнітного поля (МП) промислової частоти (50-60 Гц) при його довготривалому впливі. Високовольтні повітряні лінії електропередачі (ПЛ) є джерелом достатньо інтенсивного МП. Для його екранування використовуються різні типи екранів [1-5]. У своїх попередніх роботах авторами було запропоновано новий тип електромагнітного екрана: так званий, ґратчастий екран, який складається з набору проводів, з'єднаних між собою паралельно [7]. Подальші дослідження, результати яких представлено в [4], показали, що ефективність ґратчастого екрана може бути підвищена за рахунок використання U-подібного профілю.

Метою даної роботи є визначення металоємності ґратчастого екрана за умови ефективного екранування МП ПЛ.

Дослідження проведено для ґратчастого екрана, представленого в [4]. Металоємність зазначеного екрану ми прийняли за умовну одиницю. При цьому вважалося, що нескінченно довгі проводи ПЛ паралельні один одному. Параметри ПЛ та будівлі взяті з [4, 7]. На рисунку будівля позначена прямокутником. Її висота складає 40 м, ширина 20 м. Будівля розташована за 20 м від ПЛ. Як видно з рисунку, за відсутності екрана, діюче значення магнітної індукції перевищує гранично допустимий рівень 0,5 мкТл у всій будівлі.

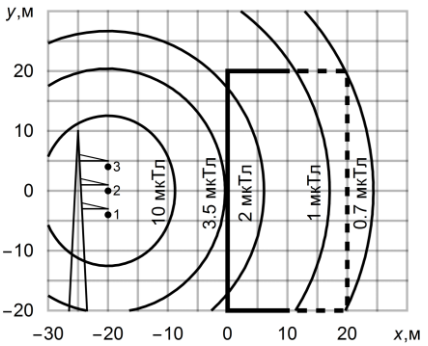


Рисунок – ПЛ та зона екранування

Металоємність ґратчастого екрана варіювалася від 0,5 до 2,0 відносних одиниць. Для кількісної оцінки ефективності екранування використано коефіцієнт екранування:

$$\eta = 100 \cdot S/S_0,$$

де S_0 – загальний переріз екранованого простору, а S – площа тієї частини, де рівень МП менший за 0,5 мкТл. Береться до уваги простір всередині будівлі, що віддалена більше ніж на 0,5 м від стін.

Результати чисельного моделювання, представлені в таблиці, показують, що збільшення металоємності вдвічі призводить до підвищення коефіцієнта екранування менш ніж на 1%.

Таблиця

Залежність коефіцієнта екранування від металоємності гратчастого екрана

Металоємність, у відн.од.	Коефіцієнт екранування η, %
0,5	83,6
0,6	91,8
0,7	95,8
0,8	98,0
0,9	98,8
1,0	99,1
1,1	99,2
1,2	99,3
1,3	99,4
1,4	99,5
1,5	99,5
2,0	99,6

При зменшенні металоємності на 10-20% має місце несуттєве зниження коефіцієнта екранування в межах 1-2%. Зменшення металоємності на 30-50% призводить до зниження коефіцієнта екранування на 4-15%.

[1] Budnik K., Machczyński W. Power line magnetic field mitigation using a passive loop conductor. Poznan University of Technology Academic Journals. Electrical Engineering. 2013. No. 73. Pp. 137-145.

[2] Canova A., del-Pino-López J.C., Giaccone L., Manca M. Active shielding system for ELF magnetic fields. IEEE Trans. Magn. 2015. Vol. 51. No 3. Pp. 1-4.

[3] De Wulf M., Wouters P., Sergeant P., Dupré L., Hoferlin E., Jacobs S., Harlet P. Electromagnetic shielding of high-voltage cables. Journal of Magnetism and Magnetic Materials. 2007. Vol. 316. No. 2. Pp. e908-e911.

[4] Grinchenko V., Pyrohova U. Mitigation of overhead line magnetic field by U-shaped grid shield. 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering. 2019. Pp. 345-348.

[5] Kuznetsov B., Bovdui I., Voloshko A., Nikitina T. Modeling and active shielding of magnetic field in residential buildings located near group of high voltage power lines. 2018 IEEE 3rd International Conference on Intelligent Energy and Power Systems. 2018. Pp. 106-109.

[6] The World Health Organization, “The International EMF Project”. [Online]. Available: http://www.who.int/peh-emf/project/en/. [Accessed: 22-Apr-2020].

[7] Грінченко В.С. Зниження магнітного поля трифазних ліній електропередачі гратчастим електромагнітним екраном / В.С. Грінченко // Технічна електродинаміка. – 2018. – № 4. – С. 29-32.

О.В. Маєвський, В.О. Артемчук, Ю.Б. Бродський,
П.П. Топольницький, І.А. Пількевич

МОДЕЛЮВАННЯ ПРОЦЕСУ УПРАВЛІННЯ ПАРАМЕТРАМИ ТЕХНІЧНИХ СИСТЕМ НА ПРИКЛАДІ ЗАСОБІВ ДЗЗ

Задача побудови імітаційних моделей процесів в системах різної фізичної природи за отриманими експериментальними даними зазвичай зводиться до визначення параметрів апроксимуючої функції.

Але, достатньо складний характер динаміки відхилення параметрів бортових систем космічних апаратів (КА) призводить до складних нелінійних залежностей не тільки у вигляді апроксимуючих функцій, а й у вигляді диференціальних рівнянь та їх систем. При цьому, побудова адекватної математичної моделі за експериментальними даними забезпечує необхідне відтворення динаміки досліджуваного процесу з мінімальною загальною похибкою і, як наслідок, отримується підвищення ефективності керування системами КА.

При використанні математичних моделей представлених системами диференціальних рівнянь спостерігається ускладнення обчислювальних алгоритмів.

Для поліноміальних математичних моделей має місце зростання похибок моделювання за рахунок збільшення кількості коефіцієнтів (у відповідному функціональному базисі), які також мають відповідні похибки обчислень.

Запропонований в статті підхід (на основі створеної моделі) запобігання виникненню ризикових ситуацій, на відміну від схожих типових задач, не передбачає проведення екстраполяції, а орієнтується на створення факторного простору параметрів бортових систем КА в визначених межах та оптимальне керування критичними значеннями контрольних параметрів таких систем.

Таким чином, важливою і актуальною є науково - практична задача, що полягає в ефективності управління бортовими системами КА. В зв’язку з цим пропонується імітаційна модель, яка оптимізує процес відновлення бортових параметрів КА в рамки робочих діапазонів, і являє собою факторний простір. Станам бортових параметрів КА в різні моменти часу ставиться у відповідність множина точок, що формує поверхню прийняття рішень в цьому факторному просторі.

У разі досягнення критичних або неприпустимих значень (за рамками робочих діапазонів) бортових параметрів КА, система прийняття рішень надає «управляючі сигнали корегування», які повертають відповідні параметри в границі робочого діапазону, що відповідає переміщенню кінця радіус-вектора від точки до точки по поверхні прийняття рішень в факторному просторі, див. рис. 1.

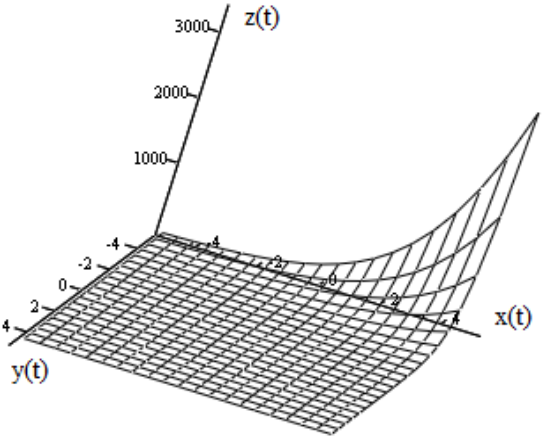


Рис. 1. Поверхня прийняття рішень у факторному просторі (одиниці вимірювань вказано умовно)

Для підвищення ефективності системи прийняття рішення, необхідно, щоб радіус-вектор переміщався від точки до точки за оптимальними траєкторіями, що належать поверхні прийняття рішень. При цьому, оптимальними траєкторіями будуть «прямі» на поверхні прийняття рішень, яка має Ріманову геометрію.

В такому випадку, необхідно встановити геометрію поверхні прийняття рішень і знайти рівняння оптимальних траєкторій на ній, що являється основною метою проведених досліджень.

Як відомо, рівняння оптимальних траєкторій отримується після прирівнювання до нуля всіх криволінійних компонент прискорення точки, що рухається по заданій поверхні:

$h_k = \sqrt{g_{kk}}$ - коефіцієнти Ляме, де g_{kk}, відповідні компоненти метричного тензора (фундаментальний об'єкт). З урахуванням коефіцієнтів Ляме, прирівняні до нуля криволінійні компоненти прискорення W_k мають вигляд:

$$\sqrt{g_{kk}} \cdot W_k = \frac{d}{dt}\left(\frac{\partial v^2/2}{\partial \dot{q}^k}\right) - \frac{\partial v^2/2}{\partial q^k} = 0\,. \qquad (1)$$

З урахуванням значення квадрата швидкості $v^2 = g_{ij}\dot{q}^i\dot{q}^j$, отримаємо після перетворень:

$$\ddot{q}^m + \frac{1}{2} g^{mk}\left[\frac{\partial g_{kj}}{\partial q^i} + \frac{\partial g_{ik}}{\partial q^j} - \frac{\partial g_{ij}}{\partial q^k}\right]\dot{q}^i\dot{q}^j = 0\,, \qquad (2)$$

де $\Gamma_{ij}^m = \frac{1}{2} g^{mk}\left[\frac{\partial g_{kj}}{\partial q^i} + \frac{\partial g_{ik}}{\partial q^j} - \frac{\partial g_{ij}}{\partial q^k}\right]$ - символ Кристофеля 2-го роду (коефіцієнт афінного зв'язку), який не є тензором.

Остаточно, рівняння оптимальних траєкторій має вигляд:

$$\ddot{q}^m + \Gamma_{ij}^m \dot{q}^i \dot{q}^j = 0; \quad (3)$$

m=1,2….M, M – розмірність простору. Система буде складатись з *M* диференційних рівнянь другого порядку і мати *2M* констант інтегрування.

Далі визначаємо коефіцієнти Ляме і аналізуємо прикладну задачу для трьох факторів.

Поверхню прийняття рішень апроксимуємо функцією двох змінних виду $z(x, y) = a_0 a_1^x a_2^y$ (апроксимація передбачає можливість використання і інших видів функції). Значення параметрів a_0, a_1, a_2 визначимо з результатів обробки статистичних даних. Виберемо масштабні коефіцієнти таким чином, щоб аналізовані величини z, x, y були безрозмірними. Введемо узагальнені координати: h – висота точок поверхні прийняття рішень над площиною *oxy* і кут азимута φ точок поверхні прийняття рішень, відлічуваний проти часової стрілки в додатному напрямку, тобто узагальнені координати точок - (*h, φ*).

Запропонована модель дає можливість оптимального керування заданими параметрами технічних систем з метою запобігання виникненню аварійних та ризикових ситуацій. На підставі даної моделі можливо створювати системи підтримки прийняття рішень для організації заходів спрямованих на зменшення ризикових ситуацій в технічних системах.

[1] Прийняття рішень оператором аеронавігаційної системи: монографія / В.П. Харченко, Т. Ф. Шмельова, Ю. В. Сікірда. – Кіровоград: КЛА НАУ, 2012. – 292 с.

[2] Popov, O.; Iatsyshyn, A.; Kovach V.; Artemchuk V.; Taraduda D.; Sobyna V.; Sokolov D.; Dement M.; Yatsyshyn T. (2018). “Conceptual Approaches for Development of Informational and Analytical Expert System for Assessing the NPP impact on the Environment”. Nuclear and Radiation Safety. Iss. 3(79), pp. 56—54. doi:10.32918/nrs.2018.3(79).09 (Ukr)

[3] Popov, O.; Iatsyshyn A.; Kovach, V.; Artemchuk, V.; Taraduda, D.; Sobyna, V.; Sokolov, D.; Dement, M.; Yatsyshyn, T.; Matvieieva, I. (2019). “Analysis of Possible Causes of NPP Emergencies to Minimize Risk of Their Occurrence”. Nuclear and Radiation Safety. Iss. 1 (81), pp. 75—80. doi: 10.32918/nrs.2019.1(81).13 (Ukr)

[4] Конотоп, Д. І. (2019). Інформаційна технологія створення та супроводження узагальненої моделі складних технічних об'єктів.

[5] Москаленко, В. В., Москаленко, А. С., Москаленко, А. С., Берест, О. Б., Мартиненко, С. С., Мартыненко, С. С., Окопный, Р. П. (2018). Інтелектуальна автономна бортова система безпілотного літального апарату для ідентифікації об'єктів на місцевості. Сумський державний університет.

[6] Каханер Д. Численные методы и программное обеспечение: пер. с англ. /Д. Каханер К. Моулер, С. Нэш.-М.:Мир,1998.-575с.

[7] Флеминг У., Ришел Р. Оптимальное управление детерминированными и стохастическими системами / У. Флеминг, Р. Ришел .-М.:Мир,1978.-312с.

В.С. Подгуренко, В.Е. Терехов

МОДЕЛИРОВАНИЕ СТОИМОСТИ ЭНЕРГИИ, ВЫРАБАТЫВАЕМОЙ ВЕТРОЭЛЕКТРИЧЕСКОЙ УСТАНОВКОЙ

Проведенный анализ многочисленных ветроэнергетических публикаций показал, что важнейшая научно–прикладная проблема подбора эффективных ветровых электрических установок (ВЭУ) мультимегаваттного класса для конкретных ветровых условий строительства промышленных ветроэлектрических станций (ВЭС), далека от разрешения.

Проблемные вопросы математического и компьютерного моделирования параметров ВЭУ большой мощности, которые должны вырабатывать как можно больше товарной энергии и удовлетворять соотношению цена/качество, остаются открытыми. Уже стало мировой тенденцией, что эффективность работы ВЭУ повышается за счет роста их номинальной мощности. Выполненные же исследования показывают, что ориентация только на этот показатель может привести к значительному удорожанию производства электроэнергии.

В работе [4] детально исследовано влияние параметров ВЭУ (номинальная мощность генератора *X1*, диаметр ветроколеса *X2* и высота его расположения *X3*) на годовую выработку *Q* путем условного размещения в ветровые условия Северного Причерноморья 43-х единиц ВЭУ мегаваттного класса ведущих мировых производителей. В результате исследования была получена математическая модель (ММ) годовой выработки ВЭУ $Q_Г$ с заданными параметрами:

$$Q_{\text{г}} = -7125{,}25 + 1348{,}594 \cdot X1 + 97{,}52617 \cdot X2 + 28{,}81139 \cdot X3. \left[\text{МВт} \cdot \text{ч}\right] \quad (1)$$

Как видно из (1), увеличение выработки $Q_Г$ достигается за счет трех соответствующих параметров, однако стоимость увеличения каждого параметра различна.

Цель исследования: на основании анализа капитальных затрат (КЗ) на строительство ВЭУ различных параметров, определить наиболее выгодные их значения, позволяющие минимизировать стоимость вырабатываемой электроэнергии в условиях Северного Причерноморья.

В работе [1] определен критерий оценки стоимости вырабатываемой электроэнергии (СЭ) в виде соотношения капитальных затрат на строительство ВЭУ к её годовой выработке $Q_Г$:

$$\text{СЭ} = \frac{\text{КЗ}}{Q_Г}. \left[\frac{\$}{\text{МВт} \cdot \text{ч}}\right]$$

В мировой практике широко применяется критерий стоимости капитальных затрат на 1 МВт установленной мощности (далее – КЗ_1):

$$КЗ_1 = \frac{КЗ}{X1}. \left[\frac{\$}{МВт}\right]$$

Очевидно, что при равных установленных мощностях (*X1*) КЗ на ВЭУ с более высокой башней и/или бóльшим размером лопастей будут выше. Кроме того, остается открытым вопрос о наличии или отсутствии связи между $КЗ_1$ и мощностью устанавливаемой ВЭУ.

На сайте статистики [3] представлены $КЗ_1$ американских ВЭС за период 2008 – 2019 гг (рис. 1).

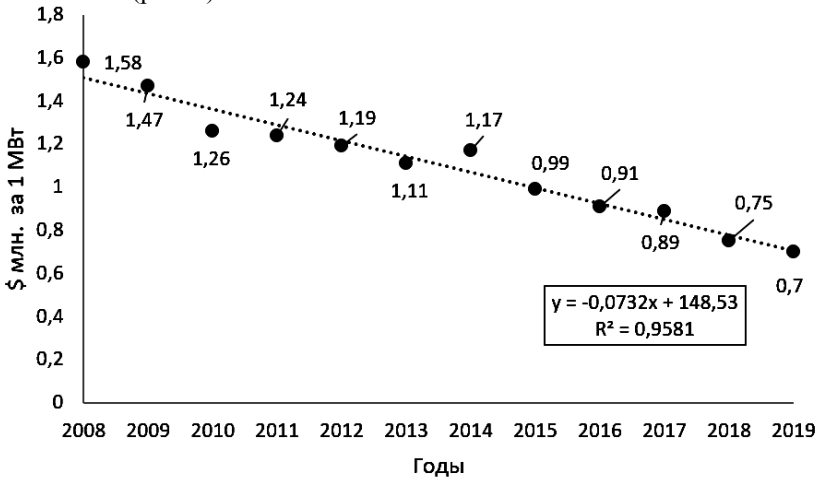


Рис.1 Стоимость 1 МВт установленной мощности ВЭС

Будем считать, что ввиду глобализации и существенного объема ветроэнергетического рынка США, цены на мировом рынке будут примерно соответствовать приведенным выше данным, т.е. рис.1 отображает стоимость среднестатистических $КЗ_1$ (далее – базовая стоимость, БС). Очевидно, что в зависимости от выбранных параметров ВЭУ $КЗ_1$ будут несколько больше или меньше БС на некоторый поправочный коэффициент *k*:

$$k = \frac{КЗ_1}{БС}.$$

На основании стоимости КЗ по некоторым ВЭУ по состоянию на 2012г [2] определены поправочные коэффициенты *k* (табл. 1).

Корреляционный анализ данных столбцов 2 – 4 и 8 показал высокую корреляцию между *k* и *X3* (0,96), *k* и *X2* (0,90) и среднюю между *k* и *X1* (0,50).

Полученная модель (2) имеет высокий коэффициент множественной корреляции R (0,993); высокий коэффициент детерминации R2 (0,986); небольшую стандартную ошибку (0,02). Модель значима в целом по Фишеру (P_F < 4,9·10-5). Уровень значимости коэффициентов при объясняющих факторах по Стьюденту также мал (p < 0,02).

Таблица 1

Технико-экономические показатели ВЭУ

№ п/п	Мощность *X1*, МВт	Диаметр ВК *X2*, м	Высота оси ВК *X3*, м	КЗ на 2012 г, $ млн.	$КЗ_1$, $ млн.	БС на 2012 г, $ млн.	*k*
1	1,5	77	80	1,731	1,154	1,190	0,970
2	2,5	100	80	3,048	1,219	1,190	1,025
3	1,5	110	100	2,163	1,442	1,190	1,212
4	2,5	90	100	3,322	1,329	1,190	1,117
5	3,6	104	100	4,622	1,284	1,190	1,079
6	2,5	112	120	3,793	1,517	1,190	1,275
7	3	116,4	120	4,454	1,485	1,190	1,248
8	3	122	140	4,880	1,627	1,190	1,367
9	5	129	140	8,027	1,605	1,190	1,349

Полученная ММ имеет вид:

$$k = 0{,}36884 - 0{,}0376 \cdot X1 + 0{,}003345 \cdot X2 + 0{,}00505 \cdot X3. \qquad (2)$$

Уравнения (1) и (2) показывают, что увеличение высоты оси ВК практически в 1,5 раза дороже и в 3 раза менее результативно соответствующего увеличения диаметра ВК, что увеличивает стоимость вырабатываемой электроэнергии. Отрицательный знак при *X1* указывает на то, что с увеличением номинальной мощности ВЭУ стоимость одного её МВт уменьшается, однако достичь существенного увеличения номинальной мощности ВЭУ без соответствующего увеличения диаметра ВК, и соответственно высоты его расположения невозможно.

[1] Lee J.-T., Kim H.-G. *, Kang Y.-H., Kim J.Y.. Determining the Optimized Hub Height of Wind Turbine Using the Wind Resource Map of South Korea. Energies 2019, 12, 2949; doi:10.3390/en12152949.

[2] Levandowski C. Evaluating Tall Wind Turbine Towers in the Field. 2015. https://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=1116&context=undergradresearch_symposium.

[3] Price index for wind turbines in the U.S. from 2008 to 2019. https://www.statista.com/statistics/499491/us-wind-turbine-price-index.

[4] Подгуренко В.С., Гетманец О.М., Терехов В.Е.. Повышение эффективности производства электроэнергии ветроэлектрической установкой на основе математического моделирования. Електрон. моделювання. 2020. Т.42, №2, с. 121 –127; doi:10.15407/emodel.42.02.121.

А.А. Владимирский, И.А. Владимирский

ОБЕСПЕЧЕНИЕ ТРЕБУЕМОЙ ТОЧНОСТИ ИЗМЕРЕНИЯ ПАРАМЕТРОВ ВИБРАЦИИ

Область применения оборудования диагностического, охранного и бытового применения, работающего в низкочастотном и инфранизкочастотном диапазонах постоянно расширяется, поэтому все большую актуальность получает разработка соответствующих средств метрологического обеспечения. Данная работа посвящена одному из аспектов разработки низкочастотной виброкалибровочной установки, а именно: обеспечению заданной точности измерения среднеквадратического значения (СКЗ) сигнала, формируемого испытуемым устройством (вибропреобразователем) под воздействием гармонического механического воздействия. Известно [1], что для синусоидального сигнала измеряемое СКЗ является точным и не зависит от выбора момента измерения и начальной фазы сигнала, если интервал τ измерения СКЗ определенным образом соотносится с частотой F_c анализируемого сигнала:

$$\tau = \frac{k}{2 \cdot F_C}, \; k \in Z \qquad (1)$$

Отклонение от данного условия приводит к значительным ошибкам. Поэтому, для согласования частоты F_c сигнала и величины интервала τ измерения СКЗ, в разрабатываемом устройстве используется узкополосная избирательная фильтрация каждой из анализируемых гармоник. Однако, неидеальность фильтров, помехи и различного рода возможные отклонения характеристик системы от первоначальных или заданных могут приводить к нарушению строгого выполнения условия (1). На этапе разработки виброкалибровочной установки, необходимо оценить возможную степень нарушения данного условия и принять меры по не допущению выхода погрешности определения СКЗ за установленные границы для каждой из анализируемых гармоник. В работе рассматриваются схемотехнические и алгоритмические аспекты решения данной задачи в установке НАВКУ-3 [2], особенностью которой является поддержание постоянного соотношения частоты тестирующего механического колебания, частоты дискретизации и центральной частоты цифрового согласованного избирательного фильтра в измерительном канале.

[1] С.В. Бушуев, А.Н. Попов Исследование точности измерений среднеквадратических значений электрических сигналов на ограниченных интервалах времени. Транспорт Урала №2(29)//2011 с. 46-50.

[2] О.А. Владимирський. Низькочастотна віброкалібрувальна установка на основі лінійного актуатора з зубчастим ременем і кроковім двигуном. Науково-практична конференція «Безпека енергетики в епоху цифрової трансформації», 20.12.2019р. – С48-49.

А.А. Владимирский, И.А. Владимирский

ОБ УЧЕТЕ ВЛИЯНИЯ ХАРАКТЕРИСТИК ЧАСТОТНО-ИЗБИРАТЕЛЬНЫХ ФИЛЬТРОВ НА ДОСТОВЕРНОСТЬ ОПРЕДЕЛЕНИЯ СКЗ ГАРМОНИК В ВИБРОКАЛИБРОВОЧНЫХ УСТАНОВКАХ

В виброкалибровочных установках для исследования реакции различных устройств на испытательные механические колебания определяются величины СКЗ гармоник. Для выделения гармоник применяются частотно-избирательные цифровые фильтры. Рассматривая применение данных фильтров в контексте определения величин СКЗ выходных сигналов, целесообразно учитывать ряд особенностей:

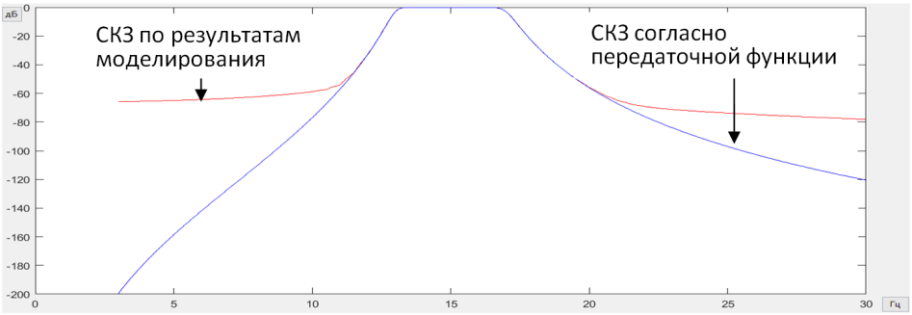
- необходимость определенного интервала времени для переходного процесса (ПП) фильтра перед началом определения достоверной величины СКЗ сигнала;
- зависимость фактической степени подавления в полосе непропускания фильтра от величины интервала времени, отводимого на переходной процесс, особенно на низких частотах;
- возможность попадания в полосу пропускания и переходные полосы фильтра сигналов, не совпадающих по частоте с требуемой для анализа частотой гармоники, с которой согласован интервал времени определения СКЗ (ИСКЗ), что может приводить с значительным ошибкам.

Для иллюстрации вышесказанного на рис.1 представлены частотные характеристики СКЗ на выходе рекурсивного цифрового фильтра Баттерворта, полученные по передаточной функции и путем численного моделирования посредством разностного уравнения фильтра с представленными в табл.1 параметрами. При увеличении числа отсчетов сигналов, отводимых на ПП и ИСКЗ, частотная характеристика по результатам моделирования фильтра приближается к рассчитанной характеристикой по его передаточной функции с уменьшением погрешности определения СКЗ. В работе представлен выбор параметров фильтров с учетом конкретных требований к их характеристикам, к параметрам измерений, частотам гармоник и точности определения их СКЗ.

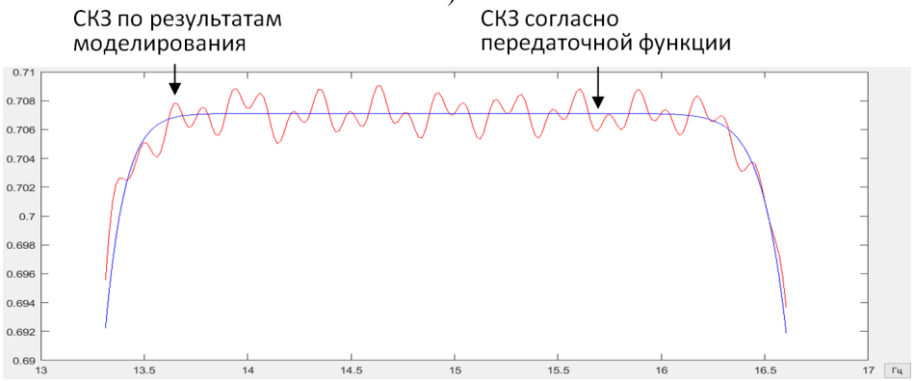
Таблица 1

Пример параметров полосового фильтра для определения СКЗ гармоник.

Порядок фильтра	Полоса пропускания, Гц	Частота дискретизации, Гц	Число пропущенных отсчетов для учета ПП	Число отсчетов ИСКЗ	Погрешность определения СКЗ в полосе пропускания
16	13-17	2000	4000	4000	0,2%



а)



б)

Рис.1. Сравнение частотных характеристик СКЗ на выходе фильтра согласно передаточной функции и согласно результату численного моделирования в диапазоне частот 3 … 30 Гц (а) и в полосе пропускания - 13,31 … 16,62 Гц (б).

А.А. Владимирский, И.А. Владимирский, И.П. Криворучко

ТЕРМОАКУСТИЧЕСКИЙ ТЕЧЕИСКАТЕЛЬ А-10Т3

Группой технической диагностики ИПМЭ им. Г.Е. Пухова НАН Украины в рамках темы “МОНИТОР” разработана новая модификация термоакустического течеискателя А-10Т3. Термоакустический течеискатель А-10Т3, так же как его предшественник А-10Т2 [1], предназначен для определения мест утечек подземных трубопроводов горячего и холодного водоснабжения, теплосетей, других инженерных коммуникаций. Информационными параметрами для выявления утечек являются уровень вибрации и температура грунта над трубопроводом. В состав течеискателя входят: герметичный блок оператора (БО), вибродатчик с магнитным держателем ВДМ-6 для установки непосредственно на поверхность металлического трубопровода, трехножная оснастка для установки ВДМ-6 на грунт, датчик теплового излучения ИКДТ-1, головные телефоны, зарядное устройство, транспортно-рабочая укладка. В новом течеискателе внедрены усовершенствования, повышающие удобство использования. Включение электропитания блока оператора (БО) осуществляется автоматически при подключении одного из датчиков, при отключении датчика - происходит выключение БО. Таким образом, исключаются случайные включения БО и разряд аккумуляторов при транспортировке и хранении. С учетом жестких условий эксплуатации это полезное свойство. При включении БО автоматически определяется тип датчика и выбирается соответствующий режим работы - измерение уровня вибросигнала (текущий и минимальный) или уровень теплового излучения. Необходимость в управлении режимами работы с клавиатуры исключена. Указанные нововведения позволили сократить количество кнопок управления на передней панели БО. Внесены коррекции в программное обеспечение и некоторые изменения в схемотехнику течеискателя. В частности улучшена работа системы автоматической регулировки усиления и системы “защиты слуха” оператора.

Технические решения, реализованные в течеискателе, защищены патентом Украины [2] и авторским свидетельством Украины [3].

[1] А.А.Владимирский, И.А. Владимирский, А.И.Дрозденко. Модернизированный термоакустический течеискатель А-10Т2. Збірник наукових праць. Інститут проблем моделювання в енергетиці НАН України. Вип. 70, Київ, 2014р.-с.93-97.

[2] О.А.Владимирский, І.П., Криворучко. Пристрій для установки вібродатчика з магнітним тримачем на ґрунт при пошуку витоків. Заявка u201912229 від 24.12.2019р. на корисну модель (патент). Рішення про видачу деклараційного патенту на корисну модель № 6750/ЗУ/20 від 07.04.2020р.

[3] Владимирський О.А., Владимирський І.А. Комп'ютерна програма “Термо-акустический течеискатель”. Свідоцтво про реєстрацію авторського права на твір №60778. Україна. 23.07.2015р. /ІПМЕ НАН України.

А.А. Владимирский, Г.В. Анфимова

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ РЕГИСТРАТОРА СЕЙСМИЧЕСКОЙ АКТИВНОСТИ

Группой технической диагностики ИПМЭ им. Г.Е. Пухова НАН Украины в рамках инициативной работы с Институтом геофизики ім. С.І. Субботіна НАН України и ННПМ НАН Украины разработано программное обеспечение регистратора сейсмической активности с англоязычным интерфейсом. Регистратор предназначен для построения систем мониторинга сейсмической активности в районах добычи полезных ископаемых, для оценки состояния фундаментов городских строений [1, 2] и пр. Аппаратной основой регистратора является 4-х канальный блок АЦП, разработанный в ходе темы “Новинтех” и PC-совместимый ноутбук с интерфейсом USB. Параметры блока АЦП: количество входных каналов – 4; частота дискретизации (синхронно всех 4-х каналов) – 4,032 кГц; диапазон частот входных сигналов – 10 … 400 Гц, форматы данных в файлах – “тхт” (текстовый) и “дат” (32 разрядные числа со знаком). В каждом файле записывается 207305 синхронных отсчетов по 4 каналам и номер отсчета (последовательный ряд чисел от 0 до 2^{18}). Номер отсчета (является уникальным в пределах файла записи) формируется регистратором аппаратно и предназначен для контроля целостности данных – отсутствие разрывов и перекрытий в последовательности отсчетов в файлах записей.

Предусмотрено 4 режима работы:

- Аналого цифровое преобразование и запись 4-х сигналов в течение одной минуты в файлы данных. Режим предназначен для тестирования системы.
- “Бесконечная запись” – регистрация входных данных в последовательность минутных файлов. Это основной режим работы регистратора. Длительность записи ограничивается объемом памяти ноутбука и возможностями автономного электропитания.
- Формат просмотра (“осциллограф”) текстовых файлов.
- Формат просмотра (“осциллограф”) файлов данных.

Работа выполнена с использованием Developer Studio Delphi 2006.

[1] Анфімова Г.В. Досвід створення системи метрологічного та технічного супроводу впроваджених засобів технічної діагностики енергетичного та енергоємного обладнання. Науково-практична конференція «Безпека енергетики в епоху цифрової трансформації», ІПМЕ ім. Г.Е.Пухова НАН України, Київ, 20.12.2019р. – С 35-36.

[2] С.В. Щербина, А.І. Фещенко, ОА. Владимирський, І.П. Криворучко, А.П. Іващенко, О.В. Адаменко. Сертифікована автоматизована цифрова система оцінки стану безпеки різних об’єктів. Моделювання та інформаційні технології. Вип. 86, Київ, 2019р.-с.36-41.

І.П. Криворучко

РОЗРОБКА СХЕМИ ІМПУЛЬСНОГО АКТИВАТОРА ЕЛЕКТРОМАГНІТНОГО КЛАПАНА ДЛЯ СТВОРЕННЯ ІМІТАТОРА ЗВУКОВОГО ГІДРОДИНАМІЧНОГО УДАРУ

В основу схеми імпульсного активатора електромагнітного клапана для створення імітатора звукового гідродинамічного удару (мал.1) покладено генератор на базі таймеру NE556, одна половина якого формує періодичний імпульсний сигнал (частота визначається R16), а інша - одновібратор з регульваною тривалістю імпульсного сигналу (R18).

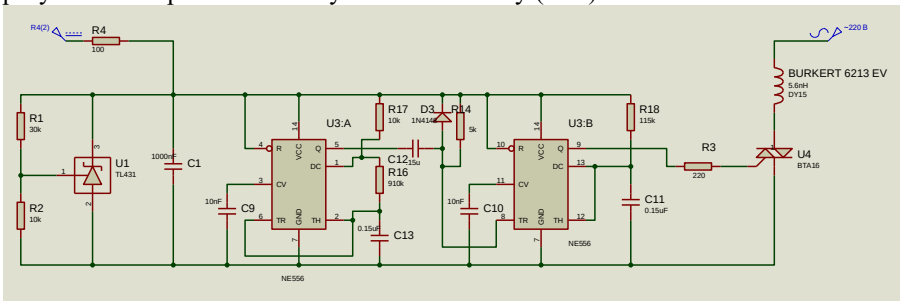


Рис.1. Принципова схема пристрою імпульсного активатора

В якості об’єкта дослідження взято електромагнітний клапан типу Burkert 6213EV, який розрахований на роботу від мережі змінного струму 220 В. Для живлення схеми використовується адаптер стандартного живлення на 12 В постійного струму величиною 1 А. Для стабілізації роботи схеми використано елементи схеми R1, R2 та U1 (TL431), які забезпечують стабільний рівень напруги близько 10В. У відповідності зі схемою було створено макет пристрою.

Згідно технічних умов клапан цього типу гарантовано спрацьовує з частотою не більше за 6 включень за 1 хвилину. Ця частота включень гарантує повне відкриття клапана. Але для створення ударної хвилі вздовж труби неохідності в повному відкритті клапану немає. Тому було проведено дослідження роботи пристрою для більших частот включення. Виявилося, що клапан частково відкривається з частотою аж до 5 Гц.

Імітатор звукового гідродинамічного удару планується використовувати при діагностиці трубопроводів:

1) Спільно з акустичним течошукачем для пошуку трас прихованих пластмасових трубопроводів.

2) Як генератор зондирующих сигналів.

Є.С. Чернозьомов

ПРОБЛЕМИ ОПТИЧНОЇ ТРАНСФОРМАЦІЇ СОНЯЧНОЇ ІНСОЛЯЦІЇ ТА ЇХ РІШЕННЯ

Ефективність використання сонячної енергії є актуальним завданням на сьогоднішній день, існуючі геліоенергетичні пристрої дозволяють використовувати лише невелику частину сонячної інсоляції, як за спектральною, так і за амплітудною складовою. Що потребує дослідження і розробки принципово нових, більш ефективних способів збору і використання сонячної енергії.

Оптична концентрація сонячного випромінювання є єдиним способом підвищення енергетичної щільності процесів перетворення сонячної енергії, і, отже, підвищення ККД сонячних установок для покращення їх техніко-економічних показників.

Геліоенергетичні пристрої, засновані на принципах підвищення енергетичної щільності за рахунок концентрації сонячного випромінювання, потенційно можуть зібрати близько 95% сонячної інсоляції що падає на концентратор.

Основною ідеєю і відмінністю від аналогів є здатність запропонованого концентратора передавати зібрану енергію до стаціонарного приймача за допомогою оптичного хвилеводу, що істотно спрощує конструкцію сонячної установки і дозволяє отримати заявлену ефективність. Що представляє не тривіальне завдання, оскільки концентратор в цьому випадку є оптичною системою, яка складається з декількох елементів і виконує трансформацію одного плоского хвилевого фронту (сонячної інсоляції) в інший плоский хвилевий фронт високої щільності, для подачі його в хвилевід. При цьому необхідно враховувати залежність характеру енергетичних ефектів від інтенсивності випромінювання, оскільки при відбиванні щільних енергетичних потоків, дзеркала оптичних елементів супроводжуються дуже помітними термодинамічними явищами, які призводять не лише до їх нагріву, а і до теплового руйнування.

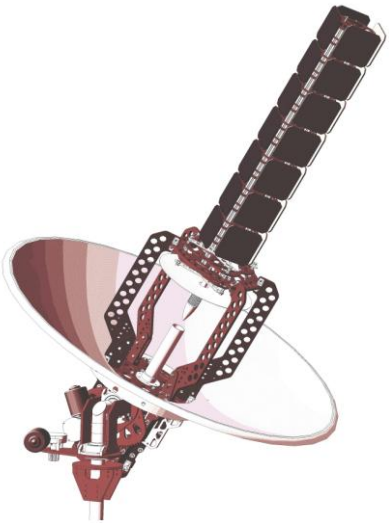


Рисунок 1. Сонячний енергетичний концентратор

Був досліджений характер впливу викривлень хвилевих фронтів в оптичній системі, виправлена аберація шляхом застосування дзеркал із

зв'язаними фокусами (гіперболоїдів), які компенсують сферичну аберацію. Також застосовані методи будови астрономічних телескопів-апланатів Шварцшильда і умова синусів Аббе для усунення коми і зменшення впливу аберацій в системі енергетичного концентратора. Що дозволило покращити якість формування високопотенційного пучка на ширшому кутовому полі прийому.

Були отримані математичні моделі термодинамічних процесів при дії енергетично щільних потоків на силову оптику, досліджені способи забезпечення допустимих теплових режимів роботи, зокрема розглянуті способи створення ефекту повного віддзеркалення на поверхні дзеркал концентратора.

На підставі аналізу спектральних властивостей відбиваючих поверхонь, вдалося розробити оптичну систему здатну забезпечити передачу усього хвилевого діапазону сонячного випромінювання, у тому числі і в інфрачервоному вікні атмосфери (у лазерній оптиці випромінювання з подібною спектральною шириною називається суперконтинуумом), що робить можливим приймати частину сонячного випромінювання в умовах зменшення прозорості атмосфери.

Отримані результати допоможуть в розробці більш ефективних геліоенергетичних пристроїв, заснованих на принципах підвищення енергетичної щільності сонячної інсоляції. Зроблять можливим створення сонячного енергетичного концентратора рис.1 (патент на винахід № 120802), що відрізняється наступними особливостями :

- здатного зібрати близько 95% інсоляції що падає на концентратор;
- незалежного від температури довкілля, здатного однаково ефективно працювати в екваторіальному, помірному і змінному континентальних кліматах;
- працюючого на частотах інфрачервоного вікна атмосфери, що дозволить зібрати частину енергії сонячного випромінювання навіть в похмуру погоду;
- високі і критичні температури на виході не лише підвищать ККД перетворення теплової енергії в електричну, а і значно розширять сферу застосування пристрою, сонячна установка може дати енергію наприклад для піролізу розкладання речовин або для розкладання води - отримання водню;
- з можливістю отримання водню з води або вуглеводнів вирішується основна проблема в геліоенергетиці - акумулювання енергії.

Д.О. Дімітрієва, І.П. Каменева

ВПЛИВ СУБ'ЄКТИВНОГО ФАКТОРУ ПРИ АВАРІЯХ ТА ПОРУШЕННЯХ НОРМАЛЬНОЇ ЕКСПЛУАТАЦІЇ АЕС

Зниження ризику аварійних ситуацій на енергетичних об'єктах є одним з пріоритетних напрямків управління безпекою АЕС На аварійну ситуацію впливають різні чинники, серед яких зміни зовнішніх умов, технічний стан обладнання, а також суб'єктивний фактор [1, 4]. На сучасному етапі розвитку атомної енергетики значно покращилися показники надійності технічних систем, але досить часто спостерігаються випадки некомпетентних дій персоналу, які потребують додаткових досліджень.

Контроль компетентності та системи навчання

Керівники експлуатуючої організації, окремі категорії персоналу ядерної установки та персонал підрядних організацій, що працюють в радіаційних умовах або виконують роботи щодо систем, важливих для безпеки ядерної установки, повинні усвідомлювати вплив своєї діяльності на безпеку, як власну, так і інших осіб та населення. Оскільки вимоги безпеки сформульовані в нормах, правилах та стандартах з ядерної безпеки, то в усіх країнах на ядерних установках та радіаційно-небезпечних об'єктах запроваджена система вивчення керівниками та персоналом цих стандартів з наступною перевіркою закріплення цих знань. Таке навчання та перевірку знань здійснює експлуатуюча організація самостійно.

Органи державного регулювання перевіряють повноту функціонування цієї системи навчання та перевірки знань. Для найбільш важливих з точки зору управління ядерною установкою посад вводиться ліцензування, як підтвердження факту проходження всіх передбачених законодавством процедур з навчання та перевірки знань. Для решти персоналу експлуатуюча організація запроваджує різні заходи з підтримки кваліфікації з урахуванням можливого впливу цього персоналу на ядерну та радіаційну безпеку.

В Україні джерелом даних про події, які трапились на АЕС, є звіти про розслідування порушень нормальної експлуатації та інформаційна система «Порушення в роботі АЕС», яка призначена для забезпечення обліку інформації про такі події в роботі АЕС України та подальшого статистичного аналізу цієї інформації. Огляд статистичних даних щодо порушень у роботі АЕС України за останні 10 років (з 2010 по 2019 роки) показав [1, 2, 5], що загалом відбулось 159 порушень, з яких 45 відносяться до помилкових дій персоналу і організаційних чинників. Їх основною причиною є незадовільна організація відповідних робіт, зокрема, питання щодо компетентності персоналу, який несе відповідальність за забезпечення безпеки.

Психологічні причини порушень норм безпеки

В більшості випадків особи, винні в порушеннях вимог безпеки, проходили встановлені перевірки знань, тобто знали правила безпеки. Виявлені при проведенні відповідного контролю порушення вимог безпеки також показали, що працівники проходять всі інструктажі та перевірки знань,

але тим не менше порушують вимоги безпеки. В зв'язку з цим виявлена закономірність у вигляді усвідомленого порушення правил безпеки в силу певних обставин. До психологічних причин таких порушень віднесено наявність занадто великого обсягу правил, що повторюються в різних варіантах; тривалість і рутинність окремих процедур щодо забезпечення безпеки, що знижує продуктивність праці по основним показникам; складність сприйняття та запам'ятовування правил, процедур, а також їх послідовностей недосвідченими фахівцями; складність процесу сприйняття інформації, що надходить одночасно з різних джерел [3, 4].

Посилаючись на психологічні дослідження в області ризику і безпеки, можна зробити висновок, що при оцінюванні ступеня небезпеки і прийнятті рішення важливу роль відіграє індивідуальне сприйняття ризику [3].

З одного боку, кожна небезпечна подія вимагає прийняття рішення з урахуванням накопиченого досвіду. З іншого боку, вибір рішення (точніше, його наслідки) впливають на структуру сформованого раніше простору знань, тобто кожен новий крок призводить до чергової корекції цих знань і впливає на прийняття рішень в майбутньому. Підвищена індивідуальна схильність до ризику може формуватися в результаті придбання позитивного життєвого досвіду в тих ситуаціях, коли ризикована поведінка приводила до позитивного результату. Негативний життєвий досвід в аналогічних умовах сприяє вибору стратегії мінімізації ризику.

Проведені дослідження показали, що на процес прийняття рішень в аварійних ситуаціях мають вплив психологічні фактори, які призводять до помилкових дій персоналу та порушень правил безпеки, зокрема, особливості індивідуального сприйняття ризику та реагування в умовах стресу.

[1] Аналіз можливих причин виникнення надзвичайних ситуацій на АЕС з метою мінімізації ризику їх виникнення / [О.О. Попов, А.В. Яцишин, В.О. Ковач, В.О. Артемчук, Д.В. Тарадуда, В.О. Собина, Д.Л. Соколов, М.О. Дement, Т. М. Яцишин, І. В. Матвєєва] - Ядерна та радіаційна безпека, 2019, Вип. 1(81). - с. 75-80.

[2] Звіт про надання послуг зі статистичної та аналітичної обробки інформації щодо подій (порушення, відхилення та малозначущі події) у роботі АЕС України, які відбулись у II півріччі 2019 року та I півріччі 2020 року «Статистична та аналітична обробка інформації щодо подій у роботі АЕС України, які відбулись у II півріччі 2019 року». – Київ: ДНТЦ ЯРБ, 2020.

[3] Когнитивная психология /Андерсон Дж. Р.- СПб.: Питер, 2002.-496 с.

[4] Оценка риска аварий с использованием экспертных систем /Немчинов Д. В. - Вестн. Астрахан. гос. техн. ун-та. , 2007. , № 1 (36). - с. 40-45.

[5] Результати аналізу порушень, які сталися протягом 2015 — першого півріччя 2016 років на АЕС України/ [С.В. Недбай, Д.В. Воронцов, О.М. Горпинченко, О.В. Печериця] - Ядерна та радіаційна безпека, 2016, Вип. 3(71). - с. 15-18.

Є.О. Зайцев, М.В. Панчик

ВИЗНАЧЕННЯ ХАРАКТЕРИСТИК МЕХАНІЧНИХ ЕЛЕМЕНТІВ ВИМІРЮВАЧІВ ТИСКУ СИСТЕМ КОНТРОЛЮ ТА ДІАГНОСТУВАННЯ СТАБІЛІЗАЦІЇ ЗУСИЛЛЯ В СТЯЖНИХ ПРИЗМАХ ПОТУЖНИХ ГЕНЕРАТОРІВ

Актуальність даної тематики визначається необхідністю контролю тиску пресування осердя статора потужних генераторів при їх виготовленні та експлуатації, що дозволяє підвищити достовірність діагностування технічного стану та забезпечити безпечність їх експлуатації.

Як наведено в [2] при складанні осердя статора, контроль тиску пресування осердя статора доцільно проводити з використанням картини нерівномірності торцевої поверхні відносно пресувальної плити, тобто її відхилення від площинності в як можна більшій кількості точок.

При реалізації описаного методу контролю виникла задача в реалізації спеціального пружного елементу механічні характеристики, якого залежать від навантаження, а характеристика лінійна при малих прогинах [3, 4, 5]. Зміна навантаження(тиск) фіксується через зміну геометричних параметрів пружного елементу ємнісним сенсором.

Отримані характеристики та дослідний зразок приведено на рис.1.

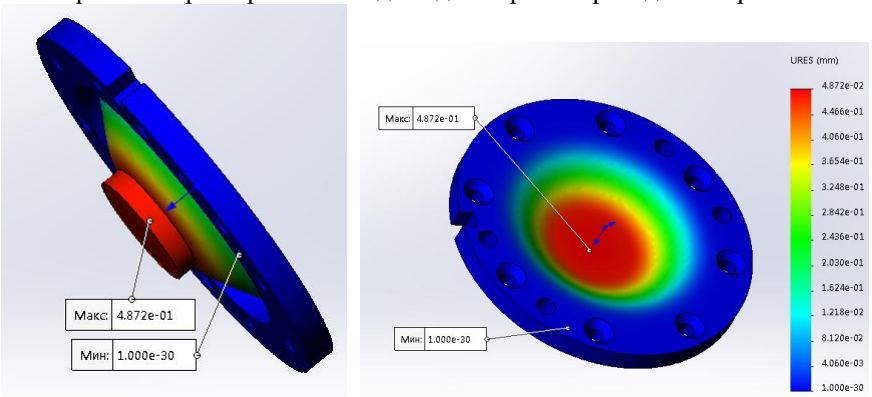


Рис. 1 Вимірювальна мембрана під дією питомого тиску

При моделюванні було враховано, що під час пресування осердя питомий тиск p_X діє на спеціальний пружний елемент, що деформується (прогнеться) під дією навантаження. Переміщення W_X жорсткого центру пружного елементу при цьому згідно з [1] може бути визначене за формулою

$$W_X = A_P \frac{p_X \cdot R_0^4}{Eh^3},$$

де $A_p = f(k) = \frac{3(1-\mu^2)}{16} \cdot \frac{k^4 - 1 - 4k^2 \ln k}{k^4}$, $k = R_0 / r_0$, μ – коефіцієнт Пуассона, E – модуль пружності.

Для розробки та дослідження характеристик пружного елементу було використано стандартну програму розрахунку навантажень, що базується на використанні методів чисельного моделювання(метод кінцевих елементів).

Отже, проведені дослідження з використанням створеної моделі спеціального пружного елементу показали, що максимальний прогин мембрани складає 0,487 мм та є близьким до розрахункового, а саме 0,5 мм. Це дозволило підтвердити адекватність прийнятої методики розрахунку механічного компоненту системи контролю зусилля пресування осердя статора при його складанні.

[1] Андреева Л Е. Упругие элементы приборов. 2-е изд. перераб. и доп. М: Машиностроение, 1981. 392 с.

[2] Зайцев Є.О., Левицький А.С., Панчик М.В. Особливості процесу пресування осердя статора потужного турбогенератора. Електромеханічні та енергетичні системи. Методи моделювання та оптимізації: Збірник наукових праць XVII Міжнародної науково-технічної конференції молодих учених і спеціалістів, 11-12 квітня 2019 м. Кременчук, Україна, 2019. С.81-83.

[3] Писаренко Г. С. Сопротивление материалов: монография. 5-е изд. К.: Вища школа, 1986. 775 с.

[4] Феликсон Е. И. Упругие элементы приборов : монография. М.: Машиностроение, 1977. 311 с.

[5] Guide to the Measurement of Force. URL: http://resource.npl.co.uk /docs/science_technology/mass_force_pressure/clubs_groups/instmc_weighing_panel/forceguide.pdf. (дата звернення : 29.11.2019).

Ю.О. Фуртат

ПРО ДЕЯКІ ПІДХОДИ ДО МОДЕЛЮВАННЯ СИЛОВИХ ЕНЕРГЕТИЧНИХ УСТАНОВОК

Процес розвитку сучасних автономних силових енергетичних установок характеризується стійкою тенденцією до розширення галузі їх застосування та зростання рівня складності [1]. Від систем з простими аналоговими регуляторами автономні силові установки розвинулись до сучасних систем з комп'ютерним керуванням і, як наслідок, з новими можливостями, зокрема гнучкістю алгоритмів керування, забезпеченням віддаленого контролю тощо. Значно підвищились вимоги щодо функціональності та надійності таких установок, покращення їх динамічних характеристик, розвитку підсистем контролю та діагностики, розширенню та ускладненню функцій керування із застосуванням нових смарт-технологій. Одним із шляхів забезпечення зазначених вимог є подальший розвиток методів і засобів математичного і комп'ютерного моделювання як самих автономних силових енергетичних установок, так і їх складових частин, а також залучення їх до процесів проектування, керування, контролю та діагностування.

Характерним прикладом силових енергетичних установок є електромеханічні системи, які широко використовуються в машинобудуванні, енергетиці, при видобутку корисних копалин, в металургії, на транспорті тощо. Оскільки під час функціонування електромеханічних систем спостерігається значне споживання електричної енергії, протягом багатьох років інтенсивно ведуться роботи по покращенню їх енергетичних характеристик. Також актуальними залишаються задачі покращення динамічних характеристик завдяки використанню систем автоматичного керування. В залежності від поставленої задачі автоматизована система керування повинна забезпечувати необхідні режими функціонування електромеханічної системи з контролем швидкості, потужності, механічного моменту, частоти тощо. Зараз для сучасних електромеханічних систем намітилась стійка тенденція зростання вимог щодо точності відпрацювання складних рухів виконавчих механізмів при умові збільшення швидкості їх переміщення. Це стало можливим з появою потужних напівпровідникових силових перетворювачів та високоточних цифрових систем керування, які поклали початок розвитку мехатронних систем.

Функціональна схема електромеханічної системи мехатронного типу приведена на рис.1. Вона включає три підсистеми: 1 — інформаційну, 2 — енергоелектронну і 3 — електромеханічну.

Інформаційна підсистема містить систему керування, контролю і діагностики (СККД), набір сенсорних пристроїв (НСП), локальний інтерфейс (ЛІ) та зовнішній інтерфейс (ЗІ). *Енергоелектронна* підсистема включає силовий напівпровідниковий перетворювач (СНП) і силовий блок живлення

(СБЖ). *Електромеханічна* підсистема містить виконавчий механізм (ВМ) і електромеханічний перетворювач (ЕМП). Слід відзначити, що в деяких мехатронних системах функціональні блоки можуть відрізнятись від приведених на схемі. Так, наприклад, електромеханічний перетворювач може бути конструктивною ланкою виконавчого механізму, або в деяких мехатронних системах може бути відсутній зовнішній інтерфейс, якщо не передбачається робота в складі групи пристроїв з централізованим управлінням.

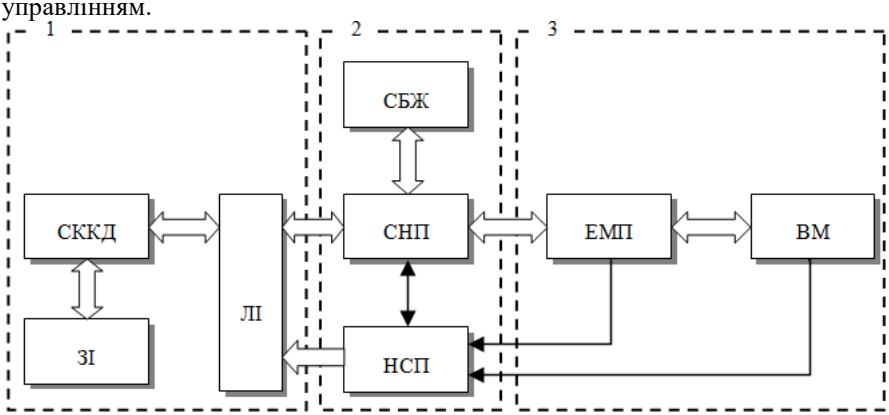


Рис. 1. Електромеханічна система мехатронного типу

Особливістю мехатронних систем є те, що вони охоплюють широкий клас задач завдяки універсальності комп'ютеризованих систем керування, контролю та діагностики. В залежності від особливостей виконавчого механізму (об'єкта керування) в мехатронній системі може використовуватись різний набір сенсорних пристроїв та різні алгоритми вироблення керуючих впливів. Наприклад, для керування асинхронними електродвигунами широкого розповсюдження набув векторний метод з використанням спостерігача Люенбергера, який передбачає використання моделі електродвигуна і виконавчого механізму (рис. 2). Для підвищення ефективності керування складними багатоканальними та багатозв'язними об'єктами використовуються їх еталонні та прогнозні моделі (рис. 3). До таких моделей висуваються додаткові вимоги, зокрема здатність функціонування в режимах реального та прискореного часу, високої надійності, можливості синхронізації поточного стану моделі відносно реально діючого об'єкта тощо.

Використання в мехатронних пристроях комп'ютеризованих систем керування (рис. 2) дозволило не лише підвищити показники якості керування, але й розв'язати комплекс задач, пов'язаних з управлінням складними системами із великою кількістю електромеханічних перетворювачів. Специфіка цих задач полягає в тому, що при виробленні сигналів керування необхідно враховувати їхню взаємозв'язність через спільність об'єкта керування, який може мати складну структуру. Для розв'язування таких задач виникає необхідність створення математичних моделей багатозв'язних

об’єктів керування. Відмітимо, що для таких об’єктів керування побудова параметричних моделей викликає значні труднощі, тому приходиться відшуковувати інші способи їх математичного опису. Ефективним підходом до побудови математичних моделей багатозв’язних динамічних об’єктів є використання математичного опису у вигляді інтегральних рівнянь та їх систем [2].

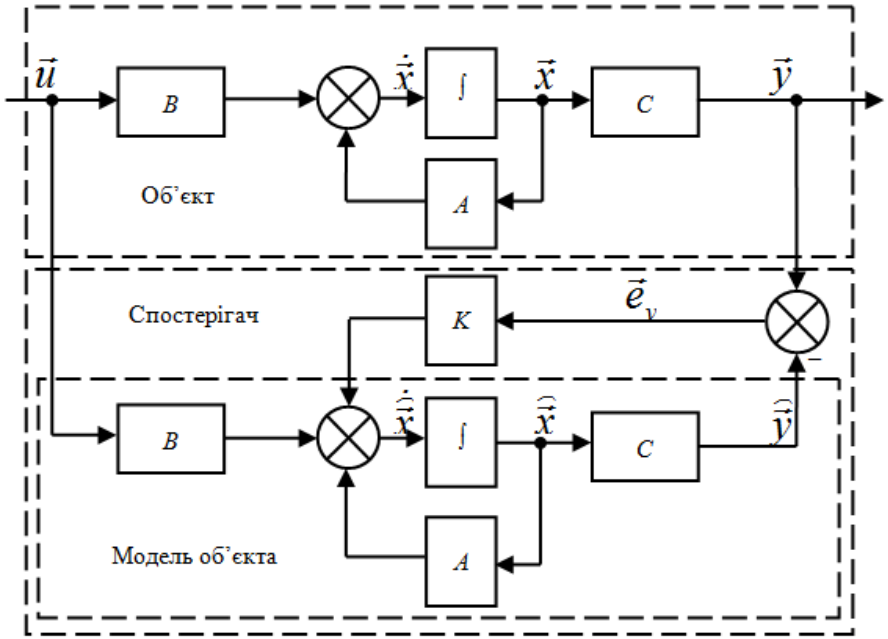


Рис. 2. Векторне керування на основі спостерігача Люенбергера

Відмінною особливістю сучасних мехатронних систем є використання принципів уніфікації, агрегатування та типізації. Це дає змогу проводити конструювання мехатронної системи на основі уніфікованих блоків, які, при потребі, можуть замінюватись аналогічними типовими блоками. Така гнучкість структури мехатронної системи дозволяє оперативно проводити в ній зміни з метою оптимізації структури для конкретного класу задач. В доповнення до структурної гнучкості, мехатронні системи володіють також програмною гнучкістю, завдяки використанню в системах керування, контролю і діагностики програмованих мікроконтролерів та мікрокомп’ютерів. Зміна алгоритмів керування в мехатронних системах, в переважній більшості випадків, проводиться шляхом зміни програмних модулів. Також позитивним моментом для мехатронних систем є суттєве підвищення ефективності алгоритмів керування, контролю та діагностики при використанні в них математичних моделей об’єктів керування. При цьому, на сучасному етапі розвитку мехатронних систем виникла необхідність створення ефективних високошвидкісних алгоритмів для

моделювання динаміки різноманітних виконавчих механізмів як об'єктів керування [3].

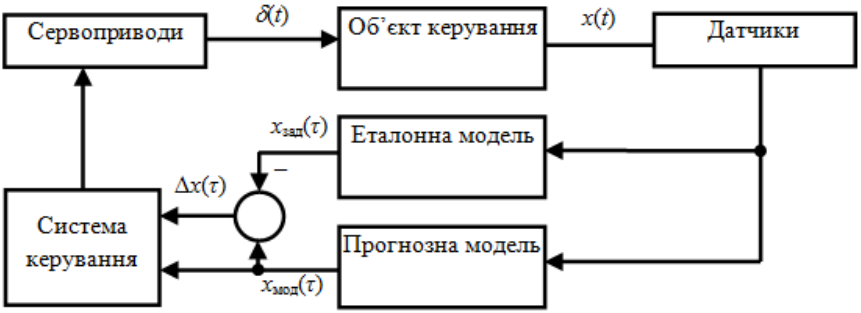


Рис. 3. Схема контролера з використанням еталонної та прогнозної моделей

Отже, особливості сучасних електромеханічних систем слід шукати в площині аналізу властивостей виконавчих механізмів (об'єктів керування) з метою отримання для них відповідних математичних залежностей у такому вигляді, який би давав змогу ефективно розв'язувати задачі їх моделювання.

[1] Андрианов С.Н. Некоторые проблемы теоретического и компьютерного моделирования. Андрианов С.Н. Труды I Междунар. науч.-практ. конф. "Современные информационные технологии и ИТ-образование". Москва, 2005. С. 92–99.

[2] Верлань А.А. Интегральные динамические модели электромеханических объектов: Монография. Верлань А.А., Сагатов М.В., Федорчук В.А. Т.: IQTISOD-MOLYA ISBN 978-9943-13-581, 2015. 328 с.

[3] Верлань А.А. Підходи до побудови скалярних динамічних моделей розподілених ланок керованих електромеханічних систем. Верлань А.А., Федорчук В.А. Математичне та комп'ютерне моделювання. Серія: Технічні науки : зб. наук. праць.– Інститут кібернетики імені В. М. Глушкова НАНУ. Кам'янець-Подільський національний університет ім. Івана Огієнка.– Кам'янець-Подільський: К-ПНУ. 2016. Вип. 13. С. 49-61.

В.В. Станиціна

ВПЛИВ РОЗМІРУ СТАВОК ЕКОЛОГІЧНОГО ПОДАТКУ НА СЕРЕДНЮ ВАРТІСТЬ ТЕПЛОВОЇ ЕНЕРГІЇ ЗА ЖИТТЄВИЙ ЦИКЛ ОПАЛЮВАЛЬНИХ КОТЕЛЕНЬ

Наразі в Україні теплопостачання здійснюється системами централізованого (СЦТ) та децентралізованого теплопостачання. Основним постачальником теплової енергії в СЦТ є опалювальні котельні, побудовані в основному ще за радянських часів, які морально та фізично застарілі. Хоча в останні роки є чітка тенденція виведення з експлуатації опалювальних котелень [1], вони ще довго займатитуть перше місце в теплопостачанні.

Для визначення економічної ефективності будівництва нових об'єктів та впровадження новітніх технологій в СЦТ і прогнозування розвитку системи теплопостачання необхідне проведення досліджень та оцінювання вартості виробництва теплової енергії проектними теплогенеруючими джерелами. Для порівняння різних технологій теплогенерації у світі застосовується метод оцінювання середньої вартості теплоенергії за життєвий цикл - метод LCOH (levelized cost of heat). Показник LCOH визначається як постійна вартість генерації одної кВт·год теплоти, яка дорівнює дисконтованим витратам, понесеним протягом усього життєвого циклу інвестиції [2-3].

Враховуюче постійне зростання екологічних вимог до спалюючих установок та зростання ставок екологічного податку, необхідним є врахування екологічного фактору під час визначенні середньої вартості теплової енергії за життєвий цикл для теплогенеруючих установок, перспективних для будівництва в Україні [4].

У листопаді 2019 р. до Верховної Ради України подано 3 законопроекти щодо збільшення ставок екологічного податку. Одним проектом передбачається поступове зростання ставок податку на певні забруднюючі речовини на 50% до 2030 р. [5], іншим – одночасне зростання ставок в 4 рази, в тому числі й за викиди CO_2 до 40 грн/т [6].

В країнах ЄС ставки податку різняться в десятки раз, в Польщі одні з найнижчих в ЄС, у Швеції – найбільші. В Польщі ставки податку за викиди оксидів сірки та азоту більші на 40%, ніж в Україні, в Швеції – за викиди SO_2 більші у 3,3 разу, NO_x – у 5,8 разу.

З використанням підходу [4] проведено дослідження впливу розміру екологічного податку на середню вартість теплової енергії за життєвий цикл для нових котлоагрегатів різної потужності, які найбільш поширені в опалювальних котельних СЦТ, що працюють на природному газі, кам'яному вугіллі та мазуті. Визначено окремо екологічну складову, обумовлену екологічним податком. За існуючих ставок екологічного податку згадана екологічна складова складає від 0,3% від LCOH для газових котлів до 4,7 % для вугільних.

В разі зростання ставок податку за викиди забруднюючих речовин на 50% згідно [5] екологічна складова середньої вартості за життєвий цикл (податки) зросте на 10% для котлів, що працюють на природному газі, на 32% для котлів, що спалюють мазут та на 43 % для котлів, що працюють на вугіллі. Нерівномірне зростання пов'язане з тим, що в даному законопроекті не згадується про зміну ставки податку за викиди CO_2.

В разі зростання ставок податку за викиди забруднюючих речовин в 4 рази [6], екологічна складова середньої вартості за життєвий цикл (податки) зросте в 4 рази.

В Польщі найнижчі ставки екологічного податку, тому екологічна складова LCOH (податки) для випадку запровадження таких же ставок, як і в Польщі зросте не суттєво для котлів на мазуті (30%); для котлів на вугіллі зросте в 2 рази, а для котлів на природному газі взагалі зменшиться вдвічі (за рахунок меншої ставки податку за викиди CO_2).

У разі запровадження найбільших ставок екологічного податку у ЄС (Швеція), екологічна складова для котлів на вугіллі буде вдвічі більша ніж складова, що враховує інвестиційні, експлуатаційні та паливні витрати, тобто LCOH зросте в 3 рази. Для котлів на природному газі екологічна складова (податки) складе 70% від LCOH, а для мазутних котлів – 85%. Найбільший внесок в цьому випадку має податок за викиди CO_2, ставка податку за який в Швеції в 300 разів більша ніж в Україні.

Таким чином, залежно від ставок екологічного податку за викиди забруднюючих речовин, екологічна складова (податки) середньої вартості теплової енергії за життєвий цикл опалювальної котельні складе від 0,3% від LCOH до 200 %.

[1] Куц Г.О., Маляренко О.Є., Станиціна В.В., Богославська О.Ю. Оцінка стану та прогноз структури палива та енергії для систем теплопостачання України з урахуванням регіональних особливостей. Проблеми загальної енергетики. 2017. Вип. 4 (51). С. 23-32. URL: https://doi.org/10.15407/pge2017.04.023

[2] Baez, M.J., Larriba Martínez, T., 2015. Technical Report on the Elaboration of a Cost Estimation Methodology. No. D.3.1. Creara, Madrid, Spain.

[3] Projected Costs of Generating Electricity. International Energy Agency (IEA). 2010. 218 p.

[4] Станиціна В.В. Артемчук В.О. Врахування екологічної складової у середній вартості теплової енергії за життєвий цикл. Зб. тез конференції «Безпека енергетики в епоху цифрової трансформації», м. Київ, 20 грудня 2019 р. ІПМЕ ім. Г.Є. Пухова НАН України. 2019. С. 86-89.

[5] Проект Закону про внесення змін до Податкового кодексу України щодо збільшення ставок екологічного податку та впровадження європейських принципів модернізації української промисловості № 2367-1 від 18.11.2019.

[6] Проект Закону про внесення змін до Податкового кодексу України щодо збільшення ставок екологічного податку з метою проведення додаткових заходів, що сприятимуть зміцненню здоров'я та покращенню медико-санітарного забезпечення громадян України № 2367 від 01.11.2019 р.

А.В. Давидюк

КІБЕР РИЗИК. ПІДХІД ДО ОЦІНЮВАННЯ КІБЕР РИЗИКІВ

Актуальність даної тематика показана в [1]. Рекомендації NIST 8183 визначають кібер ризик як ризик фінансових втрат, збоїв у роботі або пошкодження у результаті відмови цифрових технологій, що використовуються для інформаційних та/або операційних функцій, впроваджених до промислової системи за допомогою електронних засобів, із-за несанкціонованого доступу, використання, розкриття, порушення, модифікації або поломки промислової системи [1].

За анологією з міжнародним стандартом ISO 27001:2013 в рамках системи менеджменту інформаційної безпеки для управління кібер ризиками рекомендується шість базових кроків:

1. Визначитись з методологією оцінювання кібер ризиків;
2. Впровадження процедури оцінювання кібер ризиків;
3. Впровадження процедури обробки ризиків;
4. Створення звіту про оцінювання кібер ризиків в системі менеджменту інформаційної безпеки;
5. Створення заяви про застосовуваність
6. Створення плану обробки кібер ризиків [2].

Також даний стандарт в рамках впровадження процедури оцінювання ризиків вимагає визначитись з п’ятьма складовими:

1. Визначити причину втрати конфіденційності, цілісності та доступності;
2. Визначити власників ризику;
3. Визначитись з критеріями оцінювання наслідків та імовірності;
4. Визначитись з тим як буде обчислюватись значення ризику;
5. Визначити критерії прийняття ризику [2].

На перший погляд все є доволі зрозумілим для виконання, проте постає питання скільки ризиків необхідно ідентифікувати, враховуючи те, що для одного активу може бути більше десяти загроз, для кожної загрози біля п’яти вразливостей, тоді загальна кількість ризиків може сягати 2500. Для малої за розміром компанії така кількість ризиків може бути надлишковою. Замість ефективного процесу управління ризиками можливим результатом можуть стати великі затрати на обробку ризиків, порушення роботи персоналу, який буде заляканий надмірними заходами з безпеки та інше.

Постає задача визначення підходу до управління кібер ризиками як частини ризиків інформаційної безпеки, який міг би забезпечити баланс між необхідним рівнем іформаційної безпеки і неперервністю бізнес процесів організації.

Для вирішення даної задачі необхідно класифікувати організації за кількістю інформаційних активів на малі, середні та великі.

З урахуванням даної класифікації та спеціалізації організації виконати приорітезацію активів, залишивши поки активи з найменшим пріоритетом за межами процедури оцінювання ризиків, для активів що залишились визначити однакову усереднену для всіх активів кількість загроз з найвищою імовірністю, для цих загроз визначити однакому усереднену кількість найбільш розповсюджених вразливостей з використанням міжнародних баз вразливостей типу NVD та інші [3]. Після чого перейти до наступних етапів управління ризиками.

Такий підхід дасть можливість на етапі створення системи менеджменту інформаційною безпекою пройти швидко етап впровадження процесу управління ризиками без надлишкового навантаження із забезпеченням допустимого рівня інформаційної безпеки. У подальшому, звісно, в рамках створеної системи менеджменту інформаційної безпеки до процесу управління ризиками можна включати нові активи та розширювати спектр існуючих загроз, що дасть змогу персоналу організації поступово, без страху і порушення функціонування бізнес процесів усвідомити важливість виконання вимог політики безпеки та забезпечити ефективне їх виконання.

Також, враховуючи вищезазначену класифікацію організацій, доцільно розділити відомі методики оцінювання ризиків на прості та складні за кількістю критеріїв, що використовуються для даної процедури. Наприклад для малих організацій ризик обчислювати як суму або добуток оцінок імовірності та наслідків, а для середніх та великих - як суму або добуток оцінок активу, загрози та вразливості.

Отже, проведені дослідження показали, що, враховуючи розвиток інформаційних технологій, як безпосереднє середовище кібер ризиків, важливим для систем менеджменту інформаційної безпеки є не лише забезпечення вимогам міжнародних стандартів, а й можливість їх швидкого масштабування, наявність автоматизованих інструментів для контрою процедури управління ризиками, версійності та змін у документації, чому будуть присвячені подальші дослідження.

[1] Draft NISTIR 8183 Cybersecurity Framework Version 1.1 25 Manufacturing Profile [Електронний ресурс] /[K. Stouffer, T. Zimmerman, C. Tang та ін.] // Rev. 1. – 2020. – Режим доступу до ресурсу: https://csrc.nist.gov/publications/detail/nistir/8183/rev-1/draft.

[2] ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements [Електронний ресурс] / K.Passia, A. Wolf, L. Lindsay, C. Bazin de Caix // 2. – 2019. – Режим доступу до ресурсу: https://www.iso.org/ru/standard/54534.html.

[3] NATIONAL VULNERABILITY DATABASE [Електронний ресурс] // Information Technology Laboratory National Vulnerability Database – Режим доступу до ресурсу: https://nvd.nist.gov/.

Д.В. Савельєв

ФОРМУВАННЯ ПЕРЕЛІКУ АКТУАЛЬНИХ ЗАГРОЗ БЕЗПЕКИ ВЕБ-СИСТЕМ ТА ДОДАТКІВ НА СТАДІЇ РОЗРОБКИ

Загрози безпеки програмної системи зумовлені умисними чи ненавмисними діями зловмисників, недотримання заходів із забезпечення захищеності системи розробниками, діями користувачів системи (у тому числі адміністраторів та модераторів), які можуть мати серйозні негативні наслідки.

Формування переліку загроз безпеки веб-систем базується на актуальних рекомендаціях із забезпечення захищеності веб-систем для розробників та адміністраторів системи, серед яких – рекомендації OWASP для розробників веб-орієнтованого програмного забезпечення [1] та рекомендації Українського державного центру реагування на комп'ютері інциденти CERT-UA з безпеки веб-ресурсів для адміністраторів [2]:

- дотримання актуальних вимог безпеки;
- використання безпечних фреймворків та бібліотек;
- управління оновленнями програмного забезпечення;
- забезпечення захищеного доступу до даних;
- шифрування та безпека даних;
- перевірка вхідних даних;
- захист «цифрової особистості»;
- управління доступом;
- всебічний захист інформації;
- моніторинг та ведення журналів безпеки;
- коректне опрацювання помилок та виключень;
- періодична перевірка директорій на сервері веб-ресурсу;
- уникнення вразливих конфігурацій веб-сервера;
- розмежування веб-додатків.

Базуючись на наведених вище рекомендаціях, можна визначити перелік типів загроз, що можуть виникнути внаслідок їх невиконання. Перелік загроз наведено у таблиці 1.

Реалізація наведених типів загроз безпеки веб-систем може мати наступні наслідки:

- порушення конфіденційності інформації;
- порушення цілісності інформації;
- порушення доступності інформації.

У таблиці 1 для кожного типу загрози вказуються відповідні можливі наслідки.

Недоліки системи, наявність яких допускає реалізацію загроз веб-системи, можуть виникати на усіх етапах розробки. Для класифікації перелічених загроз стадії розробки веб-системи можна використати етапність

життєвого циклу розробки програмного забезпечення, запропоновану некомерційною організацією WASC (The Web Application Security Consortium), що раніше активно займалась розробкою та просуванням стандартів безпеки додатків, у проекті WASC Threat Classification від 2010 року, та має назву «Представлення фази розвитку». Пропонується розподіл типів загроз за трьома фазами розробки – проектування, реалізація та впровадження [3]. Відношення кожного типу загроз відповідно до такого розподілу наведено у таблиці 1.

Таблиця 1

Перелік загроз та можливі наслідки їх реалізації

Можливий тип загрози	Можливі наслідки реалізації загрози			Фаза розробки		
	Порушення конфіденційності	Порушення цілісності	Порушення доступності	Проектування	Реалізація	Впровадження
Негативний вплив на ПЗ з боку засобів розробки	-	+	+	+	+	-
Шкідливі закладки у коді	+	+	+	-	+	-
Зловживання функціональністю	+	-	-	+	-	-
Використання компонентів з відомими вразливостями	+	+	+	+	+	+
Ін’єкції	+	+	+	-	+	-
Міжсайтовий скриптинг	+	+	+	-	+	-
Виконання команд, не передбачених системою	+	+	+	+	+	-
Порушення автентифікації	+	+	+	+	+	-
Перехоплення HTTP-cookies	+	-	-	+	+	-
Несанкціонований контроль доступу	+	+	+	+	+	+
Використання чутливих даних	+	+	+	+	+	+
Доступ до файлів сервера через URL	+	+	+	-	+	+
Аналіз мережного трафіку	+	-	-	+	+	+
Сканування мережі	+	+	+	-	-	+
Впровадження хибного маршруту/об’єкта мережі	+	+	+	-	-	+

Недостатнє ведення журналів та моніторинг	+	+	+	-	+	+
Витік інформації	+	+	+	+	+	+
Небезпечна десеріалізація	+	+	+	-	+	-
Відмова в обслуговуванні	-	+	+	-	+	+
Розщеплення HTTP-запитів	+	+	+	-	+	-
Зовнішні об’єкти XML	+	+	-	-	+	+
Помилки безпеки	+	+	+	-	-	+
Індексація каталогів веб-сервера	+	+	+	-	-	+
Вплив через вразливості інших веб-ресурсів, розміщених на тому ж сервері	+	+	+	-	-	+

Висновки

Визначення переліку загроз безпеки розроблюваної системи є одним із ключових етапів процесу оцінки ризиків, якість виконання якого в свою чергу забезпечує ефективність аналізу безпеки та контролю ризиків.

Наведено актуальні рекомендації щодо забезпечення безпеки процесу розробки веб-систем та додатків. Визначено перелік актуальних типів загроз, виходячи з невиконання наведених рекомендацій та наслідки їх реалізації. Для кожного типу загроз визначено фазу життєвого циклу розробки проекту, під час якої аналіз безпеки необхідний контроль загрози.

[1] Anton K., Manico J., Bird J. 10 Critical Security Areas That Software Developers Must Be Aware Of // OWASP Top Ten Proactive Controls Project. 2018. – URL: https://owasp.org/www-pdf-archive/OWASP_Top_10_Proactive_Controls_V3.pdf.

[2] Рекомендації CERT-UA з безпеки вебресурсів. // CERT-UA. – URL: https://cert.gov.ua/recommendations/25

[3] Thread Classification Development View // The Web Application Security Consortium. – URL: http://projects.webappsec.org/w/page/13246969/Threat Classification Development View

О.О. Попов[1,2], А.В. Яцишин[1,2], В.О. Артемчук[2,1], В.О. Ковач[3,1], А.О. Туревич[1], В.О. Куценко[1]

СВІТОВИЙ ДОСВІД ПОБУДОВИ СИСТЕМИ МОНІТОРИНГУ СТАНУ АТМОСФЕРНОГО ПОВІТРЯ НА БАЗІ РУХОМОГО СКЛАДУ ГРОМАДСЬКОГО ТРАНСПОРТУ

[1] *ДУ «Інститут геохімії і навколишнього середовища НАН України», Київ*
[2] *Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Київ*
[3] *Навчально-науковий інститут неперервної освіти НАУ, Київ*

В розвинених країнах світу для моніторингу стану атмосферного повітря (МСАП) використовуються, як правило, великі стаціонарні станції, які об'єднуються в державну мережу моніторингу. Для точного визначення рівня забруднення повітря тими чи іншими забруднюючими речовинами ці станції наповняються дуже дорогим обладнанням, також вирішуються проблеми репрезентативності, тобто вибору оптимального розміщення станції для вирішення поставлених задач, електрозабезпечення, захисту від вандалізму тощо. Це все значно ускладнює широке використання таких великогабаритних станцій для контролю якості атмосферного повітря у щільно забудованих містах. Так, в м. Києві таких постів спостереження лише 16. Через неможливість розміщення достатньої кількості стаціонарних станцій виникає проблема низької просторової роздільної здатності вимірювань, що обмежує можливість захоплення просторової неоднорідності поля забруднення повітря. Особлива просторова неоднорідність полів забруднення повітря у міському середовищі виникає через ряд факторів, таких як: локальність джерел викидів (наприклад, підприємства, структури руху) і специфічний міський ландшафт (наприклад, топографія, вуличні «каньйони», зелені зони тощо).

Вирішити ці проблеми можливо шляхом використання у системах моніторингу дешевших малогабаритних датчиків, які закріплюються на транспортні засоби, які рухаються визначеними маршрутами. Такими рухомими об'єктами можуть бути трамваї, тролейбуси, автобуси, маршрутки, які є частиною громадського транспорту (ГТ) міста.

Аналіз іноземної наукової літератури з даної проблематики показав, що в ряді промислових міст розвинених країн світу (Ченаї (Індія) [10], Лозанні і Цюриху (Швейцарія) [3], Римі (Італія) [8] та в декількох провінціях Китаю [7, 9]) підіймаються питання використання рухомого складу ГТ для здійснення МСАП. Створення проєкту системи МСАП зачіпає декілька категорій проблем, тобто завдань які поєднані між собою, зокрема:

- «математичне завдання» – створення моделі дослідження, підрахунок кількості одиниць необхідного обладнання, створення програмного забезпечення для проекту;
- «економічне завдання» – оптимальні показники вартості обладнання та робіт для проекту;

- «технічне завдання» – підбір обладнання, робота над мінімізацією похибок дослідження;
- проблема SPL (Simple Plant Location Problem) – витрати на активацію та обслуговування (з однієї сторони вартість датчиків, а з іншої – якість моніторингу) розглядаються в рамках багатоцільового підходу.

Кожний окремий проєкт підходить до розв'язання зазначених завдань по різному. Так, дослідники G. Lancia та ін. запропонували вирішення математичного завдання, запозичивши алгоритми в генетиці. Зокрема, генетичні алгоритми є потужним підходом при вирішенні проблеми з жорсткою оптимізацією. Їх використання є доречним з двох основних причин. По-перше, в генетичних алгоритмах дуже легко здійснити зміни в цілі функції (наприклад, введення штрафних санкцій, навіть нелінійних, або наявність витрат, виражених у вигляді великого перемикача «якщо-то-інше»). По-друге, кожне рішення має представляється у вигляді бінарного вектору з N компонентів (по одному для кожного маршруту шини), у яких біти відповідають активованим маршрутам. У своїй публікації [8] вчені використовували генетичний алгоритм для розрахунку кількості датчиків, необхідних для моніторингу одного міста, підбіру маршрутів ГТ, на яких буде встановлено ці датчики, та місцерозташування вимірювачів на кузовах транспортних засобів.

Команда дослідників з Китаю під керівництвом L. Liu також займалася вирішенням математичного та інформаційно-технологічного завдання МСАП [9]. Вони зосередили свою увагу на аспектах технічної побудови системи моніторингу, а саме об'єднанні систем датчиків, які встановлено на маршрутних автобусах та центрі збору інформації (Mobile Sensing Information Gathering Centers – MSIGCs). Останній не тільки збирає та сортує інформацію, що надходить, а й здійснює автоматичний аналіз та структурування даних в реальному часі, що значно спрощує інформування пасажирів ГТ та мешканців міст в цілому. Такі системи можна використовувати для моніторингу якості повітря, моніторингу заторів, тощо.

Ще одна китайська група вчених запропонувала використання багатофункціональних модулів для ГТ [7], що не тільки допомагають здійснювати моніторинг якості повітря та трафік руху, але також виступають свого роду вишками мобільного зв'язку. На їх думку, така багатофункціональність збільшить популярність використання таких модулів серед перевізників, особливо – громадського транспорту.

В місті Ченаї, Індія H. Prasad Raju та ін. відтворили на практиці систему МСАП, використовуючи датчики показників якості повітря (NO_2, CO, SO_2) та GPS, які об'єднані в систему завдяки ARM процесору по каналам Інтернет речей (зв'язок на основі геоінформаційних систем). Після цього отримана інформація надходить до центру обчислень та у вигляді числової та візуальної інформації з'являється на інформаційному порталі. Для покриття досліджуваного району міста було обрано три маршрути ГТ. Дослідники наголошують, що мережа МСАП на основі ГТ економічно вигідна, дешева та

ефективна для постійного моніторингу якості повітря, проте точність залежить від кількості рейсів ГТ у певний проміжок часу, зокрема вночі точність буде падати через відсутність або недостатність рейсів ГТ [10].

Важливим аспектом функціонування системи моніторингу є типи, способи кріплень, а також механізми забору повітря контролюючими датчиками, які в своїй роботі досліджували Adrian Arfire та ін. [3]. Дослідження показали, що використання дешевих датчиків у мобільній системі контролю якості повітря призводить до спотворення сигналу, а також до зниження достовірності отриманої інформації. Цю проблему можливо частково вирішити за допомогою спеціальних активних пробовідбирачів (так званих сніферів). В проектуванні систем МСАП доцільно використовувати бездротові системи датчиків (БСД), у зв'язку з їх меншою вартістю та простотою монтажу та експлуатації. Оскільки вартість покриття цілого міста БСД все ще досить висока, то більшість проєктів розглядають або суміш статичних та мобільних вузлів або виключно мобільні вузли для БСД. Дослідження ефективності боксів датчиків проводилося за допомогою громадських автобусів у місті Лозанна та трамваїв в Цюріху. Найбільш ефективні бокси для датчиків з виносним пробовідбірником та активною подачею повітря на основі насосу з обтічним коробом. Дещо поступаються їм у ефективності бокси із пасивним виносним сніфером та з активним невиносним повітровідбирачем.

Ще одним способом розв'язання вказаних завдань виступає залучення концепції Громадських обсерваторій (ГО). Поняття ГО не дуже поширене [4]. Воно передбачає залучення громадян для моніторингу навколишнього середовища, а також надає їм право прийняття наукових та політичних рішень, які спрямовані на покращення можливостей спостерігати, розуміти та вживати супутніх дій для захисту навколишнього середовища. В Україні функціонує декілька проєктів МСАП на основі концепції ГО: (Save Dnipro, SaveEcoBot та інші). Їх особливістю є те, що громадяни виступають в ролі замовників та тримачів станцій моніторингу, а також надають доступ до інформації зі своєї станції громадській організації та світовим базам з моніторингу якості повітря. Тобто, громадяни виступають у ролі інформаторів про стан довкілля. На сьогодні в Україні поширення набули лише стаціонарні датчики контролю за якістю повітря.

Отже, підсумовуючи вищесказане, можна констатувати, що досвід побудови систем контролю якості повітря на базі рухомого складу громадського транспорту в Україні відсутній, як, по суті, і теоретичні дослідження в цій галузі, а наявні публікації іноземних фахівців здебільшого стосуються окремих аспектів цієї проблеми, а тому не можуть бути безпосередньо використані для побудови таких систем в Україні. У зв'язку цим, в рамках перемоги в конкурсі науково-технічних проєктів установам НАН України, що реалізовуватимуться у 2020 році, авторами було отримано фінансування на виконання проєкту, метою якого є розроблення методології побудови системи контролю якості повітря на базі рухомого складу громадського транспорту для підвищення ефективності Державної системи

моніторингу довкілля згідно європейських вимог та стандартів. На основі даної методології побудови системи контролю якості повітря на базі рухомого складу громадського транспорту можна буде проектувати, обґрунтовувати та оптимізувати такі системи, що дасть можливість зменшити витрати на комплексний аналіз екологічного стану міста або регіону, підвищити ефективність робити системи моніторингу України в цілому, що, в свою чергу, дозволить формувати обґрунтовані управлінські рішення щодо зменшення техногенного впливу техногенних об'єктів на довкілля [1, 2, 5, 6].

[1] Попов О.О. Математичне та комп'ютерне моделювання техногенних навантажень на атмосферу міста від стаціонарних точкових джерел забруднення [Текст] : автореф. дис. ... канд. техн. наук : 01.05.02 / О.О. Попов ; [Ін-т проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України]. – К., 2010. – 20 с.

[2] Яцишин А.В. Комп'ютерні засоби прогнозування техногенних навантажень на атмосферу / А.В. Яцишин, О.О. Попов, В.О. Артемчук // Східно-Європейський журнал передових технологій. – 2009. – Вип. 5/2 (41). – С. 33–36.

[3] Arfire A. Enhancing Measurement Quality Through Active Sampling In Mobile Air Quality Monitoring Sensor Networks / A. Arfire, A. Marjovi, A. Martinoli // Proceedings of the IEEE International Conference on Advanced Intelligent Mechatronics (Banff, Alberta, Canada, July 12–15, 2016). – 2016. – pp. 313–321.

[4] Castell N. Mobile technologies and services for environmental monitoring: The Citi-Sense-MOB approach / N. Castell, M. Kobernus, H.-Y. Liu, P. Schneider, W. Lahoz, A.J. Berre, J. Noll // Urban Climate. – 2015. – Vop. 14, Part 3. – pp. 370–382.

[5] Iatsyshyn A.V. The Methodology of Future Specialists Teaching in Ecology Using Methods and Means of Environmental Monitoring of the Atmosphere's Surface Layer / A.V. Iatsyshyn, O.O. Popov, V.O. Kovach, V.O. Artemchuk // Journal of Information Technologies in Education. – 2018. – Iss. 66, No 4. – pp. 217–230.

[6] Iatsyshyn A.V. The Principles and Methods of Ecological Safety Management Through the Data of Air Monitoring Network Analysis / A.V. Iatsyshyn, Yu.G. Kutsan, V.O. Artemchuk, I.P. Kameneva, O.O. Popov, V.O. Kovach // Elektronne modelyuvannya. – 2019. – Vol. 41, No. 4. – pp. 85–101.

[7] Kang L. A Public Transport Bus as a Flexible Mobile Smart Environment Sensing Platform for IoT / L. Kang, S. Poslad, W. Wang, X. Li, Y. Zhang, C. Wang // Proceedings of the 2016 12th International Conference on Intelligent Environments (London, UK, September 14-16, 2016). – 2016. – pp. 1–8.

[8] Lancia G. A Facility Location Model for Air Pollution Detection / G. Lancia, F. Rinaldi, P. Serafini // Mathematical Problems in Engineering. – 2018. – pp. 1–8.

[9] Liu L. A Fault-Tolerant Mobile Sensing Information Gathering Center (MSIGC) Using Public Transport Buses to Instrument a Smart City / L. Liu, J. Duan, Z. Xiao, C. Wang, X. Li // Proceedings of the 2017 9th International Conference on Advanced Infocomm Technology (Chengdu, China, November 22–24, 2017). – 2017. – pp. 233–238.

[10] Raju H.P. Urban Mobile Air Quality Monitoring Using GIS, GPS, Sensors and Internet / H.P. Raju, P. Partheeban, R.R. Hemamalini // International Journal of Environmental Science and Development. – 2012. – Vol. 3, No. 4. – pp. 323–327.

Ю.О. Кириленко[1], І.П. Каменева[1], О.О. Попов[2,1], А.В. Яцишин[2,1], В.О. Артемчук[1,2]

ОЦІНКА РАДІОЛОГІЧНИХ НАСЛІДКІВ ПОДІЙ ІЗ РОЗЛИВОМ РІДКИХ РАДІОАКТИВНИХ СЕРЕДОВИЩ В КОНТЕКСТІ АНАЛІЗУ БЕЗПЕКИ АЕС

[1] *Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Київ*
[2] *ДУ «Інститут геохімії і навколишнього середовища НАН України», Київ*

Вступ. На сьогодні нормативні документи України та документи експлуатуючої організації ДП НАЕК «Енергоатом» [1]-[8] включають в себе основні вимоги щодо проведення оцінки радіаційних наслідків порушень нормальної експлуатації, проектних, поза-проектних аварій на АЕС.

У світлі проведення імовірнісного аналізу безпеки для енергоблоків українських АЕС та введення вимог НРБУ-97/Д-2000 [5] щодо потенційного опромінення населення, в останні десятиріччя події із розливом рідких радіоактивних середовищ (РРС) на АЕС розглядаються як порушення нормальної експлуатації (події, частота реалізації яких може перевищити значення 10^{-2} 1/рік).

Перелік подій та критерії оцінки. В рамках оцінки порушень нормальної експлуатації із розливом РРС на АЕС України в загальному випадку можна виділити наступні можливі події:

− пошкодження ємності високоактивних сорбентів у приміщенні зберігання рідких відходів;

− розущільнення випарного апарата установки з переробки трапних вод у приміщенні спецкорпусу;

− розущільнення випарного апарата з переробки брудного конденсата з виходом середовища в приміщення спецкорпусу;

− пошкодження баку брудного конденсату з виходом середовища в приміщення спецкорпусу;

− пошкодження трапного баку з виходом середовища в приміщення спецкорпусу або зберігання рідких відходів;

− пошкодження ємності кубового залишку з виходом середовища в приміщення спецкорпусу.

Відповідно до НРБУ-97/Д-2000 [5], для даних подій діє критерій прийнятності як для умов поточного опромінення населення, а саме 40 мкЗв на рік з урахуванням всіх шляхів опромінення (за межами санітарно-захисної зони АЕС).

Оцінка доз. Оцінка дозових навантажень на населення для випадків порушень нормальної експлуатації на АЕС проводиться відповідно до методики [7], яка передбачає розрахунок дози для представника населення референтного віку τ як суму

$$E_\tau(x) = \sum_i \left[E^{air}_{\tau,i}(x) + E^{srf}_{\tau,i}(x) + E^{ing}_{\tau,i}(x) \right]$$

де x – відстань від джерела викиду;

$E_{\tau,i}^{air}$, $E_{\tau,i}^{srf}$, $E_{\tau,i}^{ing}$ – ефективні дози для референтного віку τ, сформовані i-м радіонуклідом за рахунок наступних шляхів опромінення: інгаляційне надходження і зовнішнє опромінення від хмари викиду, зовнішнє опромінення від випадіння на поверхню ґрунту та пероральне надходження.

Складові ефективної дози розраховуються на базі вихідних даних атмосферної моделі та дозових коефіцієнтів відповідно до шляху опромінення та референтного віку представника населення.

Формування викиду. Згідно з результатами проведеного аналізу інцидентів із розливом РРС у технологічних приміщеннях та їх радіаційних наслідків, огляду сучасних засобів оцінки та вимог з боку оцінки радіаційних наслідків [9], [10] було проведено дослідження у напрямку інтеграції комп'ютерних засобів моделювання – розробка математичної моделі характеристик джерела викиду, тобто миттєвої об'ємної концентрації радіонукліду у повітрі технологічного приміщення та потужності атмосферного викиду при аваріях із розливом РРС [11].

Для моделювання процесу формування характеристик та параметрів радіоактивного викиду в атмосферу щодо подій з розливом РРС обрано середовище MathCad, де при розв'язанні системи балансових диференційних рівнянь чисельними методами можна отримати шукані параметри викиду.

Розроблена математична модель базується на елементах теорії нестаціонарного тепло- та масообміну при випаровуванні з поверхні рідини, недогрітої до температури кипіння. Фізична модель включає наступні об'єкти: РРС, радіоактивна паро-аерозольна суміш, повітряні середовища припливної та витяжної вентиляції, аерозольні фільтри, а також основні будівельні конструкції приміщення. До визначальних процесів в моделі належать процеси випаровування радіоактивної рідини, її винесення з приміщення повітрям припливно-витяжної вентиляції та частковий захват матеріалом фільтруючих засобів.

Також розроблено ряд спрощених підходів щодо формування викиду при розливах РРС та розподілу радіонуклідів в системі «рідина-пара» [12]-[15]. Вони засновані на результатах досліджень (модельних та експериментальних даних) в контексті нормальної експлуатації, що зведені в стандартах та керівництвах регулюючого органу США NRC кінця 20 сторіччя та використовуються до сьогодні. До останніх досліджень у напрямку визначення інтенсивності випаровування з відкритих поверхонь рідин можна віднести [16]-[19].

Особливості використання атмосферних моделей. Викиди через технологічні приміщення спецкорпусу АЕС відбуваються через вентиляційну трубу висотою 100м. В практиці оцінок для таких висот зазвичай використовуються модель точкового джерела та спрощені гаусові моделі переносу з типовою параметризацією атмосферної дисперсії за Паскуїлом [7].

В умовах викиду з низьких труб бажано враховувати ефект аеродинамічного затінення від розташованої поряд будівлі на

проммайданчику АЕС (рис. 1). В методі покращеної оцінки застосовуються CFD/LES-моделювання. Слід зазначити, що наразі прецизійні моделі такого типу не використовуються для аналітичних обґрунтуваннях безпеки АЕС України [8].

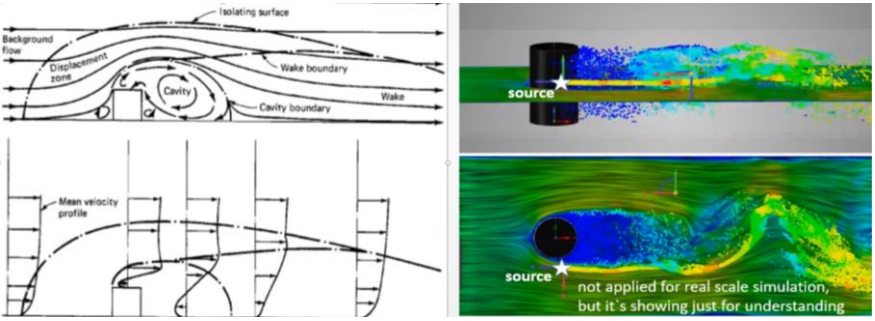


Рис. 1 – Ефект аеродинамічного затінення джерела викиду

Висновки. Оцінка радіологічних наслідків в контексті аналізу безпеки діючих енергоблоків України регулюється чинними нормами, правилами та стандартами з ядерної та радіаційної безпеки. Відповідно до практики проведення подібних оцінок та результатів імовірнісного аналізу безпеки, події із розливом РРС розглядаються як порушення нормальної експлуатації, для яких встановлено критерій щодо радіологічного впливу на населення – 40 мкЗв за рік за рахунок всіх шляхів опромінення. На сьогодні для всіх енергоблоків України підтверджено виконання даного критерію.

Однак, у випадку зміни складу РРС та/або умов їх зберігання на проммайданчиках АЕС події з розливом РРС будуть потребувати більш досконалих підходів до моделювання (застосування методу покращеної оцінки). Дане питання не задовольняється сучасною нормативною базою для подібних розрахунків і в майбутньому потребує використання комп'ютерних засобів оцінки як з боку розробника звітів з аналізу та переоцінки безпеки АЕС – ДП НАЕК «Енергоатом», так і з боку регулюючого органу – Державної інспекції з ядерного регулювання України.

[1] НП 306.2.141-2008. Загальні положення безпеки атомних станцій
[2] НП 306.2.162-2010 Вимоги до оцінки безпеки атомних станцій
[3] Требования к содержанию отчета по анализу безопасности действующих на Украине энергоблоков АЭС с реакторами типа ВВЭР. Руководящий документ. Киев, 1995
[4] Норми радіаційної безпеки України (НРБУ-97). Затверджено МОЗ Наказом №208 від 14 липня 1997р.
[5] Норми радіаційної безпеки України, доповнення: Радіаційний захист від джерел потенційного опромінення (НРБУ-97/Д-2000). Затверджено МОЗ Наказом №116 від 12 липня 2000 р.
[6] Основні санітарні правила забезпечення радіаційної безпеки України (ОСПУ-2005)

[7] НП 306.2.173-2011. Вимоги щодо визначення розмірів і меж зони спостереження АЕС. Із змінами, внесеними згідно з Наказом Державної інспекції ядерного регулювання N 206/765 від 23.11.2015

[8] Перечень разрешенных к использованию в ГП "НАЭК "Энергоатом" расчетных кодов для обоснования безопасности ядерных установок по состоянию на 01 февраля 2018 г. (введено в дію розпорядженням ДП НАЕК "Енергоатом" №137-р від 05.02.2018 р.);

[9] Кириленко Ю. О. Особливості радіаційного впливу при аваріях із розливом рідких радіоактивних середовищ. – Зб. тез науково-технічної конференції молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, м. Київ, 16 травня 2018 р. / ІПМЕ ім. Г.Є. Пухова НАН України, 2018. – С. 23-26

[10] Каменева І. П., Кириленко Ю. О. Підготовка вихідних даних для задач моделювання радіаційного впливу при аваріях із розливом рідких радіоактивних середовищ Зб. тез VI міжнародної наукової конференції «Моделювання-2018», Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, м. Київ, 12-14 вересня 2018 р. / ІПМЕ ім. Г.Є. Пухова НАН України, 2018. – С. 162-165

[11] Yurii Kyrylenko, Iryna Kameneva, Oleksandr Popov, Andrii Iatsyshyn, Volodymyr Artemchuk, Valeriia Kovach. Source Term Modelling for Event with Liquid Radioactive Materials Spill. Collective monograph “Systems, Decision and Control in Energy I”. Springer. 2020

[12] NUREG-0016 «Calculation of Releases of Radioactive Materials in Gaseous and Liquid Effluents from Boiling Water Reactors», 1979

[13] NUREG-0017 «Calculation of Releases of Radioactive Materials in Gaseous and Liquid Effluents from Pressurized Water Reactors», 1985

[14] ANSI/ANS-18.1-1999, “Radioactive Source Term for Normal Operation of Light Water Reactors”

[15] ANSI/ANS-18.1-2016 American National Standard «Radioactive Source Term for Normal Operation of Light Water Reactors»

[16] Poos T, Varju E. Determination of evaporation rate at free water surface, 8th International Symposium on Exploitation of Renewable Energy Sources, p. 66-71 2016

[17] Zilberman B. Ya., Ryabkov D. V., Puzikov E. A., Andreeva E. V. and Mishina N. E. Influence of Pressure (Temperature) on the Nitric Acid Distribution between the Liquid and Vapor in the Course of Evaporation of Nitric Acid Radioactive Waste / Radiochemistry, 2016, Vol. 58, No. 3, pp. 237–242, 2016

[18] M. Orvos, V. Szabo, and T. Poos Rate of Evaporation from the Free Surface of a Heated Liquid, Journal of Applied Mechanics and Technical Physics, Vol. 57, No. 6, pp. 1108–1117, 2016

[19] Lukashov V., S. Romanko, S. Timofeev, Protsenko A. Rate of Components Evaporation from Sulfuric Acid Solution During Its Concentrating in Air Flow / Chemistry & Chemical Technology, Vol. 11, No. 3, pp. 344–348, 2017.

О.Г. Кіслов, С.М. Головань

ПІДВИЩЕННЯ КЕРОВАНОСТІ ГРІД-СЕРВІСІВ ІНФОРМАЦІЙНОГО ЗАХИСТУ

Найбільш складною в обчислювальному сенсі функцією мережних систем виявлення вторгнень, антивірусних фільтрів та інших сигнатурних засобів інформаційного захисту є задача розпізнавання ознак шкідливої активності в інтенсивному потоці даних в реальному часі [2]. Ефективно розв'язувати цю задачу дозволяють реконфігуровні засоби на базі програмованих логічних інтегральних схем (ПЛІС) завдяки високої гнучкості у поєднанні з швидкодією, близькою до апаратної [3].

Труднощі, що виникають внаслідок складності процесу розробки та конфігурування пристроїв на базі програмованої логіки, можна усунуті, якщо ресурсномісткі процедури виконувати не локально на кожної окремої системі, а централізовано, з використанням високопродуктивних систем, зокрема, грід-інфраструктури. Такий підхід також значно спрощує використання реконфігуровних засобів інформаційного захисту їх користувачами, що не є спеціалістами з використання ПЛІС.

Протягом 2015 – 2018 рр. на базі грід-вузлу ІПМЕ ім. Г.Є. Пухова НАН України було створено у вигляді веб-додатку експериментальний грід-сервіс централізованого синтезу конфігурацій STRAGS [1]. В процесі проведення експериментів із даним сервісом виявилося, що ефективність його використання залежить не лише від можливостей, що надаються користувачам, але також від здатності керувати додатком на системному рівні з боку розробників та дослідників. Розглянемо на прикладі цього грід-сервісу, як може бути підвищена керованість такого сервісу.

З метою досягнення поставленої мети розроблений раніше функціонал грід-сервісу STRAGS був доповнений інтерфейсом адміністратора. Для цього в інтерфейс користувача було додано вкладку *Admin Interface*, що з використанням фреймворку Twitter Bootstrap та JavaScript бібліотеки jQuery реалізує звернення в API-інтерфейс керування агентами (ініційованими на вузлах грід-мережі віртуальними машинами з попередньо встановленим і налаштованим інструментальним програмним забезпеченням, необхідним для синтезу реконфігуровних пристроїв), а також візуалізує отримані дані (див. рисунок).

Доступ до вкладки *Admin Interface* обмежено згідно імені грід-сертифікату, за яким користувач автентифікувався в системі. Список користувачів сервісу з правами адміністратора задається в конфігурації.

Інтерфейс надає можливість скористатися всіма можливостями API керування. В лівій частині відображено загальну статистичну інформацію, та розміщено елементи для зміни кількості агентів в режимі очікування та перегляду журналів запуску агентів і доступу до грід-сервісу.

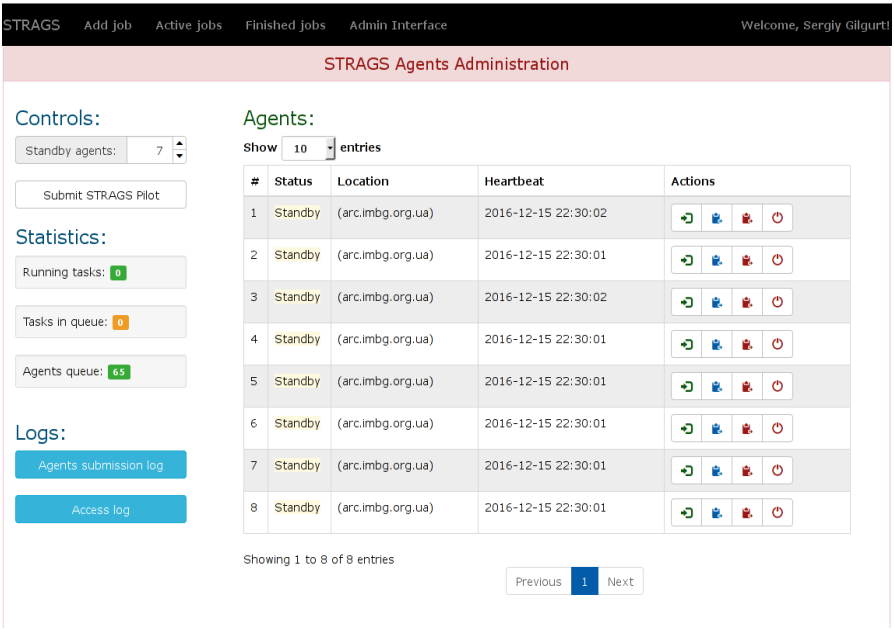


Рис. Веб-інтерфейс адміністратора грід-сервісу STRAGS

В правій частині інтерфейсу розміщено список активних агентів, з відображенням їх стану, обчислювального елементу та часу синхронізації. Для кожного агенту розміщено ряд елементів керування, що дозволяють здійснювати керування даним агентом – видаляти, переглядати потоки стандартного виводу та помилок грід-завдання та отримувати доступ до консолі віртуальної машини – агенту.

Розроблений інтерфейс адміністратора додано до макетного зразка грід-сервісу STRAGS. Як показали випробування, додані функції суттєво підвищили керованість системи централізованого програмування реконфігуровних прискорювачів, що застосовуються для вирішення задач інформаційної безпеки.

[1] Євдокимов В.Ф., Давиденко А.М., Гільгурт С.Я. Створення на базі грід-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. – Вип. 79. – К.: 2017. – С. 3-8.

[2] Гільгурт С.Я. Методи побудови оптимальних схем розпізнавання для реконфігуровних засобів інформаційної безпеки // Захист інформації. – 2019. – Т. 25, № 2. – С. 74-81.

[3] Гильгурт С.Я. Реконфигурируемые вычислители. Аналитический обзор // Электронное моделирование. – 2013. – Т. 35, № 4. – С. 49-72.

О.С. Потенко, О.А. Суліма

СПЕЦІАЛІЗОВАНІ ЗАСОБИ ЗАХИСТУ ВЕБ-РЕСУРСІВ ВІД ЗОВНІШНІХ АТАК

Відсутність єдиних стандартів безпечного програмування веб-додатків призводить до помилок в їх розробці, внаслідок чого у веб-сервісах виникають серйозні вразливості, які можуть бути скомпрометовані лише штатними можливостями браузера, без використання спеціальних засобів.

Атаки на веб-ресурси, які використовують програмне забезпечення для досягнення шкідливих цілей, як правило, проходять одночасно з сесіями легітимних користувачів і майже завжди використовують стандартні HTTP (80) і HTTPS (443) порти. Блокування всього трафіку на рівні порту не є прийнятним варіантом вирішення проблеми, оскілки доступ до веб-додатків буде повністю закритий ззовні або зсередини. Саме тому хакери шукають вразливості на рівні веб-додатків.

Ризики компаній в таких умовах занадто великі, щоб ігнорувати дану проблему, отже вразливості в веб-додатках піддають критично важливі бізнес-операції і конфіденційні дані небезпеки. Значні фінансові втрати можуть виникнути в результаті непередбачених затримок в бізнес-процесах, крадіжки інтелектуальної власності та втрати довіри клієнтів, а також репутації бренду. У багатьох випадках, безпека веб-додатків також є юридичною вимогою до компанії, яка обробляє персональні дані користувачів.

Тому зростає актуальність застосування додаткових засобів захисту, що використовуються на етапі експлуатації, такі як системи виявлення / запобігання вторгнень (IDS/IPS), міжмережеві екрани нового покоління – Next Generation Firewall (NGFW), а також засоби фільтрації трафіку прикладного рівня, спеціально орієнтовані на веб-додатки – Web Application Firewall (WAF) [1].

Системи виявлення та запобігання вторгнень на відміну від захисних екранів здатні аналізувати не тільки заголовки, а й тіла мережевих пакетів і здійснювати інспекцію на рівні додатку за певними сигнатурам. Такі засоби здатні виявляти атаки не тільки ззовні, але й всередині мережі за рахунок прослуховування SPAN-порту комутатора [6].

Для вдосконалення захисних механізмів в IDS / IPS стали застосовуватися декодери (розбір полів TCP-пакета) і препроцесори (розбір частин протоколу рівня додатки, наприклад, HTTP). Застосування препроцесорів в IPS Snort дозволило істотно поліпшити функціональність периметрового захисту в порівнянні з пакетним фільтром, навіть якщо останній перевіряє пакети на рівні додатків (iptables з модулем layer7).

Однак при цьому зберігся основний недолік пакетного фільтра: перевірка здійснюється попакетно, без урахування сесій, cookies та всієї іншої логіки роботи програми [3, 4].

Наступним етапом еволюції систем виявлення вторгнень стала поява пристроїв класу міжмережеві екрани нового покоління NGF. Такі засоби є спробою об'єднати функції різних продуктів (антивірус, IDS/IPS, пакетний фільтр, VPN-шлюз, маршрутизатор, балансувальник тощо) в одному засобі. При цьому виявлення атак в пристроях NGFW нерідко здійснюється на старій технологічній базі, за допомогою згаданих вище препроцесорів [5].

WAF – засіб фільтрації трафіку прикладного рівня, спеціально орієнтовані на веб-додатки. Застосування такого засобу вважається найбільш ефективним підходом до захисту веб-ресурсів. WAF може бути реалізований як хмарний сервіс, додаток на веб-сервері або спеціалізоване залізний або віртуальний пристрій [2].

Порівняння основних можливостей технологій IDS/IPS, NGFW та WAF наведено у Таблиці.

Таблиця

Порівняння параметрів WAF, IDS/IPS та NGFW

	IDS/IPS	NGFW	WAF
Multiprotocol Security	+	+	-
IP Reputation	-/+	-/+	-/+
Web Attack Signatures	-/+	-	+
Web Vulnerabilities Signatures	-/+	-/+	+
Automatic Policy Learning	-	-	+
URL, Parameter Cookie, and Form Protection	-	-	+
Leverage Vulnerability Scan Results	-/+	-	+

Отже захист вразливих веб-додатків може здійснюватися не тільки шляхом усунення вразливостей програмного забезпечення веб-додатків, але й за допомогою спеціалізованих засобів захисту цих продуктів – IDS/IPS, Next Generation Firewall та Web Application Firewall.

[1] Intro to Next Generation Firewalls [Електронний ресурс] – https://www.esecurityplanet.com/security-buying-guides/intro-to-next-generation-firewalls.html.

[2] Web Application Firewall – захист сайту від хакерських атак [Електронний ресурс] – https://habr.com/ru/post/60590.

[3] Ефективність Web Application Firewall [Електронний ресурс] – https://xakep.ru/2011/11/21/57840.

[4] Применение IDS / IPS [Електронний ресурс] – https://xakep.ru/2012/10/29/ids-ips/

[5] Сетевая безопасность. Часть 2. Next-Generation Firewall [Електронний ресурс] – https://habr.com/ru/company/hpe/blog/262123.

[6] Чим захищають сайти, або Навіщо потрібен WAF? [Електронний ресурс] – https://habr.com/ru/company/pt/blog/269165.

О.А. Давиденко

АВТОМАТИЧНИЙ ПОШУК НЕЙРОННОЇ АРХІТЕКТУРИ В ОБМЕЖЕНОМУ СЕРЕДОВИЩІ

Для покращення результатів роботи нейронних мереж протягом останнього десятиліття дослідники покладалися на створення все кращих і кращих архітектур нейронних мереж шляхом зміни послідовності, типів і конфігурацій шарів. Як наслідок, найкращі state-of-the-art мережі можуть бути дуже складними. Розмір нині класичної мережі VGG16 – більше ніж 144 мільйони параметрів [3]. Тому тренування оптимальної мережі для заданої задачі вимагає нагляду і тривалої роботи експерта з машинного навчання.

В зв'язку з цим автоматичний *пошук нейронної архітектури* (*neural architecture search*, NAS) стає все більш **актуальною** і популярної задачею. Особливого визнання вона зазнала після того як автоматично згенеровані нейронні архітектури стали значно перевершувати ті, що були створені людьми [2].

Провідні світові компанії уже мають власні реалізації NAS. Google AutoML включає в себе спеціалізовані NAS-модулі для областей обробки природної мови, машинного перекладу, комп'ютерного зору і роботи зі структурованими даними [4]. У той же час, існують також реалізації підходів NAS з цілком відкритим кодом, такі як AutoKeras [5].

Багато досліджень уже проведено в сфері загального NAS, тому було вирішено сфокусуватися на застосуванні NAS в предметній області візуальних даних. Це включає в себе стандартні задачі класифікації зображень, детекції об'єктів (Object Detection) і семантичної сегментації (Semantic Segmentation).

Крім того, більшість досліджень проводиться з використанням кластерів з сотень відеокарт для паралельного тренування моделей. В цій задачі простір перебору архітектур і гіперпараметрів настільки обширний, що іноді потребує сотень розрахункових днів на потужних відеокартах для досягнення хорошого результату [6]. Доцільною здається спроба максимально звузити простір перебору за допомогою розумних евристик і жадібних алгоритмів.

Таким чином, **постановка задачі**: реалізувати автоматичний пошук нейронної архітектури в умовах обмежень на час та пам'ять, використані на етапах тренування і тестування, з метою максимізації фінальної точності мережі. Часовий бюджет і ліміт пам'яті має задаватися користувачем, в діапазоні, допустимому сучасними розрахунковими пристроями.

За допомогою введення споживання пам'яті в оцінку мережі, можна задати верхню межу споживання пам'яті, і зменшити об'єм її використання під час роботи [7]. Дослідження показують, що можна успішно сумістити обмеження на час і пам'ять щоб знизити час пошуку оптимальної архітектури до кількох годин [1].

[1] Haokui Zhang, Ying Li, Hao Chen, Chunhua Shen. Memory-Efficient Hierarchical Neural Architecture Search for Image Denoising. https://arxiv.org/pdf/1909.08228.pdf
[2] Golnaz Ghaisi, Tsung-Yi Lin, Ruoming Pang, Quoc V. Le. NAS-FPN: Learning Scalable Feature Pyramid Architecture for Object Detection. https://arxiv.org/pdf/1904.07392.pdf
[3] Karen Simonyan, Andrew Zisserman. VERY DEEP CONVOLUTIONAL NETWORKS FOR LARGE-SCALE IMAGE RECOGNITION. https://arxiv.org/pdf/1409.1556.pdf
[4] Google Cloud AutoML. https://cloud.google.com/automl/
[5] Haifeng Jin, Qingquan Song, Xia Hu. Auto-Keras: An Efficient Neural Architecture Search System. https://arxiv.org/pdf/1806.10282.pdf
[6] Real, E., Aggarwal, A., Huang, Y., Le, Q.V. Aging Evolution for Image Classifier Architecture Search. In: AAAI Conference on Artificial Intelligence (2019)
[7] Peiye Liu, Bo Wu, Huadong Ma, Pavan Kumar Chundi, Mingoo Seok. MemNet: Memory-Efficiency Guided Neural Architecture Search with Augment-Trim learning. https://arxiv.org/pdf/1907.09569v1.pdf

В.В. Станиціна, В.О. Артемчук

ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ ТЕПЛОВИХ НАСОСІВ В СИСТЕМІ ТЕПЛОПОСТАЧАННЯ УКРАЇНИ

В Україні розвинуті системи централізованого та децентралізованого теплопостачання, основою яких є опалювальні котельні та ТЕЦ. Серед технологій, які є перспективними для впровадження в систему теплопостачання, є теплонасосні технології. Як показує досвід європейських країн, теплові насоси (ТН) можуть забезпечити побутове опалення за конкурентоспроможною ціною.

Оціночний максимум виробництва теплоти тепловими насосами з відновлюваних джерел енергії (ВДЕ) був досягнутий у 2015 р. – 3223 ГВт·год, обсяг виробництва у 2017 р. склав 2884 ГВт·год. Ці обсяги відносяться до вилученої енергії з відновлюваних джерел, які є нижчими за фактичне виробництво корисної енергії на величину витрат електричної енергії на привод ТН. Ця величина оцінюються у 2017 р. у 1540 ГВт·год при середньому значенні сезонного коефіцієнту продуктивності 2,87. У структурі виробництва теплоти з ВДЕ у 2017 р. за типами теплонасосних установок провідну роль відігравали реверсивні кондиціонери «повітря-повітря» – 1362 ГВт·год, ТН «ґрунт-вода» – 898 ГВт·год, ТН «вода-вода» – 540 ГВт·год, ТН «повітря-вода» – 61 ГВт·год, ТН «повітря-повітря» – 22 ГВт·год. Частка виробництва теплоти ТН з склала у 2016 р. 2,7% від обсягу відпуску теплової енергії від централізованих джерел. Оцінки Національної асоціації України по тепловим насосам щодо обсягів виробництва енергії з відновлюваних джерел засновані на рекомендованих (типових) значеннях експлуатаційних характеристик теплонасосних установок і відображають скоріше потенційні, ніж фактичні значення [1].

Статистика EHPA (European Heat Pump Association) за 2017 р. повідомляє про більш ніж 1,1 млн теплових насосів (ТН), проданих в Європі, в результаті кількість ТН зросла до 10,6 млн установок. Третій рік поспіль відбувалось зростання продажів на більш ніж 10%. В результаті роботи теплових насосів було вироблено 116 ТВт·год енергії з поновлюваних джерел, що сприяло скороченню 29,8 Мт викидів вуглецю. 50% усіх ТН продано у 3-х країнах – Франції, Італії та Іспанії.

В країнах ЄС теплові насоси - це технологія відновлюваної енергії. Різниця між корисною енергією, що виробляється від теплового насоса, і енергією, що використовується для приводу агрегату, вважається відновлюваною.

Ефективність теплових насосів з часом зростає. Оцінка продуктивності теплових насосів для різних проектів, виконаних ІСН Fraunhofer у Фрайбурзі, Німеччина, виявляє підвищення максимальної ефективності в новобудовах з 5,1 до 5,4 для геотермальних теплових насосів, тоді як теплові насоси повітря-вода підвищили їх максимальну ефективність з 3,4-4,2. Заміна

електричної системи опалення або котлів на викопному паливі тепловим насосом звільняє від 2/3 до 3/4 енергії, що використовується.

За допомогою використання холодоагентів та інтеграції відновлюваних джерел енергії в системи опалення з електрокотлами або котлами на викопному паливі теплові насоси можуть зменшити викиди вуглецю на 35-65% при заміні газу.

Промисловість теплових насосів є надійний роботодавцем в Європі - для виробництва, встановлення та підтримання щорічних продажів теплових насосів потрібно понад 54 тис. штатних робочих місць [2].

Проведені раніше дослідження показали перспективність впровадження ТН в Україні лише за певних умов [3].

Зміни, які відбулись в останні роки, а саме зростання ефективності нових теплових насосів, зміна їх вартості, а також цін на паливно-енергетичних ресурси, курсу гривні до євро, поступове зростання заробітної плати, вимагають для уточнення економічної ефективності впровадження теплових насосів та уточнення структури генеруючи потужностей у системі теплопостачання проведення нових досліджень з використанням методу оцінювання середньої вартості теплоенергії за життєвий цикл (LCOH) [4-5].

[1] Басок Б. І., Дубовський С.В. Укрупнена оцінка теплової потужності та обсягів виробництва відновлюваної енергії тепловими насосами в Україні. Теплові насоси в Україні. 2019. №1. С 2-6. URL : http://www.unhpa.com.ua/wp-content/uploads/2019/05/%D0%B6%D1%83%D1%80%D0%BD%D0%B0%D0%BB-%D1%82%D0%BD2019.pdf

[2] White Paper: Heat Pumps - Integrating Technologies to Decarbonise Heating and Cooling. Available at: https://www.ehpa.org/fileadmin/red/03._Media/Publications/ehpa-white-paper-111018.pdf

[3] Станиціна В.В. Визначення середньої вартості теплової енергії за життєвий цикл теплонасосної станції на артезіанських водах. Зб. тез XXXVII науково-технічної конференції молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України (2019). С.67-68.

[4] Baez, M.J., Larriba Martínez, T., 2015. Technical Report on the Elaboration of a Cost Estimation Methodology. No. D.3.1. Creara, Madrid, Spain.

[5] Projected Costs of Generating Electricity. International Energy Agency (IEA). 2010. 218 p.

С.М. Сергєєв, А.В. Ониськова, С.Ф. Гончар, М.Ю. Комаров, В.В. Ткаченко

АНАЛІЗ ОСНОВНИХ ТЕХНОЛОГІЙ ВИЯВЛЕННЯ ВТОРГНЕНЬ ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ АВТОМАТИЗОВАНИХ СИСТЕМ КЛАСУ 3

Системи виявлення вторгнень (IDS - intrusion detection system) – програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу в комп'ютерну систему або мережу або несанкціонованого управління ними в основному через мережу Інтернет. Створені для виявлення недоліків в системі безпеки. IDS дозволяють знизити збиток від кібератак і злому критичних вузлів.

Основне завдання IDS - відзначати підозрілі дії в мережі і своєчасно повідомляти про них, або навіть автоматично вносити зміни в політику безпеки засобів технічного захисту. Засоби IDS можуть переглядати потоки даних, знаходячи в них послідовності бітів, які можуть свідчити про сумнівні дії або події, або здійснювати моніторинг системних журналів та інших файлів журналювання діяльності. Слід виявляти будь яку ненормальну поведінку, яка може свідчити про вторгнення (або спробі вторгнення).

Хоча існують різні різновиди IDS , всі вони мають три загальних компонента:

сенсори, аналізатори та адміністративні інтерфейси. Сенсори збирають трафік або дані про дії користувачів і відправляють їх аналізаторам, які шукають в них підозрілі дії. У разі виявлення аналізатором таких дій (на які він запрограмований), він відправляє відповідні повідомлення в адміністративний інтерфейс.

Існує два основних типи IDS : рівня мережі (network - based), які відстежують весь мережевий трафік, і рівня хоста (host - based), які аналізують дії в рамках однієї комп'ютерної системи.

IDS можуть бути налаштовані для виявлення атак, аналізу журналів аудиту, переривання з'єднань, повідомлення адміністратора про події атак, захисту системних файлів, вказівки на уразливості, які повинні бути враховані, а також для допомоги у відстеженні дій окремих хакерів.

IDS рівня мережі (NIDS - network - based IDS) використовують сенсори, які є окремими комп'ютерами з встановленим на них спеціальним програмним забезпеченням, або спеціальними виділеними пристроями (appliance). Кожен сенсор має мережеву карту (NIC - network interface card), що працює в режимі прослуховування мережі (promiscuous mode). Звичайні мережеві карти отримують тільки мережеві пакети, адресовані цій мережевій карті, широкомовні (broadcast) і багатоадресні (multicast) пакети. Драйвер мережевої карти копіює дані з середовища передачі та відправляє його стеку мережевих протоколів для обробки. Якщо мережева карта знаходиться в режимі прослуховування, драйвер мережевої карти захоплює весь трафік,

робить копії всіх пакетів, а потім передає одну копію в стек TCP , а другу копію - аналізатору, для пошуку певних шаблонів (сигнатур).

NIDS контролює мережевий трафік і не може побачити події, що відбуваються всередині окремого комп'ютера. Для відстеження таких дій слід використовувати IDS рівня хоста.

IDS рівня хоста (HIDS - host - based IDS) може бути встановлена на окремі робочі станції і / або сервери для виявлення небажаних або аномальних дій. HIDS зазвичай використовуються для забезпечення впевненості, що користувачі не видаляють системні файли, не змінюють важливі настройки або піддають систему ризику іншими способами. Так, якщо NIDS розуміє і контролює мережевий трафік, функціонал HIDS обмежуються тільки самим комп'ютером. HIDS не розуміє і не відстежує мережевий трафік, а NIDS не контролює дії всередині системи. Кожне з цих коштів має свої завдання і виконує їх своїми способами.

У більшості середовищ системи HIDS встановлюються тільки на критичні сервери, а не на кожен комп'ютер в мережі, оскільки це могло б викликати істотне підвищення навантаження на комп'ютери і на адміністраторів.

Щоб зробити життя трохи простіше, HIDS і NIDS можуть бути одного з наступних типів:

1. Сигнатурні (signature based)
- Відстежують шаблони (pattern matching)
- Відстежують стан (stateful matching)
2. Засновані на аномаліях (anomaly based)
- Засновані на статистичних аномаліях (statistical anomaly - based)
- Засновані на аномаліях протоколів (protocol anomaly - based)
- Засновані на аномаліях трафіку (traffic anomaly - based)
3. Засновані на правилах (rule - based) або евристичні (heuristic - based)

Виявлення вторгнень на основі знань або сигнатур

Знання про окремі атаках накопичуються виробниками IDS і зберігаються у вигляді моделей, що відображають процес їх виконання. Ці моделі називаються сигнатурами. Як тільки виявляється новий вид атаки, виробник сигнатурного IDS створює відповідну сигнатуру, яка в подальшому використовується при перевірці мережевого трафіку для виявлення такої ж атаки. Дозволяються будь-які дії, що не були ідентифіковані як атака.

Прикладом сигнатури є мережевий пакет, в якому адреса відправника та одержувача збігаються - це, так звана, Land -атаки. У Land -атаки хакер змінює заголовок пакета і коли система одержувача відправляє відправнику відповідь, вона відправляє його на свій же адресу.

Зараз це виглядає досить безневинно, але все ще є вразливі системи, що не мають програмного коду, що дозволяє розпізнати таку ситуацію, яка призводить до їх «зависання» або перезавантаження.

Сигнатурні IDS є найбільш популярними IDS в наш час, але їх ефективність безпосередньо залежить від регулярності оновлення баз

сигнатур, як в антивірусному програмному забезпеченні. Цей тип IDS практично не захищає від нових атак, так як він не може їх розпізнати до появи їх сигнатур в його базі даних. Атаки або віруси, виявлені в реальних середовищах, називаються «дикими» (in the wild). Атаки або віруси, існуючі, але не випущені в реальний світ, називаються «в зоопарку» (in the zoo). Це не жарт. IDS на основі стану . Перед тим, як заглибитися в вивчення роботи IDS на основі стану, вам слід зрозуміти, що являє собою стан системи. Кожна зміна в роботі системи (вхід користувача, запуск програми, взаємодія додатків, введення даних і т.д.) призводить до зміни стану. З технічної точки зору, всі операційні системи і додатки є просто безліч рядків команд, написаних для виконання певних функцій над даними. Команди працюють зі змінними, які містять дані. Коли ви, наприклад, використовуєте утиліту «Калькулятор» і вводите цифру «5», спеціальна порожня змінна відразу ж отримує це значення. Ввівши цю цифру, ви змінюєте стан додатку. Коли додатки взаємодіють один з одним, вони заповнюють порожні змінні спеціальними наборами команд. Таким чином, перехід стану - це коли змінюється значення змінної, що відбувається постійно в будь-якій системі. При проведенні атак, відбуваються відповідні зміни станів (дії).

Виявлення вторгнень на основі статистичних аномалій

IDS на основі статистичних аномалій (statistical anomaly - based IDS) - це системи, засновані на поведінці. Вони не використовують сигнатури. Замість цього вони створюють профіль «нормальної» діяльності, працюючи в режимі навчання. Профіль будується на основі постійного аналізу який відбувається в середовищі діяльності. Точність профілю і якість захисту залежить від часу знаходження IDS в режимі навчання. Після створення профілю, весь наступний трафік і діяльність порівнюються з ним. Все, що не схоже на профіль, вважається атакою, про яку надсилається відповідне повідомлення. Такі IDS використовую складні статистичні алгоритми, вишукуючи аномалії в мережевому трафіку і дії користувачів. Кожному пакету присвоюється рейтинг його « аномальність », який вказує на ступінь його відхилення від нормального профілю. Якщо рейтинг вище певного порогу «нормальної» поведінки, виконується заздалегідь визначені дії.

Перевагою IDS на основі статистичних аномалій є їх можливість реагувати на нові типи атак, в тому числі атаки «нульового дня», для яких ще немає сигнатур або патчів . Ці IDS також можуть виявляти «низькі і повільні» атаки, при яких атакуючий намагається залишитися нижче порога спрацьовування засобів моніторингу, відправляючи пакети потроху протягом тривалого періоду часу. IDS на основі статистичних аномалій можуть виявляти ці типи атак, оскільки вони досить відрізняються від профілю.

Але є і погані новини. Вкрай складно створити для мережі якісний профіль «нормальної» діяльності, який не приводить до величезної кількості помилкових спрацьовувань. Це пов'язано з тим, що в мережі відбуваються постійні зміни. Часто це призводить до того, що організації просто

відключають свої IDS , через те, що вони вимагають вкрай багато часу для своєї належної підтримки. Щоб скоротити число помилкових спрацьовувань, потрібен дуже висококваліфікований IT-персонал . Також, важливим моментом є правильне визначення порогу спрацьовування IDS .

Якщо організація вирішує використовувати IDS на основі статистичних аномалій, вона повинна переконатися, що її співробітники, які будуть впроваджувати і підтримувати систему, розбираються в проведенні аналізу протоколів і пакетів. Це пов'язано з тим, що такі IDS (на відміну від IDS інших типів) відправляють малоінформативні повідомлення і мережевий інженер повинен в кожному випадку розбиратися, у чому насправді полягає проблема. Наприклад, сигнатурної IDS повідомляє тип виявленої атаки, IDS на основі правил повідомляє яке правило було порушено. IDS на основі статистичних аномалій просто повідомляють про те, що сталося щось «ненормальне», що не відповідає профілю.

IDS на основі аномалій протоколів

IDS на основі статистичних аномалій можуть використовувати фільтри, засновані на аномаліях протоколів. Такі IDS мають знання про кожний протоколі, який вони контролюють. Аномалії протоколів виявляються на підставі формату і поведінки протоколу. IDS будує модель (профіль) «нормального» використання кожного протоколу. Потрібно мати на увазі, що теоретичне використання протоколів описано у відповідних RFC , але їх реальна робота майже завжди відрізняється від теоретичної , оскільки виробники програмного забезпечення в більшості випадків не строго слідують RFC . Таким чином, більшість профілів окремих протоколів є сумішшю з офіційних і реальних варіантів їх використання. Коли IDS включається в роботу, вона шукає аномалії, які не збігаються з профілями, побудованими для конкретних протоколів. Хоча в самих операційних системах і додатках досить експлуатованих вразливостей, більшість успішних атак використовують вразливості самих протоколів. Наприклад, на канальному рівні моделі OSI протокол ARP (Address Resolution Protocol) не має захисту від атак, при яких в таблицю ARP вставляються підроблені дані.

IDS на основі аномалій трафіку

Більшість поведінкових IDS мають фільтри, засновані на аномаліях трафіку, які виявляють зміни в шаблонах трафіку, наприклад DoS -атаки або поява нових сервісів в мережі. Створений профіль є таким собі базисом звичайного трафіку середовища, і весь наступний трафік порівнюється з цим профілем. Як і у всіх фільтрах, тут потрібно налаштування порогу спрацьовування для зменшення числа помилкових спрацьовувань (як помилкових дозволів, так і хибних заборон). Такий тип IDS також здатний виявляти невідомі атаки.

IDS на основі правил

IDS на основі правил (rule - based IDS) використовують інший підхід, що відрізняється від підходу сигнатурних IDS або IDS на основі статистичних аномалій. Наприклад, якщо сигнатурної IDS виявляє пакет, в

якому всі прапори заголовка TCP встановлені в «1», він знає, що це свідчить про xmas -атаки, і відправляє відповідне сповіщення. IDS на основі статистичних аномалій також досить прямолінійні. Наприклад, якщо Олександр зареєструвався на своєму комп'ютері о 6 ранку, а відповідно до його профіля це ненормально, IDS відправляє повідомлення про це, бо це виглядає як дії, які повинні бути проаналізовані. IDS на основі правил веде себе хитріше в залежності від складності застосованих правил.

IDS на основі правил схожі на експертні системи. Експертна система заснована на базі знань (knowledge base), механізмі логічних висновків (inference engine) і програмуванні на основі правил (rule - based programming). Знання є правила, а аналізовані дані - факти. Знання системи описуються з допомогою програмування на основі правил (ЯКЩО ситуація ТОДІ дію). Ці правила застосовуються до фактів, до даних, що отримуються сенсором, або до контрольованих систем.

Звичайні мови програмування - це приблизно як «чорне і біле» в житті. Вони відповідають тільки «так» або «ні», але не «може бути так» або «може бути ні». Хоча комп'ютери виконують складні обчислення набагато швидше, ніж люди, їм важче робити припущення, висновки, давати відповіді - оскільки вони дуже жорстко структуровані. Мови програмування п'ятого покоління (мови штучного інтелекту) здатні працювати з «сірим» кольором життя і можуть намагатися приймати правильні рішення на основі отриманих даних.

Таким чином, в IDS заснованих на правилах, які працюють аналогічно експертним системам, IDS збирає дані з сенсорів або з журналів аудиту, а механізм логічних висновків обробляє їх, використовуючи попередньо запрограмовані правила. Якщо характеристики задовольняють правила, відправляється відповідне повідомлення або виконується певна дія для вирішення виниклої проблеми.

Сенсори IDS

IDS мережевого рівня використовують сенсори для здійснення моніторингу. Сенсор, який працює як аналітичний движок (analysis engine), розміщується в мережевому сегменті, який має контролювати IDS . Сенсор отримує «сирі» (raw) дані від генератора подій, і порівнює їх з базою даних сигнатур, профілем або моделлю - в залежності від типу IDS . Якщо виявляється якийсь збіг, який свідчить про підозрілу активність, сенсор працює як модуль реагування для визначення виду дій, які потрібно зробити (повідомлення через систему миттєвих повідомлень, мобільний телефон, електронну пошту, уера і т.д.).

Сенсор призначений для фільтрації данних, які на нього надходять, відкидаючи непотрібну інформацію і виявляючи підозрілу діяльність.

Консоль моніторингу контролює всі сенсори і надає мережному персоналу огляд роботи всіх сенсорів в рамках всієї мережі. Розміщення сенсорів є одним з критичних етапів конфігурації IDS . Організація може розмістити один сенсор перед фаєрволом для виявлення атак, а інший сенсор за фаєрволом (в мережевому периметрі) для виявлення реальних

вторгнень. Сенсори слід також розміщувати в висококритічних областях, DMZ і в екстрамережі .

Проведений аналіз показує, як важливо розуміти характеристики, що відрізняють один від одного різні типи технологій IDS.

1. Сигнатурні (signature - based): відстежують шаблони (pattern matching), що працюють подібно антивірусного програмного забезпечення, сигнатури повинні постійно оновлюватися, не можуть виявити нові атаки.

2. Засновані на аномаліях (anomaly - based):засновані на поведінці системи (behavioral - based), які вивчають «нормальну» діяльність у середовищі, можуть виявляти нові атаки, також називаються поведінковими або евристичними.

3. Засновані на правилах (rule - based): використовують ЯКЩО / ТОДІ програмування, засноване на правилах, в рамках експертних систем, використовують експертну систему, що має характеристики штучного інтелекту, не може виявляти нові атаки.

[1] “The Science of IDS Attack Identification” (Cisco Systems whitepaper) www.cisco.com/en/US/products/sw/secursw/ps976/products_white_paper09186a0080092334.shtml;

[2] Honeypots.net IDS Software links page www.honeypots.net/ids/products;

[3] Корченко А.О. Методология построения систем выявления аномалій порожденных кибератаками / Захист інформації. – 2016 - №1. Т.18. – С. 30-38;

[4] Терейковский И.А. Система выявления кибератак / Безпека інформації. –Т.23, №3. -2017, С. 176-180.

В.О. Гурєєв, Є.М. Лисенко

ПОБУДОВА ТА ДОСЛІДЖЕННЯ АНАЛІТИЧНОЇ МОДЕЛІ ВТРАТ АКТИВНОЇ ПОТУЖНОСТІ В ЕЛЕКТРИЧНИХ МЕРЕЖАХ ДЛЯ КОМП'ЮТЕРНИХ ТРЕНАЖЕРІВ

Актуальність даної тематика наведена в [1,2,3,5,7,8].

Важливими параметрами режимів роботи електроенергетичних систем (ЕЕС) і енергооб'єднань (ЕО) в реальному часі [2,3] є втрати активної потужності. Останні характеризують міру ефективності роботи ЕЕС і/або ЕО та використовуються в якості критерія оцінки кваліфікації оперативно-диспетчерського персоналу ЕЕС. Розрахунок активних втрат виконується шляхом розв'язання системи нелінійних алгебраїчних рівнянь, що потребує пошук і застосування в комп'ютерних тренажерах надійних і швидких алгоритмів моделювання нормальних й аварійних режимів їх роботи.

Втрати електроенергії в електричних мережах та її транспортування до споживача є одним із основних показників економічності їхньої роботи. Він наглядно відображає проблеми, які вимагають невідкладного розв'язання щодо розвитку, реконструкції й технічного переоснащення електричних мереж, удосконалювання методів і засобів експлуатації, обліку та керування енергопостачанням [7].

Технічні втрати в елементах мережі (фізично обумовлені втрати, викликані транспортуванням електроенергії по мережі від постачальників до споживачів), визначаються розрахунком моделі мережі за методиками згідно з нормативними документами. Уточнення визначення технічних втрат може бути здійснено за рахунок удосконалення математичної моделі мережі, розширення та достовірності вихідних даних розрахунку, зокрема, графіків надходження електроенергії в мережу за обліковий період, графіків навантаження основних споживчих вузлів, а також за рахунок оптимізації режимів мережі та інших організаційних і технічних заходів [7].

Відповідно до аналізу міжнародних енергетичних організацій відносні втрати електроенергії під час її передавання та розподілу в електричних мережах у більшості країн вважаються задовільними, якщо вони не перевищують 4–5%. Втрати електроенергії до 8–8,5% вважаються максимально допустимими з точки зору економічної ефективності передавання електроенергії електромережами [7].

Електричні мережі з втратами електроенергії під час транспортування до споживача у разі перевищення зазначених показників вважаються економічно не ефективними.

Зазвичай аналіз втрат активної потужності виконують після серії розрахунків режимів ЕЕС або ОЕС. У складі систем підготовки оперативного персоналу ЕЕС і ОЕС перспективними є веб-орієнтовані електронні навчальні й режимні тренажерні засоби, які здатні адекватно моделювати

режими та аналізувати ефективність їх роботи в ринкових умовах.

Параметри режиму роботи будь-якої електричної мережі або її частини можуть бути розраховані в результаті рішення системи нелінійних рівнянь із використанням відомих [4] виразів для кожного *s*-го вузла мережі. Якщо відомі або задані потужності (генерація) *s*-х вузлів, то таку систему нелінійних рівнянь можна записати у вигляді скалярного добутку вектору струмів вузлів $[\dot{I}_s]$ на зв'язаний вектор напруги вузлів $[\hat{U}_s]$:

$$[\dot{S}_s] = ([\hat{U}_s], [\dot{I}_s]), \quad (1)$$

де $[\dot{S}_s]$ – вектор-стовпець заданих потужностей вузлів.

В якості основних методів розрахунку режимів роботи великих ЕЕС, які містять більше 2 тисяч вузлів, використовують методи Ньютона-Рафсона, Гауса, Зейделя та ін. [4,6,7]. Розрахунок режиму роботи довільної електричної мережі із заданими параметрами (навантаження, генерація і топологія) полягає у визначенні невідомого вектору напруги *s*-х вузлів $[\dot{U}_s]$ та перевірки балансу потужності, який можна представити у вигляді рівності: сума генерації вузлів мережі повинна дорівнювати сумі заданого навантаження всіх вузлів і втрат потужності в мережі в кожний момент часу.

Недоліком таких методів розрахунку є значний час розрахунку режимів великих ЕЕС і/або ЕО, що є неприйнятним для використання в дистанційних режимних тренажерах.

Для розв'язання системи (1) та аналізу втрат активної потужності у роботі використано алгоритм багатоопорного методу розрахунку контурних струмів (БМРКС), що відрізняється від відомих [4,6] наявністю вироджених контурів, які утворюються між вузлами з джерелами енергії ЕЕС і/або ЕО. Уся мережа завжди представлена сукупністю окремих дерев з хордами, які використовуються для представлення мережі в початковому замкнутому стані.

Струми хорд $[\dot{I}_h]^{(i)}$ постійно обчислюються на кожній ітерації розрахунку напруг вузлів та додаються до струмів вузлів для розрахунку струмів гілок і напруги вузлів. Струми контурів (хорд) розраховуються доти, доки мережа не стане адекватної мережі у початковому замкнутого стані. Для замкнутої схеми уточнюють нові значення струмів вузлів і повторюють внутрішній цикл ітерації для струмів хорд. Розрахунки режимів закінчують у разі, коли нові значення напруги вузлів або потужностей вузлів від ітерації до ітерації вже сильно не змінюються.

В роботі запропоновано алгоритм побудови аналітичної функції залежності активних втрат електричної мережі від сумарного навантаження вузлів мережі та реактивної генерації у вигляді поліному з використанням методу повного факторного експерименту (ПФЕ).

Досліджується вплив трьох важливих факторів: суми активного навантаження вузлів електричної мережі K_1, який знаходиться у діапазоні від 0.8 до 1.2 від сумарного навантаження вузлів мережі, суми реактивного

навантаження вузлів електричної мережі K_2, який знаходиться у тому же діапазоні, та суми реактивної генерації вузлів електричної мережі K_3 у тому же діапазоні, на цільову функцію Y у вигляді втрат активної потужності для відомої тестової електричної мережі 14-bus TEST IEEE.

Апріорний аналіз функцій відгуку показав, що зміну втрат активної потужності Y доцільно описати рівнянням регресії наступного виду:

$$\hat{y} = b_0 + b_1x_1 + b_2x_2 + b_3x_3 + \\ + b_{12}x_1x_2 + b_{13}x_1x_3 + b_{23}x_2x_3 + b_{123}x_1x_2x_3 \quad (2)$$

Коефіцієнти рівняння регресії (2) у загальному вигляді визначаються за методом найменших квадратів наступним чином:

$$B = \left(X^T X\right)^{-1} X^T Y$$

Отже, будь-який коефіцієнт рівняння регресії b_j визначається скалярним добутком стовпця y на відповідний стовпець x_j, поділений на кількість дослідів у матриці планування експериментів N :

$$b_j = \frac{1}{N}\sum_{i=1}^{N} x_{ji}y_i \ .$$

Ефект взаємодії визначається аналогічно лінійним ефектам. Так, розрахунок b_{ji} виконується за формулою:

$$bij = \frac{1}{N}\sum_{i=1}^{N}\left(x_j x_i\right)_i y_i \ .$$

Аналогічно обчислюються інші коефіцієнти рівняння регресії.

В таблиці 1 наведена структура плану ПФЕ для тестової ЕМ із 14 вузлів, відомою в літературі під назвою 14-bus TEST IEEE.

Таблиця 1

№ досліду	Фактори у натуральному масштабі			Фактори у безрозмірній системі координат			Y (втрати активної потужності)
	k_1	k_2	k_3	x_1	x_2	x_3	
1	0.8	0.8	0.8	-1	-1	-1	9.6
2	1.2	0.8	0.8	+1	-1	-1	9.8
3	0.8	1.2	0.8	-1	+1	-1	10.3
4	1.2	1.2	0.8	+1	+1	-1	11.1
5	0.8	0.8	1.2	-1	-1	+1	10.2
6	1.2	0.8	1.2	+1	-1	+1	13.1
7	0.8	1.2	1.2	-1	+1	+1	15.2
8	1.2	1.2	1.2	+1	+1	+1	17.6

Користуючись наведеними в таблиці 1 даними, можна знайти такі коефіцієнти рівняння регресії

$$\hat{y} = 12.1 + 2.4x_1 - 1.5x_2 - 7.2x_3 + 2.3x_1x_2 - 1.7x_1x_3 - 2.5x_2x_3 - 1.3x_1x_2x_3.$$

Ця аналітична модель залежності активних втрат від сумарних навантажень і реактивної генерації вузлів використовується в комп'ютерних тренажерах для швидкого створення тренувальних занять без застосування комплексу розрахунку усталених режимів роботи ЕЕС або ОЕС. Також це дозволяє підвищити гнучкість комп'ютерних тренажерів та розширити тематику протиаварійних тренувань в короткі строки.

Отримані результати дають можливість застосовувати найбільш сучасні методи моделювання різноманітних режимів роботи складних ЕЕС, що дозволяє проводити більш ґрунтовний їх аналіз процесі підготовки персоналу.

Використання ПФЕ для побудови аналітичних залежностей дозволяє забезпечити можливість аналізу роботи ЕЕС і ОЕС в широкому діапазоні деталізації параметрів мережі і режимів їх роботи.

[1] Гурєєв В.О. Розробка алгоритмів і програм швидкодійних методів розрахунку режимів роботи великих електроенергетичних систем (ЕЕС) і енергооб'єднань (ЕО) для тренажерів // Наукові праці ВНТУ, - 2018, № 1, С. 1-5.

[2] Гурєєв В.О. Моделювання великих енергосистем для побудови комп'ютерних розподілених тренажерних систем в енергетиці // Моделювання та інформаційні технології. Збірник наукових праць ІПМЕ ім. Г.Є. Пухова. – 2018. Вип. 83.– С. 94–105.

[3] Simulation and study of modes for full-scale mode simulator for Ukrainian energy systems / V.Gurieiev, O.Sanginova//2nd International Conference on Intelligent Energy and Power Systems (IEPS'2016), June 7–11,Kyiv, Ukraine. –2016. –P. 97–100.

[4] Холмский В.Г. Расчет и оптимизация режимов электрических сетей (специальные вопросы): учебное пособие для вузов / В. Г. Холмский. –М.: Высшая школа, 1975. –280 с.

[5] Energy Efficiency in the Power Grid. https://www.nema.org.

[6] Электрические системы. Электрические сети: Учеб. для электро-энерг. спец. вузов / В.А. Веников, А.А. Глазунов, Л.А. Жуков и др.: Под ред. В.А. Веникова, В.А. Строева. – 2-е изд., перераб и доп. – М.: Высш. шк., 1998. – 511с.: ил.

[7] Зарубіжний досвід підвищення ефективності передавання та розподілу електроенергії, оптимізації втрат електроенергії в електромережах всіх рівнів напруги/ НТЦЕ НЕК «Укренерго». 2015.

[8] Тарасов В.И. Нелинейные методы минимизации для расчета установившихся режимов электроэнергетических систем. – Новосибирск: Наука, 2001. – 214 с.

М.В. Антонішин

ОБ'ЄКТНО-ОРІЄНТОВАНА МОДЕЛЬ ПРОГРАМНОГО ЗАСОБУ ТЕСТУВАННЯ БЕЗПЕКИ МОБІЛЬНИХ ПРОГРАМНИХ ЗАСТОСУНКІВ

Актуальність дослідження обумовлена тим, що тестуванняя відповідно до настанов OWASP Mobile TOP 10 та OWASP API TOP 10 Security ускладнюється різнорідністю інструментів та етапів тестування [1 - 3]. При цьому вони не розглядаються як єдиний процес. Хоча архітектурою на рис. 1 схематично демонструється застосовність даних настанов стосовно веб застосунків. Такі інструменти характеризуються ручним виконанням або охопленням тільки окремих аспектів тестування.

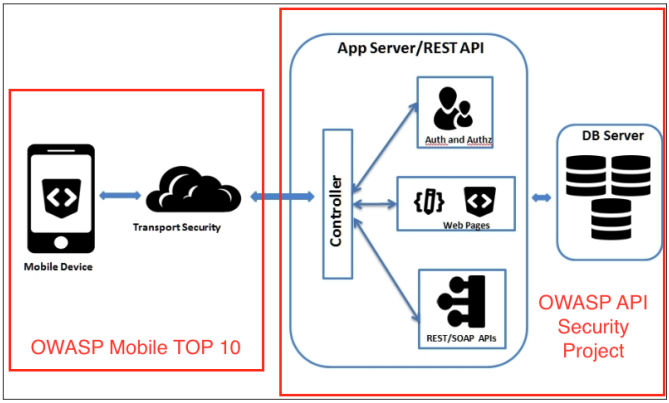


Рис. 1. Архітектура використання критеріїв тестування

Спробу розробити інструментальний засіб без даних обмежень здійснено в [4]. Цим засобом проводиться статичне та динамічне тестування, але він має такі недоліки:

1) статичний аналіз видає багато надлишкової інформації;
2) спеціаліст не може втручатися або слідкувати за динамічним тестом;
3) імлементовані модулі SSL-pinning та інші працюють не коректно.

Для подолання даних обмежень необхідно розробити програмний засіб, який дозволить провести тестування та проводити необхідне налаштування мобільного програмного застосунку, який тестується, відповідно до Secure Software Development Life Style. Зважаючи на це, можливості програмного засобу представлено діаграмою варіантів використання на рис. 2. На діаграмі виокремлено двох дійових екторів, які залучаються до тестування. Кожен варіант використання – це окремий модуль програмного засобу, яким проводиться тестування. Деякі кейси тестування можуть бути специфічними, тому й розробляються окремі тестові модулі під цільову задачу. Це допомогло оптимізувати час роботи спеціаліста [5].

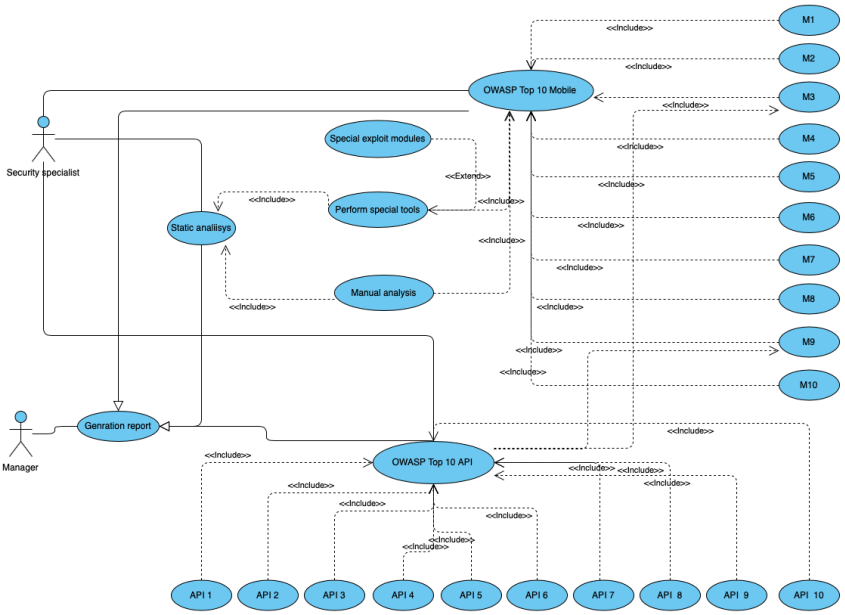


Рис. 2. Діаграма варіантів використання програмного застосунку

Отже, за результатами проведених досліджень встановлено, що на даний час відсутній інструмент комплексного тестування безпеки мобільних програмних застосунків. Для запобігання цьому розроблено об'єктно-орієнтовану модель програмного засобу. Його використання дозволяє адаптуватися до виконання специфічних тестів, які залежать від особливостей мобільного програмного застосунку.

[1] М.В. Антонішин, О.І. Міснік, В.В. Цуркан, "Оцінювання стану захищеності програмних застосунків операційної системи Android за методологією OWASP Mobile TOP 10", Моделювання та інформаційні технології. 2018. Вип. 82. С. 94-101.
[2] OWASP API Security Project: specification. URL: https://owasp.org/www-project-api-security/ (дата звернення: 30.04.2020).
[3] OWASP Mobile security testing guide (MSTG). URL: https://github.com/OWASP/owasp-mstg/ (дата звернення: 30.04.2020).
[4] MobSF Documnetation. URL: https://mobsf.github.io/docs/#/ (дата звернення: 30.04.2020).
[5] Unified Modeling Language: maual - URL: https://www.omg.org/spec/UML/2.5.1/PDF (дата звернення: 30.04.2020).

О.І. Міснік

ПРОТОТИП ПРОГРАМНОГО ЗАСОБУ ВИЯВЛЕННЯ ВТОРГНЕНЬ У КОНТЕЙНЕРНІ СЕРЕДОВИЩА

Актуальність дослідження обумовлена тим, що швидке впровадження контейнерних технологій для підтримки розвитку створення та використання програмного забезпечення, сприяє необхідності формування стратегії забезпечення безпеки щодо запобігання та виявлення вторгнень. На даний момент існують різні механізми для виконання профілактичних заходів щодо контейнерів, наприклад, сканування зображень на виявлення відомих вразливостей. Однак, необхідність впровадження програмного забезпечення для виявлення вторгнень є не менш важливими, особливо тому, що багато зусиль зі забезпечення безпеки з часом нейтралізуються або, що ще гірше, ніколи не здійснюються належним чином [1, 2].

Також беручи до уваги практику розгортання прикладних застосунків, які динамічно розподілені поміж хостами та програмний код яких розробляється за короткий проміжок часу. Це призводить до допущення уразливостей, нападу зловмисника і, як наслідок, експлуатування контейнерного середовища [3, 4].

Інфраструктуру забезпечення безпеки контейнерів можна розділити на кілька частин, які потрібно враховувати при розробленні прототипу програмного засобу [5]:

- агент, який може забезпечити видимість внутрішньої поведінки контейнера (відкриті файли, мережеві з'єднання, процеси, що виконуються):
    1. Правила поведінки, які можуть визначити, що вважається нормальним, а не аномальним для даного контейнера і про що потрібно повідомляти.
    2. Індикатори компрометації, за якими можна ідентифікувати аномальну активність та ознаки потенційного вторгнення до контейнерного середовища.
- механізм реагування, що дозволяє звертати увагу на події від простої маршрутизації або системи ведення журналу аудиту, до виконання більш запобіжних дій для зупинення або пом'якшення наслідків атаки;
- політики безпеки, що містять кроки, які необхідно зробити для реагування на інциденти безпеки. Це може бути або ручний процес описаний у політиці, або написаний у вигляді коду і виконується автоматично.

У той час як виявлення аномальної поведінки у контейнерах – це перший крок, а другий – автоматичне реагування або пом'яякшення атаки. Стосовно Docker і Kubernetes важливо знати, що кластери Kubernetes охоплюють велику кількість вузлів і розгортання контейнерів. Це може

ускладнити створення попередження про час виконання аномалії у певному контейнері з можливого переліку. Реакція на інцидент безпеки повинна бути швидкою оскільки у контейнерів невелика тривалість життя, важливо виявити зловмисника до того, як порушення безпеки контейнера завдасть реальної шкоди або просто зникне та буде замінений на новий. Автоматизація важлива, ніж будь-коли, і найкращим підходом є написання процедур відповідей у вигляді коду.

Тому робочий прототип, який планується для впровадження в організації фокусується на таких умовах:

- прототип отримує видимість всередині контейнерів за допомогою інструментарію системних викликів, з високою продуктивністю і мінімальними накладними витратами, тому може працювати в виробничих системах;
- інструментарій системних викликів повністю прозорий для контейнерів, тому не потрібно змінювати свій код, зображення контейнерів або попередньо завантажувати бібліотеки;
- при виявленні аномальної активності створюється подія безпеки, наприклад, попередження. Умови, які викликають попередження, визначаються політикою, набором правил.

Проведені дослідження продемонстрували, що прототип програмного засобу виявлення вторгнень у контейнерних середовищах оптимізує роботу під час інсталяції програмного забезпечення та оброблення результатів настання інцидентів безпеки – скорочується час, який витрачається на пошук артефактів та можливих шляхів компрометації контейнерного середовища та хостових машин.

[1] Наміот Д., Снепс-Снеппе М., «Про мікросервісну архітектуру», Міжнародний журнал відкритих інформаційних технологій, Вип 9, 2014, 24-27 С.

[2] Артамонов Ю.С., Востокін С.В., «Розробка розподілених додатків збору і аналізу даних на базі мікросервісної архітектури», Вісті Самарського наукового центру Російської академії наук, Вип. 4, 2016, 688-693 С.

[3] Антонішин М.В., Міснік О.І., Цуркан В.В., «Оцінювання стану захищеності програмних застосунків операційної системи Android за методологією OWASP Mobile TOP 10», Моделювання та інформаційні технології. 2018. Вип. 82. С. 94-101.

[4] Антонішин М.В., Міснік О.І., Цуркан В.В., «Аналіз якості роботи сканерів уразливостей веб – застосунків», Моделювання та інформаційні технології, Вип. 83, 2018, С. 77-86.

[5] Міснік О.І., «Проблеми використання систем виявлення та запобігання вторгнення в контейнерні середовища», Комп'ютерні та інформаційні системи та технології : зб. тез доп. четвертої міжнародної науково-технічної конференції, (м. Харків, Квітень 22-23, 2020), Харків, 2020, С. 15.

О.В. Цуркан, Р.П. Герасимов, О.М. Крук, Т.М. Клименко

МЕТРИКИ СУБ'ЄКТА ТА ОБ'ЄКТА СОЦІОІНЖЕНЕРНОГО ВПЛИВУ

Суб'єкт соціоінженерного впливу цілеспрямовано впливає на свідомість об'єкта проти волі, але за його згодою [1]. При цьому враховуються їх психолого-особистісні якості та професійні компетенції. Такий вплив орієнтований на отримання конфіденційної інформації [1, 2]. Для запобігання цьому рекомендовано суб'єкта з об'єктом представляти соціальним графом [1]. Ним відображаються взаємодія і зв'язки між даними соціальними об'єктами. Тому визначення їх метрик є актуальним.

Як соціальні об'єкти розглядаються соціальний інженер (суб'єкт соціоінженераного впливу) та працівник організації (об'єкт соціоінженерного впливу). Крім цього, беруться до уваги технічний або програмний засіб, психолого-особистісні якості, професійні компетенції. З огляду на це, можливі такі варіанти зв'язків: соціальний інженер – працівник, соціальний інженер – технічний засіб, соціальний інженер – програмний засіб, соціальний інженер – якість, соціальний інженер – компетенція, працівник – технічний засіб, працівник – програмний засіб, працівник – якість, працівник – компетенція.

Для врахування особливостей даних соціальних об'єктів і зв'язків між ними визначаються такі метрики як взаємин, зв'язків і сегментування [3, 4]. Метриками взаємин відображаються відношення між соціальним об'єктами, зокрема, встановлюється їх подібність, множинність і взаємозалежність. Особливості зв'язків враховуються використанням відповідних метрик. Вони орієнтовані на визначення важливості та кількості зв'язків між соціальними об'єктами. Їх розподіленість характеризується метриками сегментування. Такі метрики дозволяють виокремити групи соціальних об'єктів за характером зв'язків. Отже, розглянуто представлення взаємодії суб'єкта та об'єкта соціоінженерного впливу соціальним графом. Виокремлено вірогідні варіанти такої взаємодії. Для врахування її особливостей визначено метрики взаємин, зв'язків і сегментування.

[1] Tsurkan O., Herasymov R., Kruk O., "Presentation the interaction of the subject and the object of socio-engineering influence with a social graph", Computer and Information systems and technologies : fourth International Scientific and Technical Conference (Kharkiv, April 22-23, 2020). Kharkiv, 2020. P. 46.

[2] Кириченко Л., Радивилова Т., Барановский А., «Обнаружение киберугроз с помощью анализа социальных сетей», Information Technologies & Knowledge, 2017, vol. 11, no 1, P. 23-48.

[3] Коршунов А., Белобородов И., Бузун Н., и др., «Анализ социальных сетей: методы и приложения», Труды Института системного программирования РАН, 2014. Том 26, № 1. С. 439-456.

[4] Gross J., Yellen J., Anderson M., Graph theory and its applications. Boca Raton, USA: CRC Press, 2019, 593 p.

І.А. Біловицька, В.В. Цуркан

СПЕЦИФІКАЦІЯ ВИМОГ ДО ПРОГРАМНОГО КОМПОНЕНТУ АНАЛІЗУВАННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Окремим напрямом забезпечення кібербезпеки є протидія шкідливому програмному забезпеченню [1]. Це досягається завдяки його виявленню і аналізуванню. Результативність процесу аналізування залежить від інформації про шкідливе програмне забезпечення, зокрема [2], категорію (наприклад, віруси, хробаки, трояни). На її основі визначаються характеристики та пріоритети оброблення інцидентів зі шкідливим програмним забезпеченням Тому специфікування вимог до програмного компоненту аналізування шкідливого програмного забезпечення є актуальним.

Вимоги до програмного компоненту визначаються відповідно до [3]: [Програмний компонент] [Аналізування шкідливого програмного забезпечення] [Категорія шкідливого програмного забезпечення]. Як наслідок, у графічній нотації UML виокремлено основний варіант використання – аналізування шкідливого програмного забезпечення. Він включає представлення шкідливого програмного забезпечення зображенням і визначення категорії шкідливого програмного забезпечення. Перший варіант використання специфікує дії з, по-перше, представлення їх двійкового файлу 8 бітним вектором цілих чисел без знаку; по-друге, представлення двійкового значення кожного компоненту вектору десятковим; по-третє, представлення десяткового вектору зображенням з відтінками сірого [4]. Категорія шкідливого програмного забезпечення визначається за видом отриманого зображення. Це обумовлено тим, у межах однієї категорії воно характеризується схожістю візуального представлення. Для цього отримані зображення шкідливого програмного забезпечення зіставляються з еталонами в межах другого варіанту використання.

Отже, визначені варіанти використання у графічній нотації UML розглядаються як специфікація вимог до програмного компоненту аналізування шкідливого програмного забезпечення.

[1] ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT). [Чинний від 2018-01-01]. Вид. офіц. Київ : ТК «Інформаційні технології», 2018. 50 с.

[2] NIST Special Publication 800-83r1. Guide to Malware Incident Prevention and Handling for Desktops and Laptops. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf (дата звернення: 29.04.2020).

[3] ISO/IEC/IEEE 29148:2011. Systems and software engineering. Life cycle processes. Requirements engineering. [First edition]. Geneva, 2011. 94 p

[4] Nataraj L., Karthikeyan S., Jacob G., Manjunath B., “Malware Images: Visualization and Automatic Classification”, International Symposium on Visualization for Cyber Security (VizSec), (Santa Barbara, July 20, 2011), Santa Barbara, 2011, pp. 1-7.

Д.О. Юдіна, В.В. Цуркан

СПЕЦИФІКАЦІЯ ВИМОГ ДО ПРОГРАМНОГО КОМПОНЕНТУ ОЦІНЮВАННЯ РИЗИКУ КІБЕРБЕЗПЕКИ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Критична інформаційна інфраструктура є одним із основних об'єктів забезпечення кібербезпеки. Для цього розробляється і впроваджується система управління інформаційною безпекою. В межах такого впровадження оцінюється ризик кібербезпеки. Його методологічною основною є настанови державного стандарту ДСТУ ISO/IEC 27005:2019 [1, 2]. Тому специфікування вимог до програмного компоненту оцінювання ризику кібербезпеки критичної інформаційної інфраструктури є актуальним.

Програмним компонентом визначатимуться оцінки ризику кібербезпеки. Отримані результати розміщуватимуться в порядку зменшення їх значень з встановленням пріоритету оброблення кожного з них. Для представлення вимог використано синтаксис [Тема] [Дія] [Значення] [3]:

[Програмний компонет] [Визначення оцінок ризику кібербезпеки] [Оцінка]

З огляду на це, основним варіантом використання програмного компоненту в графічній нотації UML є визначення оцінок ризику кібербезпеки. Цей варіант розширяється визначенням оцінок вірогідності та наслідків реалізації загрози кібербезпеці, а також ранжуванням оцінок ризику кібербезпеки за пріоритетами. При цьому найбільша оцінка ризику матиме найвищий пріоритет – 1. Для його оцінювання використовуватиметься шкала зміни значень вірогідності та наслідків від 0 до 8, а саме [4]: 0 – 2 (низька оцінка); 3 – 5 (середня оцінка); 6 – 8 (висока оцінка). Тоді оцінка ризику кібербезпеки визначатиметься низькою від 0 до 8; середньою від 9 до 35; високою від 36 до 64.

Отже, описанням можливостей програмного компоненту специфіковано вимоги до нього. Кожну з можливостей відображено варіантом використання у графічній нотації UML. Завдяки цьому можливе розроблення логічної і фізичної структур програмного компоненту.

[1] Про основні засади забезпечення кібербезпеки України : Закон України від 08.07.2018 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 30.04.2020).

[2] Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : постанова Кабінету міністрів України від 19.06.2019 № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF (дата звернення: 30.04.2020).

[3] ISO/IEC/IEEE 29148:2011. Systems and software engineering. Life cycle processes. Requirements engineering. [First edition 2011-12-01]. Geneva, 2011. 94 p.

[4] ДСТУ ISO/IEC 27005:2019. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT). [Чинний від 2019-11-01]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2019. 65 с.

С.О. Черната, В.В. Цуркан

СПЕЦИФІКАЦІЯ ВИМОГ ДО ПРОГРАМНОГО КОМПОНЕНТУ АВТОМАТИЗУВАННЯ МЕРЕЖЕВИХ НАЛАШТУВАНЬ

Забезпечення кібербезпеки критичної інформаційної інфраструктури характеризується багатоаспектністю [1]. Серед них виокремлюється розглядання її як коду [2]. Такий спосіб керування мережевими ресурсами орієнтований на автоматизування їх налаштувань. Зокрема [3], конфігурування і взаємодії мережевого обладнання. Тому специфікування вимог до програмного компоненту автоматизування мережевих налаштувань є актуальним

[Програмний компонент] [Автоматизування мережевих налаштувань] [Мережеве налаштування].

Вимоги до програмного компоненту специфіковано діаграмою варіантів використання у графічній нотації UML. Для побудови даної діаграми виокремлено такі варіанти використання: налаштування мережевого обладнання, налаштування взаємодії між мережевим обладнанням, налаштування одночасного конфігурування мережевого обладнання. Вони включаються в основний варіант використання, зокрема, автоматизування мережевих налаштувань. Характерними особливостями такого представлення є як конфігурування окремого мережевого обладнання, так і оброблення інформації з системних журналів [3]. При цьому передбачається можливість їх відправлення на сервер. Водночас організовується перевірка відправлень тільки визначеної інформації з системних журналів. Крім цього, виокремлюється багатопотоковість налаштувань мережевого обладнання. Таку можливість варто враховувати за потреби одночасного налаштування декількох пристроїв, наприклад, маршрутизаторів.

Отже, важливим аспектом забезпечення кібербезпеки критичної інформаційної інфраструктури є розглядання її як коду. Цим визначається необхідність автоматизування мережевих налаштування і, як наслідок, специфікування вимог до програмного компоненту діаграмою варіантів використання у графічній нотації UML.

[1] Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури : постанова Кабінету міністрів України від 19.06.2019 № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF (дата звернення: 30.04.2020).

[2] Wittig A., Wittig M. Amazon Web Services in Action. Shelter Island : Manning Press, 2018. 528 p.

[3] Ratan A. Practical Network Automation Birmingham : Packt Publishing Ltd., 2018, 220 p.

[4] ISO/IEC/IEEE 29148:2011. Systems and software engineering. Life cycle processes. Requirements engineering. [First edition]. Geneva, 2011. 94 p.

М.І. Гітько, В.В. Цуркан

СПЕЦИФІКАЦІЯ ВИМОГ ДО ПРОГРАМНОГО КОМПОНЕНТУ АНАЛІЗУВАННЯ УРАЗЛИВОСТЕЙ ВЕБ ЗАСТОСУНКІВ

Важливим інформаційним активом будь-якої організації є веб застосунки. Вимоги до забезпечення їх (зокрема, сторінок) безпеки від несанкціонованого доступу викладено в [1]. Тоді як настанови зі запобігання реалізуванню загроз через уразливості програмних застосунків описано в [2]. За основу такого підходу стосовно веб застосунків взято OWASP [3, 4]. Тому специфікування вимог до програмного компоненту аналізування уразливостей веб застосунків є актуальним.

Для специфікування вимог до програмного компоненту застосовано графічну нотацію UML. Це дозволило відобразити специфікацію діаграмою варіантів використання. Серед них основним є аналізування уразливостей веб застосунків. Він включає такі варіантами використання [3, 4]: визначення основних метрик, визначення часових метрик, визначення контекстних метрик. Значення даних метрик аналізуються за шкалою [4]: відсутнє – 0,0; низьке – від 0,1 до 3,9; середнє – від 4,0 до 6,9; високе – від 7,0 до 8,9; критичне – від 9,0 до 10,0. Результати аналізування уразливостей веб застосунків представляються послідовністю метрик. Ця послідовність починається міткою «CVSS». Наступний складник – поточна версія системи оцінювання уразливостей, наприклад [4], «3.1». Далі через роздільник «/» вказується набір метрик. Тому відповідно до синтаксису вимог [Тема] [Дія] [Значення] отримаємо [5]:

[Програмний компонет] [Аналізування уразливостей] [Метрика]

Отже, специфікацію вимог до програмного компоненту відображено діаграмою варіантів використання у графічній нотації UML. Для цього враховано їх представлення за синтаксисом вимог.

[1] Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу : наказ ДСТСЗІ СБ України від 02.04.2003 № 33 (зі змінами). URL: http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106344 (дата звернення: 29.04.2020).

[2] ДСТУ ISO/IEC 27034-1:2017 Інформаційні технології. Методи захисту. Безпека прикладних програм. Частина 1. Огляд і загальні поняття (ISO/IEC 27034-1:2011; Cor 1:2014, IDT). [Чинний від 2019-11-01]. Вид. офіц. Київ : ТК «Інформаційні технології», 2019. 79 с.

[3] OWASP Web Security Testing Guide. URL: https://owasp.org/www-project-web-security-testing-guide/ (дата звернення: 29.04.2020).

[4] Common Vulnerability Scoring System SIG. URL: https://www.first.org/cvss/ (дата звернення: 29.04.2020).

[5] ISO/IEC/IEEE 29148:2011. Systems and software engineering. Life cycle processes. Requirements engineering. [First edition]. Geneva, 2011. 94 p.

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

Збірник тез конференції
15 травня 2020 р.

Зб. тез XXXVIII науково-технічної конференції молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, м. Київ, 15 травня 2020 р. / ІПМЕ ім. Г.Є. Пухова НАН України. – 2020. – 147 с.

Інформаційна підтримка:

Сторінка конференції на сайті Інституту

Telegram канал молодих вчених НАН України

Telegram канал молодих вчених ВФТПЕ НАН України

REFERENCES

[1] Andreas Reuter, Randy Bush, Italo Cunha, Ethan Katz-Bassett, Thomas C Schmidt, and Matthias Wählisch. Towards a rigorous methodology for measuring adoption of RPKI route validation and fltering. ACM SIGCOMM Computer Communication Review, 48(1):19–27, 2018.

[2] Andrii Iatsyshyn, Anna Iatsyshyn, Volodymyr Artemchuk, Iryna Kameneva, Valeriia Kovach and Oleksandr Popov. Software means for tasks of sustainable development of environmental problems: peculiarities of programming and implementation in the specialists` preparation. E3S Web of Conferences 166, 01001 (2020). https://doi.org/10.1051/e3sconf/202016601001.

[3] ANSI/ANS-18.1-1999, “Radioactive Source Term for Normal Operation of Light Water Reactors”

[4] ANSI/ANS-18.1-2016 American National Standard «Radioactive Source Term for Normal Operation of Light Water Reactors»

[5] Anton K., Manico J., Bird J. 10 Critical Security Areas That Software Developers Must Be Aware Of // OWASP Top Ten Proactive Controls Project. 2018. – URL: https://owasp.org/www-pdf-archive/OWASP_Top_10_Proactive_Controls_V3.pdf.

[6] Arfire A. Enhancing Measurement Quality Through Active Sampling In Mobile Air Quality Monitoring Sensor Networks / A. Arfire, A. Marjovi, A. Martinoli // Proceedings of the IEEE International Conference on Advanced Intelligent Mechatronics (Banff, Alberta, Canada, July 12–15, 2016). – 2016. – pp. 313–321.

[7] Artemchuk, V. O., & Yatsyshyn, A. V. (2018). Intelligent analysis of data in the system of monitoring of atmospheric air. Modelyuvannya ta Informatsiyni tehnologiyi: GE Pukhov's IMPPE NAS of Ukraine, 82, 48-52.

[8] Artemchuk, V. O., Kameneva, I. P., & Yatsyshyn, À. V. (2017). Specificity of the applicationof cognitive analysis of information in the tasks of ensuring environmental safety. Elektronnoe modelirovanie, 39(6), 107-124.

[9] Artemchuk, V.O. (2011). Mathematical and computer tools for solving the placement of observation points network monitoring air. Dissertation for a Candidate Degree of Engineering Sciences in specialty, Pukhov Institute for Modelling in Energy Engineering of NAS of Ukraine, Kyiv

[10] Artemchuk, V.O., Kameneva, I.P. and Yatsyshyn, À.V. (2017), “Specificity of the applicationof cognitive analysis of information in the tasks of ensuring environmental safety”, Elektronnoe modelirovanie, Vol. 39, no. 6, pp. 107-124.

[11] B. K. Bose. Modern Power Electronics and AC Drives / B. K. Bose. — Prentice Hall PTR, 2002. — 711 p.

[12] Baez, M.J., Larriba Martínez, T., 2015. Technical Report on the Elaboration of a Cost Estimation Methodology. No. D.3.1. Creara, Madrid, Spain.

[13] Bilan T.R. (2015) Methods and means of economic and mathematical modeling of coal industry development under the world market conditions. Thesis for PhD.

[14] Bilan, T. R. (2017). A balance-optimization model for determining the volume of coal production and import with regard for the influence of reconstruction and modernization on the technical and economic characteristics of functioning of coal mining enterprises. The Problems of General Energy, (4 (51)), 15-22.

[15] Bilan, T. R., & Kaplin, M. I. (2016). Security aspects of the balance of carbonaceous fuels under conditions of establishing the new fuel supply schemes in Ukraine. The Problems of General Energy, (4 (47)), 23-29.

[16] Blieberger, J., Burgstaller, B. (2018). Safe non-blocking synchronization in Ada2x. In A. Casimiro, & P. M. Ferreira (Eds.), Reliable Software Technologies – Ada-Europe 2018 - 23rd Ada-Europe International Conference on Reliable Software Technologies, Proceedings (pp. 53-69). (Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Vol. 10873 LNCS). Springer Verlag. https://doi.org/10.1007/978-3-319-92432-8_4.

[17] Blinov I.V., Parus E.V., Ivanov G.A. Complex calculation model of the day-ahead and balancing market of Ukraine // Promelectro – 2016. – No 4-5. – C. 8 – 12.

[18] Budnik K., Machczyński W. Power line magnetic field mitigation using a passive loop conductor. Poznan University of Technology Academic Journals. Electrical Engineering. 2013. No. 73. Pp. 137-145.

[19] Butkevych O.F., Pavlovskiy V.V. Hybrid system in power system problems solving. Tekhnichna elektrodynamika tematychnyi vypusk problemy suchasnoi enerhetyky Kiev 2002 .№ 4 Pp77-82.

[20] Canova A., del-Pino-López J.C., Giaccone L., Manca M. Active shielding system for ELF magnetic fields. IEEE Trans. Magn. 2015. Vol. 51. No 3. Pp. 1-4.

[21] Castell N. Mobile technologies and services for environmental monitoring: The Citi-Sense-MOB approach / N. Castell, M. Kobernus, H.-Y. Liu, P. Schneider, W. Lahoz, A.J. Berre, J. Noll // Urban Climate. – 2015. – Vop. 14, Part 3. – pp. 370–382.

[22] Common Vulnerability Scoring System SIG. URL: https://www.first.org/cvss/ (дата звернення: 29.04.2020).

[23] De Wulf M., Wouters P., Sergeant P., Dupré L., Hoferlin E., Jacobs S., Harlet P. Electromagnetic shielding of high-voltage cables. Journal of Magnetism and Magnetic Materials. 2007. Vol. 316. No. 2. Pp. e908-e911.

[24] Derii, V. O., & Zgurovets, O. V. (2017). Investigation of the schedules of electrical loads of power system for determining the possibilities of their improvement by using electric heat-generators. The Problems of General Energy, (4 (51)), 52-60.

[25] Development of the method with enhanced accuracy for solving problems from the theory of thermo-psevdoelastic-plasticity / A.Petrov, Yu.Chernyakov, P.Steblyanko, K.Demichev, V.Haydurov // Eastern-European Journal of Enterprise Technologies. 2018. Vol. 4/7 (94). P. 25–33.

[26] Energy Efficiency in the Power Grid. https://www.nema.org.

[27] Estimating the Costs and Benefits of the Smart Grid [Електронний ресурс] – http://www.rmi.org/Content/Files/EstimatingCostsSmartGRid.pdf.

[28] European Smart Grid Technology Platform [Електронний ресурс] – http://ec.europa.eu/research/energy/pdf/smartgrids_en.pdf.

[29] Gasparin A., Slobodan L., Alippi C. Deep learning for time series forecasting:the electric load case. 22 Jul 2019.

[30] Geoinformation modeling. https://magneticonemt.com/en/geoinformation-modeling.

[31] Golnaz Ghaisi, Tsung-Yi Lin, Ruoming Pang, Quoc V. Le. NAS-FPN: Learning Scalable Feature Pyramid Architecture for Object Detection. https://arxiv.org/pdf/1904.07392.pdf

[32] Google Cloud AutoML. https://cloud.google.com/automl/

[33] Grinchenko V., Pyrohova U. Mitigation of overhead line magnetic field by U-shaped grid shield. 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering. 2019. Pp. 345-348.

[34] Gross J., Yellen J., Anderson M., Graph theory and its applications. Boca Raton, USA: CRC Press, 2019, 593 p.

[35] Guide to the Measurement of Force. URL: http://resource.npl.co.uk /docs/science_technology/mass_force_pressure/clubs_groups/instmc_weighing_panel/forceguide.pdf. (дата звернення : 29.11.2019).

[36] Guidelines for Smart Grid Cyber Security: Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements.

[37] Haifeng Jin, Qingquan Song, Xia Hu. Auto-Keras: An Efficient Neural Architecture Search System. https://arxiv.org/pdf/1806.10282.pdf

[38] Haokui Zhang, Ying Li, Hao Chen, Chunhua Shen. Memory-Efficient Hierarchical Neural Architecture Search for Image Denoising. https://arxiv.org/pdf/1909.08228.pdf

[39] Hoare C. A. R. An axiomatic basis for computer programming. Communications of the ACM. 1969. Vol. 12, No. 10. P. 576-583.

[40] Hoare C. A. R. Communicating sequential processes. Communications of the ACM. 1978. Vol. 21, No. 8. P. 666-677.

[41] Hochreiter S., Schmidhuber J. Long short-term memory. Neural Computation 9(8): 1997. Pp.1735-1780.

[42] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view.

[43] Iatsyshyn A.V. The Methodology of Future Specialists Teaching in Ecology Using Methods and Means of Environmental Monitoring of the Atmosphere's Surface Layer / A.V. Iatsyshyn, O.O. Popov, V.O. Kovach, V.O. Artemchuk // Journal of Information Technologies in Education. – 2018. – Iss. 66, No 4. – pp. 217–230.

[44] Iatsyshyn, A. V., Kutsan, Y. G., Artemchuk, V. O., Kameneva, I. P., Popov, O. O., & Kovach, V. O. (2019). The principles and methods of ecological safety management through the data of air monitoring network analysis. Elektronne modelyuvannya, 41(4).

[45] Iatsyshyn, A.V., Popov, O.O., Kovach, V.O., Artemchuk, V.O.: The methodology of future specialists teaching in ecology using methods and means of environmental monitoring of the atmosphere's surface layer. Information Technologies and Learning Tools 66(4), 217–230 (2018). doi:10.33407/itlt.v66i4.2233

[46] Iatsyshyn, Anna V., Kovach, V.O., Romanenko, Ye.O., Deinega, I.I., Iatsyshyn, Andrii V., Popov, O.O., Kutsan, Yu.G., Artemchuk, V.O., Burov, O.Yu., Lytvynova, S.H.: Application of augmented reality technologies for preparation of specialists of new technological era. In: Kiv, A.E., Shyshkina, M.P. (eds.) Proceedings of the 2nd International Workshop on Augmented Reality in Education (AREdu 2019), Kryvyi Rih, Ukraine, March 22, 2019, CEUR Workshop Proceedings 2547, 181–200. http://ceur-ws.org/Vol-2547/paper14.pdf (2020).

[47] IEC 61508 Edition 2.0. Functional safety of electrical/electronic/programmable electronic safety-related systems. [Approved: April 2010]. URL: https://www.iec.ch/functionalsafety/standards/page2.htm. (Accessed: 07.02.2020).

[48] IEC 62351. Power systems management and associated information exchange - Data and communications security.

[49] IEC 62443. Cyber Security for Industrial Automation and Control Systems (IACS).

[50] Intro to Next Generation Firewalls [Електронний ресурс] – https://www.esecurityplanet.com/security-buying-guides/intro-to-next-generation-firewalls.html.

[51] ISO / IEC 27001: 2013 [Електронний ресурс] // - Режим доступу: https://www.iso.org/obp/ui/fr/#iso:std:iso-iec:27001:ed-2:v1:fr (18.10.2019).

[52] ISO/IEC 27005: 2018 [Електронний ресурс] - https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-3:v1:en.

[53] ISO/IEC 27019. Information technology — Security techniques — Information security controls for the energy utility industry.

[54] ISO/IEC/IEEE 29148:2011. Systems and software engineering. Life cycle processes. Requirements engineering. [First edition]. Geneva, 2011. 94 p

[55] JETSON NANO [Електронний ресурс] // NVIDIA Corporation. – 2020. – Режим доступу до ресурсу: https://www.nvidia.com/ru-ru/autonomous-machines/embedded-systems/jetson-nano/.

[56] Jorge Alcántara, Silvia Medina. Quintana The use of Educational Itineraries (GIS) in Environmental Education. Enseñanza de las ciencias, 37-2 (2019), 173-188 doi:10.5565/rev/ensciencias.2258

[57] Kang L. A Public Transport Bus as a Flexible Mobile Smart Environment Sensing Platform for IoT / L. Kang, S. Poslad, W. Wang, X. Li, Y. Zhang, C. Wang // Proceedings of the 2016 12th International Conference on Intelligent Environments (London, UK, September 14-16, 2016). – 2016. – pp. 1–8.

[58] Karen Simonyan, Andrew Zisserman. VERY DEEP CONVOLUTIONAL NETWORKS FOR LARGE-SCALE IMAGE RECOGNITION. https://arxiv.org/pdf/1409.1556.pdf

[59] KULYK MM, D. I., & ZGUROVETS, O. (2018). Feasibility of using battery energy storage systems for frequency stabilization in integrated power systems with powerful solar power plants.

[60] KULYK MM, D. I., & ZGUROVETS, O. (2018). Investigation of the operating modes of integrated power systems with powerful wind power plants and accumulator batteries.

[61] Kulyk, M. M., & Zgurovets, O. V. (2018). Features of the use of hydroelectric power plants and battery energy storage systems for frequency stabilization in power systems. Energy Technologies & Resource Saving, (4), 3-11.

[62] Kuppe M. A., Lamport L., Ricketts D. The TLA+ Toolbox. Formal Integrated Development Environment, F-IDE 2019 : 5th Workshop (Porto, Portugal, October 7, 2019). EPTCS 310, 2019. P. 50-62. DOI: http://doi.org/10.4204/EPTCS.310.6

[63] Kuts, G. O., Malyarenko, O. Y., Stanytsina, V. V., & Bogoslavska, O. Y. (2017). Estimation of the state and forecast of structure of the consumption of fuel and energy for heat supply systems of Ukraine with regard for regional peculiarities. The Problems of General Energy, (4 (51)), 23-32.

[64] Kuznetsov B., Bovdui I., Voloshko A., Nikitina T. Modeling and active shielding of magnetic field in residential buildings located near group of high voltage power lines. 2018 IEEE 3rd International Conference on Intelligent Energy and Power Systems. 2018. Pp. 106-109.

[65] Lamport L. Specifying systems: The TLA+ language and tools for hardware and software engineers. Boston : Addison-Wesley, 2002. 382 p.

[66] Lancia G. A Facility Location Model for Air Pollution Detection / G. Lancia, F. Rinaldi, P. Serafini // Mathematical Problems in Engineering. – 2018. – pp. 1–8.

[67] Lee J.-T., Kim H.-G. *, Kang Y.-H., Kim J.Y.. Determining the Optimized Hub Height of Wind Turbine Using the Wind Resource Map of South Korea. Energies 2019, 12, 2949; doi:10.3390/en12152949.

[68] Levandowski C. Evaluating Tall Wind Turbine Towers in the Field. 2015. https://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=1116&context=undergradresearch_symposium.

[69] List of Known Meshlocals [Електронний ресурс] – https://docs.meshwith.me/meshlocals/existing/.

[70] Liu L. A Fault-Tolerant Mobile Sensing Information Gathering Center (MSIGC) Using Public Transport Buses to Instrument a Smart City / L. Liu, J. Duan, Z. Xiao, C. Wang, X. Li // Proceedings of the 2017 9th International Conference on Advanced Infocomm Technology (Chengdu, China, November 22–24, 2017). – 2017. – pp. 233–238.

[71] Lukashov V., S. Romanko, S. Timofeev, Protsenko A. Rate of Components Evaporation from Sulfuric Acid Solution During Its Concentrating in Air Flow / Chemistry & Chemical Technology, Vol. 11, No. 3, pp. 344–348, 2017.

[72] Lyudmila Datsenko. Expansion of geographic information components in the educational programs of cartographers at Taras Shevchenko National University of Kyiv. The Problems of Continuous Geographical Education and Cartography, 2017, №. 25. С. 20-23. https://periodicals.karazin.ua/pbgok/article/view/9080/8603

[73] M. Orvos, V. Szabo, and T. Poos Rate of Evaporation from the Free Surface of a Heated Liquid, Journal of Applied Mechanics and Technical Physics, Vol. 57, No. 6, pp. 1108–1117, 2016

[74] Malyarenko, O. Y., Maistrenko, N. Y., & Stanytsina, V. V. (2015). Advanced technical approach to identify appropriate energy saving potential in energy-intensive economic activities. The Problems of General Energy, (3 (42)), 23-30.

[75] Malyarenko, O. Y., Maistrenko, N. Y., & Stanytsina, V. V. (2016). Substantiation of the predictive volumes of energy saving potential in the enlarged sectors of economy with regard for technological and structural changes. The Problems of General Energy, (4 (47)), 58-67.

[76] Malyarenko, O. Y., Maystrenko, N. Y., & Stanytsina, V. V. (2015). Rozvytok teoretychnykh zasad ta rozroblennia metodiv i zasobiv prohnozuvannia potreby v enerhetychnykh resursakh z urakhuvanniam strukturnykh i tekhnolohichnykh zrushen'. Zvit pro NDR: DR№ 0113U001133, Inv.№ 0716U000186. Kyiv: Instytut zagal'noi energetyky NAN Ukrainy [in Ukrainian].

[77] MERIT. List of Routing Registries. [Електронний ресурс] Режим доступу: http://www.irr.net/docs/list.html. Дата звернення: Апр.20, 2020.

[78] MobSF Documnetation. URL: https://mobsf.github.io/docs/#/ (дата звернення: 30.04.2020).

[79] Mokhor V., Gonchar S. The Idea of the Construction of the Algebra of Risks on the Basis of the Theory of Complex Numbers. Electronic modeling, 2018, Vol.40, no. 4, pp. 107-111.

[80] Mokhor V., Gonchar S., Dybach O. Methods for the Total Risk Assessment of Cybersecurity of Critical Infrastructure Facilities. Nuclear and Radiation Safety, 2019, 2(82), pp. 4-8.

[81] N.V. Sytnyk, I.S. Zinovieva, «Evolution of the concept of database organization in the context of the digitalization of society», на II Національній науково-методичній конференції «Цифрова економіка», Київ, 2019, с. 150-153.

[82] Nataraj L., Karthikeyan S., Jacob G., Manjunath B., "Malware Images: Visualization and Automatic Classification", International Symposium on Visualization for Cyber Security (VizSec), (Santa Barbara, July 20, 2011), Santa Barbara, 2011, pp. 1-7.

[83] NIST Special Publication 800-83r1. Guide to Malware Incident Prevention and Handling for Desktops and Laptops. URL: https://nvlpubs.nist.gov/nistpubs/ SpecialPublications/NIST.SP.800-83r1.pdf (дата звернення: 29.04.2020).

[84] Nochvay V., Kryvakovska R., Ishchuk O. Use of GIS in the problems of air quality management. Electronics and information technologies. 2012. Issue 2. P. 154–163.

[85] NUREG-0016 «Calculation of Releases of Radioactive Materials in Gaseous and Liquid Effluents from Boiling Water Reactors», 1979

[86] NUREG-0017 «Calculation of Releases of Radioactive Materials in Gaseous and Liquid Effluents from Pressurized Water Reactors», 1985

[87] О.А. Владимирський. Низькочастотна віброкалібрувальна установка на основі лінійного актуатора з зубчастим ременем і кроковім двигуном. Науково-практична конференція «Безпека енергетики в епоху цифрової трансформації», 20.12.2019р. – С48-49.

[88] OWASP API Security Project: specification. URL: https://owasp.org/www-project-api-security/ (дата звернення: 30.04.2020).

[89] OWASP Mobile security testing guide (MSTG). URL: https://github.com/OWASP/ owasp-mstg/ (дата звернення: 30.04.2020).

[90] OWASP Web Security Testing Guide. URL: https://owasp.org/www-project-web-security-testing-guide/ (дата звернення: 29.04.2020).

[91] Pakonen A., Tahvonen T., Hartikainen M., Pihlanko M. Practical applications of model checking in the Finnish nuclear industry. Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies : Proc. 10th International Topical Meeting (San Francisco, CA, USA, 11-15 June 2017). P. 1342-1352.

[92] Pavlos Sermpezis, Vasileios Kotronis, Alberto Dainotti, and Xenofontas Dimitropoulos. A survey among network operators on BGP prefx hijacking. ACM SIGCOMM Computer Communication Review, 48(1):64–69, 2018.

[93] Peiye Liu, Bo Wu, Huadong Ma, Pavan Kumar Chundi, Mingoo Seok. MemNet: Memory-Efficiency Guided Neural Architecture Search with Augment-Trim learning. https://arxiv.org/pdf/1907.09569v1.pdf

[94] Poos T, Varju E. Determination of evaporation rate at free water surface, 8th International Symposium on Exploitation of Renewable Energy Sources, p. 66-71 2016

[95] Popov, O., Iatsyshyn, A., Kovach, V., Artemchuk, V., Taraduda, D., Sobyna, V., ... & Yatsyshyn, T. (2019). Physical Features of Pollutants Spread in the Air During the Emergency at NPPs. Nuclear and Radiation Safety, (4 (84)), 88-98.

[96] Popov, O., Iatsyshyn, A., Kovach, V., Artemchuk, V., Taraduda, D., Sobyna, V., ... & Matvieieva, I. (2019). Analysis of Possible Causes of NPP Emergencies to Minimize Risk of Their Occurrence. Nuclear and Radiation Safety, (1), 81.

[97] Popov, O.; Iatsyshyn, A.; Kovach V.; Artemchuk V.; Taraduda D.; Sobyna V.; Sokolov D.; Dement M.; Yatsyshyn T. (2018). "Conceptual Approaches for Development of Informational and Analytical Expert System for Assessing the NPP impact on the Environment". Nuclear and Radiation Safety. Iss. 3(79), pp. 56—54. doi:10.32918/nrs.2018.3(79).09 (Ukr)

[98] Popov, O.O., Iatsyshyn, A.V., Kovach, V.O., Artemchuk, V.O., Kameneva, I.P., Taraduda, D.V., Sobyna, V.O., Sokolov, D.L., Dement, M.O., Yatsyshyn, T.M.: Risk Assessment for the Population of Kyiv, Ukraine as a Result of Atmospheric Air Pollution. Journal of Health and Pollution 10(25), 200303 (2020). doi:10.5696/2156-9614-10.25.200303.

[99] Pramod J. Sadalage, Martin Fowler, «Introduction to Polyglot Persistence: Using Different Data Storage Technologies for Varying Data Storage Needs», InformIT, #5, 2012. [Online]. Available: https://www.informit.com /articles/article.aspx?p=1930511. Accessed on: April 21, 2020.

[100] Price index for wind turbines in the U.S. from 2008 to 2019. https://www.statista.com/statistics/499491/us-wind-turbine-price-index.

[101] Projected Costs of Generating Electricity. International Energy Agency (IEA). 2010. 218 p.

[102] R. Leszczyna. A Review of Standards with Cybersecurity Requirements for Smart Grid. // Computers & Security, 2018.

[103] Radio Wave Characterization and Modeling in Underground Mine Tunnels/ [Mathieu Boutin, Ahmed Benzakour, Charles L. Despins]- IEEE Trans. Antennas Propag., vol. 23, no.2, pp. 540–549 Feb. 2008

[104] Raju H.P. Urban Mobile Air Quality Monitoring Using GIS, GPS, Sensors and Internet / H.P. Raju, P. Partheeban, R.R. Hemamalini // International Journal of Environmental Science and Development. – 2012. – Vol. 3, No. 4. – pp. 323–327.

[105] Ratan A. Practical Network Automation Birmingham : Packt Publishing Ltd., 2018, 220 p.

[106] Ray-optical prediction of radio-wave propagation characteristics in tunnel environments/ [Y. P. Zhang, Y. Hwang, and R. G. Kouyoumjian] - Part 2: Analysis and measurements," IEEE Trans. Antennas Propag., vol. 46, no. 9, pp. 1337–1345, Sep. 1998.

[107] Real, E., Aggarwal, A., Huang, Y., Le, Q.V. Aging Evolution for Image Classifier Architecture Search. In: AAAI Conference on Artificial Intelligence (2019)

[108] RIPE NCC. BGP Origin Validation. [Електронний ресурс] Режим доступу: https://www.ripe.net/manage-ips-and-asns/resource-management/certification/bgp-origin-validation. Дата звернення: Апр.20, 2020.

[109] Risk Management in Software Development and Software Engineering Projects [Електронний ресурс] Режим доступу: https://www.castsoftware.com/research-labs/risk-management-in-software-development-and-software-engineering-projects. Дата звернення: Апр.22,2020.

[110] Rosenblatt F. The perceptron: a probabilistic model for information storage and organization in the brain. Psychological Review Vol. 65, No. 6, 1958.

[111] RPKI ROA Deletion: Post-mortem [Електронний ресурс] Режим доступу: https://www.ripe.net/ripe/mail/archives/routing-wg/2020-April/004072.html. Дата звернення: Апр.21,2020.

[112] Shifttstas. Hyperboria [Електронний ресурс] – https://habr.com/post/181862/.

[113] Shm non-blocking algorithm [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/exist009/Shm.

[114] Shm non-blocking algorithm performance test [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/exist009/Shm_test.

[115] Simulation and study of modes for full-scale mode simulator for Ukrainian energy systems / V.Gurieiev, O.Sanginova//2nd International Conference on Intelligent Energy and Power Systems (IEPS'2016), June 7–11,Kyiv, Ukraine. –2016. –P. 97–100.

[116] Strong Theory of the propagation of UHF radiowaves in coal mine tunnels/ [A. Emslie, R. Lagace] - IEEE Trans. Antennas Propag.,vol. 23, no. 2, pp. 192–205, Mar. 1975.

[117] The World Health Organization, "The International EMF Project". [Online]. Available: http://www.who.int/peh-emf/project/en/. [Accessed: 22-Apr-2020].

[118] This is how you deal with route leaks. Qrator Labs corporate blog, Information Security, Network technologies [Електронний ресурс] Режим доступу: https://habr.com/en/company/qrator/blog/495260/. Дата звернення: Апр.21,2020.

[119] Thread Classification Development View // The Web Application Security Consortium. – URL: http://projects.webappsec.org/w/page/13246969/Threat Classification Development View

[120] Tsurkan O., Herasymov R., Kruk O., "Presentation the interaction of the subject and the object of socio-engineering influence with a social graph", Computer and Information systems and technologies : fourth International Scientific and Technical Conference (Kharkiv, April 22-23, 2020). Kharkiv, 2020. P. 46.

[121] Unified Modeling Language: maual - URL: https://www.omg.org/spec/UML/2.5.1/PDF (дата звернення: 30.04.2020).

[122] V. Kuchanskyy, "The application of controlled switching device for prevention resonance overvoltages in nonsinusoidal modes," 2017 IEEE 37th International Conference on Electronics and Nanotechnology (ELNANO), Kiev, 2017, pp. 394-399.

[123] V.O. Artemchuk, and A.V. Yatsyshyn, «Intelligent analysis of data in the system of monitoring of atmospheric air», Modelyuvannya ta Informatsiyni tehnologiyi: G.E.Pukhov's IMPPE NAS of Ukraine, Vol. 82, pp. 48-52, 2018.

[124] Web Application Firewall – захист сайту від хакерських атак [Електронний ресурс] – https://habr.com/ru/post/60590.

[125] White Paper: Heat Pumps - Integrating Technologies to Decarbonise Heating and Cooling. Available at: https://www.ehpa.org/fileadmin/red/ 03._Media/ Publications/ehpa-white-paper-111018.pdf

[126] Wittig A., Wittig M. Amazon Web Services in Action. Shelter Island : Manning Press, 2018. 528 p.

[127] Yerofeyev V.A., Miller S.S. Ul'trazvukovoy monitoring mikrodefektov v metalle. Zhurnal “Izvestiya Tul'skogo gosudarstvennogo universiteta”, mashinostroyeniye i mashinovedeniye. 2014. S. 211–217.

[128] Yurii Kyrylenko, Iryna Kameneva, Oleksandr Popov, Andrii Iatsyshyn, Volodymyr Artemchuk, Valeriia Kovach. Source Term Modelling for Event with Liquid Radioactive Materials Spill. Collective monograph “Systems, Decision and Control in Energy I”. Springer. 2020

[129] Zaporozhets A.O. Review of quadrocopters for energy and ecological monitoring / A.O. Zaporozhets // Systems, Decision and Control in Energy I. Studies in Systems, Decision and Control. – 2020. – vol. 298.

[130] Zgurovets, O. V. (2018). Influence of dead band and speed of the regulator on frequency stabilization process in power system with powerful wind power plants and battery energy storage systems. The Problems of General Energy, (3 (54)), 31-35.

[131] Zilberman B. Ya., Ryabkov D. V., Puzikov E. A., Andreeva E. V. and Mishina N. E. Influence of Pressure (Temperature) on the Nitric Acid Distribution between the Liquid and Vapor in the Course of Evaporation of Nitric Acid Radioactive Waste / Radiochemistry, 2016, Vol. 58, No. 3, pp. 237–242, 2016

[132] Zinovieva, I. S., Artemchuk, V. O., & Atsyshyn, A. V. (2018). The use of open geoinformation systems in computer science education. Information Technologies and Learning Tools, 68(6), 87-99.

[133] А.А.Владимирский, И.А. Владимирский, А.И.Дрозденко. Модернизированный термоакустический течеискатель А-10Т2. Збірник наукових праць. Інститут проблем моделювання в енергетиці НАН України. Вип. 70, Київ, 2014р.-с.93-97.

[134] Аксенов С.В. Организация и использование нейронных сетей (методы и технологии) / С.В. Аксенов, В.Б. Новосельцев. – Томск.: Изд-во НТЛ, 2006. – 128 с.

[135] Аналіз зарубіжної практики впровадження автоматизованих систем управління технологічними процесами в електроенергетиці [Електронний ресурс] - https://ua.energy/wp-content/uploads/2018/01/2.-SMART-GRID.pdf.

[136] Аналіз можливих причин виникнення надзвичайних ситуацій на АЕС з метою мінімізації ризику їх виникнення / [О.О. Попов, А.В. Яцишин, В.О. Ковач, В.О. Артемчук, Д.В. Тарадуда, В.О. Собина, Д.Л. Соколов, М.О. Дement, Т. М. Яцишин, І. В. Матвєєва] - Ядерна та радіаційна безпека, 2019, Вип. 1(81). - с. 75-80.

[137] Андреева Л Е. Упругие элементы приборов. 2-е изд. перераб. и доп. М: Машиностроение, 1981. 392 с.

[138] Андрианов С.Н. Некоторые проблемы теоретического и компьютерного моделирования. Андрианов С.Н. Труды I Междунар. науч.-практ. конф. “Современные информационные технологии и ИТ-образование”. Москва, 2005. С. 92–99.

[139] Антонішин М.В., Міснік О.І., Цуркан В.В., «Аналіз якості роботи сканерів уразливостей веб – застосунків», Моделювання та інформаційні технології, Вип. 83, 2018, С. 77-86.

[140] Антонішин М.В., Міснік О.І., Цуркан В.В., «Оцінювання стану захищеності програмних застосунків операційної системи Android за методологією OWASP Mobile TOP 10», Моделювання та інформаційні технології. 2018. Вип. 82. С. 94-101.

[141] Анфімова Г.В. Досвід створення системи метрологічного та технічного супроводу впроваджених засобів технічної діагностики енергетичного та енергоємного обладнання. Науково-практична конференція «Безпека енергетики в епоху цифрової трансформації», ІПМЕ ім. Г.Е.Пухова НАН України, Київ, 20.12.2019р. – С 35-36.

[142] Апаратно-програмне забезпечення моніторингу об’єктів генерування, транспортування та споживання теплової енергії / [В.П. Бабак, С.В. Бабак, В.С. Берегун та ін.; за ред. чл.-кор. НАН України В.П. Бабака]. – К., Ін-т технічної теплофізики НАН України, 2016. – 352 с.

[143] Артамонов Ю.С., Востокін С.В., «Розробка розподілених додатків збору і аналізу даних на базі мікросервісной архітектури», Вісті Самарського наукового центру Російської академії наук, Вип. 4, 2016, 688-693 С.

[144] Артемчук В.О. Перспективи розробки математичних та програмних засобів перевірки екологічної ефективності прийняття управлінських рішень / В.О. Артемчук, А.В. Яцишин, О.О. Попов, Ю.О. Кириленко, Т.М. Яцишин // Моделювання та інформаційні технології. - 2018. - Вип. 85. - С. 75-80.

[145] Архангельский Н.Л. Электропривод постоянного тока с импульсным преобразователем. /Архангельский Н.Л., Виноградов А.Б. // Учебн. пособ. Иваново: Изд-во Иван. гос. энерг. ун-т., 1995. 92 с.

[146] Блинов И.В. Определение вида короткого замыкания ЛЭП на основе искусственных нейронных сетей. Тех. електродинаміка. Тем. випуск: Силова електроніка та енергоефективність. 2007. С. 49-52.

[147] Блінов І.В., Корхмазов Г.С. Використання штучних нейронних мереж для розв'язання задачі короткострокового прогнозування оптових ринкових цін на електричну енергію. Праці інституту електродинаміки НАН України. Тем. вип.: Енергетичні ринки: перехід до нової моделі ринку двосторонніх контрактів і балансуючого ринку. 2009. С. 15 – 22.

[148] Блінов І.В., Мірошник В.О., Шиманюк П.В. Короткостроковий інтервальний прогноз сумарного відпуску електроенергії виробниками з відновлюваних джерел енергії. Праці інституту електродинаміки НАН України. 2019р. №54 С. 5-12.

[149] Блінов І.В., Мірошник В.О., Шиманюк П.В. Короткостроковий інтервальний прогноз сумарного відпуску електроенергії виробниками з відновлювальних джерел енергії // Праці Інституту електродинаміки НАН України. Вип. 54: 5-12, 2019.

[150] Блінов І.В., Парус Є.В., Іванов Г.А. Імітаційне моделювання функціонування балансуючого ринку електроенергії з урахування системних обмежень на параметри ОЕС України // Технічна електродинаміка. 2017. №6. С.72 – 79.

[151] Блінов І.В., Попович В.І. Гармонізована рольова модель європейського ринку електроенергії. Проблеми загальної енергетики. 2011. № 3(26). С. 5 – 11.

[152] В. З. Стецюк, А. В. Малєй, О. І. Лісовиченко, Н. О. Пічкур , Л. Ю. Бабінцева Особливості розроблення концептуальної математичної моделі процесу раннього діагностування спадкових орфанних захворювань ISSN 1996-1960. Медична інформатика та інженерія. 2018, No 2 -44 - 53 с

[153] Верлань А.А. Интегральные динамические модели электромеханических объектов: Монография. Верлань А.А., Сагатов М.В., Федорчук В.А. Т.: IQTISOD-MOLYA ISBN 978-9943-13-581, 2015. 328 с.

[154] Верлань А.А. Підходи до побудови скалярних динамічних моделей розподілених ланок керованих електромеханічних систем. Верлань А.А., Федорчук В.А. Математичне та комп'ютерне моделювання. Серія: Технічні науки : зб. наук. праць.– Інститут кібернетики імені В. М. Глушкова НАНУ. Кам'янець-Подільський національний університет ім. Івана Огієнка.– Кам'янець-Подільський: К-ПНУ. 2016. Вип. 13. С. 49-61.

[155] Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу : наказ ДСТСЗІ СБ України від 02.04.2003 № 33 (зі змінами). URL: http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106344 (дата звернення: 29.04.2020).

[156] Владимирський О.А., Владимирський І.А. Комп'ютерна програма “Термо-акустический течеискатель”. Свідоцтво про реєстрацію авторського права на твір №60778. Україна. 23.07.2015р. /ІПМЕ НАН України.

[157] Волков И.В. Принципы построения и оптимизация схем индуктивно-емкостных преобразователей / И.В. Волков, В.Н. Губаревич, В.Н. Исаков, В.П. Кабан // К: Наукова думка, 1981. 173 с.

[158] Галушкин А.И. Теория нейронных сетей. / А.И. Галушкин. [учеб. пособие для ВУЗов] – М.:ИПРЖР, 2010. – 496 с.

[159] Гильгурт С.Я. Реконфигурируемые вычислители. Аналитический обзор // Электронное моделирование. – 2013. – Т. 35, № 4. – С. 49-72.

[160] Гільгурт С.Я. Методи побудови оптимальних схем розпізнавання для реконфігуровних засобів інформаційної безпеки // Захист інформації. – 2019. – Т. 25, № 2. – С. 74-81.

[161] Гончар С.Ф. Оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури. Монографія – Київ: Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національна академія наук України, 2019. - 175с.

[162] Грінченко В.С. Зниження магнітного поля трифазних ліній електропередачі ґратчастим електромагнітним екраном / В.С. Грінченко // Технічна електродинаміка. – 2018. – № 4. – С. 29-32.

[163] Гурєєв В.О. Моделювання великих енергосистем для побудови комп'ютерних розподілених тренажерних систем в енергетиці // Моделювання та інформаційні технології. Збірник наукових праць ІПМЕ ім. Г.Є. Пухова. – 2018. Вип. 83.– С. 94–105.

[164] Гурєєв В.О. Розробка алгоритмів і програм швидкодійних методів розрахунку режимів роботи великих електроенергетичних систем (ЕЕС) і енергооб'єднань (ЕО) для тренажерів // Наукові праці ВНТУ, - 2018, № 1, С. 1-5.

[165] ДСТУ EN 61000-3-12:2014 Електромагнітна сумісність. Частина 3-12. Норми. Норми на силу струму гармонік, створені обладнанням із номінальним вхідним струмом силою понад 16 А та до 75 А включно на фазу, підключеним до низьковольтних елекропостачальних систем загальної призначеності (EN 61000-3-12:2011, IDT)

[166] ДСТУ ISO/IEC 27005:2019. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT). [Чинний від 2019-11-01]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2019. 65 с.

[167] ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT). [Чинний від 2018-01-01]. Вид. офіц. Київ : ТК «Інформаційні технології», 2018. 50 с.

[168] ДСТУ ISO/IEC 27034-1:2017 Інформаційні технології. Методи захисту. Безпека прикладних програм. Частина 1. Огляд і загальні поняття (ISO/IEC 27034-1:2011; Cor 1:2014, IDT). [Чинний від 2019-11-01]. Вид. офіц. Київ : ТК «Інформаційні технології», 2019. 79 с.

[169] Енергетична стратегія України на період до 2030 року [Електронний ресурс] – http://www.niss.gov.ua/ public/File/2014_nauk_an_rozrobku/Energy %20Strategy %202035.pdf.

[170] Ефективність Web Application Firewall [Електронний ресурс] – https://xakep.ru/2011/11/21/57840.

[171] Євдокимов В.Ф., Давиденко А.М., Гільгурт С.Я. Створення на базі грід-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. – Вип. 79. – К.: 2017. – С. 3-8.

[172] Жежнич, П.І., Осика, В.О. Функціональні та структурні вимоги до побудови сучасних географічних інформаційних систем. Інформаційні системи та мережі. 2011, №715, С. 104-113

[173] Зайцев Є.О., Левицький А.С., Панчик М.В. Особливості процесу пресування осердя статора потужного турбогенератора. Електромеханічні та енергетичні системи. Методи моделювання та оптимізації: Збірник наукових праць XVII Міжнародної науково-технічної конференції молодих учених і спеціалістів, 11-12 квітня 2019 м. Кременчук, Україна, 2019. С.81-83.

[174] Закон України «Про ринок електричної енергії» від 13.04.2017 №2019-VIII.

[175] Зарубіжний досвід підвищення ефективності передавання та розподілу електроенергії, оптимізації втрат електроенергії в електромережах всіх рівнів напруги/ НТЦЕ НЕК «Укренерго». 2015.

[176] Звіт про надання послуг зі статистичної та аналітичної обробки інформації щодо подій (порушення, відхилення та малозначущі події) у роботі АЕС України, які відбулись у ІІ півріччі 2019 року та І півріччі 2020 року «Статистична та аналітична обробка інформації щодо подій у роботі АЕС України, які відбулись у ІІ півріччі 2019 року». – Київ: ДНТЦ ЯРБ, 2020.

[177] І.С. Зінов'єва, В.О. Артемчук, «Сучасні підходи до подальшої еволюції концепції баз даних», in III International scientific and practical conference «Dynamics of the development of world science», Canada, 2019, pp. 34–44.

[178] Iatsyshyn, A. V., Popov, O. O., Artemchuk, V. O., Kovach, V. O., & Zinovieva, I. S. AUTOMATED AND INFORMATION DECISION SUPPORT SYSTEMS FOR ENVIRONMENTAL SAFETY.

[179] Каменева І. П., Кириленко Ю. О. Підготовка вихідних даних для задач моделювання радіаційного впливу при аваріях із розливом рідких радіоактивних середовищ Зб. тез VI міжнародної наукової конференції «Моделювання-2018», Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, м. Київ, 12-14 вересня 2018 р. / ІПМЕ ім. Г.Є. Пухова НАН України, 2018. – С. 162-165

[180] Каменева, И. П., Яцишин, А. В., & Артемчук, В. А. (2013). Компьютерные средства оценивания экологических рисков с использованием структурного анализа данных мониторинга. Электронное моделирование.

[181] Карпов А.И. Психология групповых решений – М.: Юрист.2008.-55 с.

[182] Каханер Д. Численные методы и программное обеспечение: пер. с англ. /Д. Каханер К. Моулер, С. Нэш.-М.:Мир,1998.-575с.

[183] Кириленко О.В., Блінов І.В., Парус Е.В. Визначення результатів аукціону з купівлі-продажу електричної енергії. Проблеми загальної енергетики. 2010. № 3. С. 5 – 12.

[184] Кириленко Ю. О. Особливості радіаційного впливу при аваріях із розливом рідких радіоактивних середовищ. – Зб. тез науково-технічної конференції молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, м. Київ, 16 травня 2018 р. / ІПМЕ ім. Г.Є. Пухова НАН України, 2018. – С. 23-26

[185] Кириченко Л., Радивилова Т., Барановский А., «Обнаружение киберугроз с помощью анализа социальных сетей», Information Technologies & Knowledge, 2017, vol. 11, no 1, P. 23-48.

[186] Когнитивная психология /Андерсон Дж. Р.- СПб.: Питер, 2002.-496 с.

[187] Конотоп, Д. І. (2019). Інформаційна технологія створення та супроводження узагальненої моделі складних технічних об'єктів.

[188] Коршунов А., Белобородов И., Бузун Н., и др., «Анализ социальных сетей: методы и приложения», Труды Института системного программирования РАН, 2014. Том 26, № 1. С. 439-456.

[189] Кузнецов В.Г. Використання штучної нейронної мережі для визначення характеристик анормальних перенапруг / В.Г. Кузнецов, Ю.І. Тугай В.В. Кучанський // Праці Інституту електродинаміки НАН України. – К.: ІЕД НАНУ, 2012. – Вип. 31. – С. 8–14.

[190] Куц Г.О., Маляренко О.Є., Станиціна В.В., Богославська О.Ю. Оцінка стану та прогноз структури палива та енергії для систем теплопостачання України з урахуванням регіональних особливостей. Проблеми загальної енергетики. 2017. Вип. 4 (51). С. 23-32. URL: https://doi.org/10.15407/pge2017.04.023

[191] М. Комаров, «Підсистема управління доступом системи управління базами даних ORACLE DATABASE 12C ENTERPRISE EDITION», Моделювання та інформаційні технології, №84, С. 87-96, 2018.

[192] М. Комаров, С. Гончар, «Аналіз механізмів безпеки системи управління базами даних Oracle Database 12C enterprise Edition», Моделювання та інформаційні технології, №85, С. 107-116, 2018.

[193] М.В. Антонішин, О.І. Міснік, В.В. Цуркан, “Оцінювання стану захищеності програмних застосунків операційної системи Android за методологією OWASP Mobile TOP 10”, Моделювання та інформаційні технології. 2018. Вип. 82. С. 94-101.

[194] Математичне моделювання термомеханічних процесів в пружно-пластичних циліндричних тілах / [К.Е.Дьомічев, П.О.Стеблянко, Ю.А.Черняков, О.Д.Петров]. – Київ, 2017. – 169 с.

[195] Машинне навчання. / [Іван Гудфелов, Йоша Бенгіо, Арон Коурвілле] MIT Press, 2016. Режим доступу: http://www.deeplearningbook.org.

[196] Міснік О.І., «Проблеми використання систем виявлення та запобігання вторгнення в контейнерні середовища», Комп’ютерні та інформаційні системи та технології : зб. тез доп. четвертої міжнародної науково-технічної конференції, (м. Харків, Квітень 22-23, 2020), Харків, 2020, С. 15.

[197] Москаленко, В. В., Москаленко, А. С., Москаленко, А. С., Берест, О. Б., Мартиненко, С. С., Мартыненко, С. С., Окопный, Р. П. (2018). Інтелектуальна автономна бортова система безпілотного літального апарату для ідентифікації об'єктів на місцевості. Сумський державний університет.

[198] Наміот Д., Снепс-Снеппе М., «Про мікросервісну архітектуру», Міжнародний журнал відкритих інформаційних технологій, Вип 9, 2014, 24-27 С.

[199] Норми радіаційної безпеки України (НРБУ-97). Затверджено МОЗ Наказом №208 від 14 липня 1997р.

[200] Норми радіаційної безпеки України, доповнення: Радіаційний захист від джерел потенційного опромінення (НРБУ-97/Д-2000). Затверджено МОЗ Наказом №116 від 12 липня 2000 р.

[201] НП 306.2.141-2008. Загальні положення безпеки атомних станцій

[202] НП 306.2.162-2010 Вимоги до оцінки безпеки атомних станцій

[203] НП 306.2.173-2011. Вимоги щодо визначення розмірів і меж зони спостереження АЕС. Із змінами, внесеними згідно з Наказом Державної інспекції ядерного регулювання N 206/765 від 23.11.2015

[204] О.А. Владимирський, І.А. Владимирський, А.П. Іващенко, І.П. Криворучко. Розробка структури низькочастотної автоматизованої віброкалібрувальної установки НАВКУ-3. Моделювання та інформаційні технології. Вип. 89.

[205] О.А.Владимирский, І.П., Криворучко. Пристрій для установки вібродатчика з магнітним тримачем на ґрунт при пошуку витоків. Заявка u201912229 від 24.12.2019р. на корисну модель (патент). Рішення про видачу деклараційного патенту на корисну модель № 6750/ЗУ/20 від 07.04.2020р.

[206] Орлов А. И. Экспертные оценки. Учебное пособие. М.: ИВСТЭ, 2002

[207] Основні санітарні правила забезпечення радіаційної безпеки України (ОСПУ-2005)

[208] Оценка риска аварий с использованием экспертных систем /Немчинов Д. В. - Вестн. Астрахан. гос. техн. ун-та. , 2007. , № 1 (36). - с. 40-45.

[209] Перечень разрешенных к использованию в ГП "НАЭК "Энергоатом" расчетных кодов для обоснования безопасности ядерных установок по состоянию на 01 февраля 2018 г. (введено в дію розпорядженням ДП НАЕК "Енергоатом" №137-р від 05.02.2018 р.);

[210] Перспективы распараллеливания программ нейросетевого анализа и обработки данных / [В.Г. Царегородцев] // Материалы конф. «Математика, информатика, управление – 2008». – Иркутск, 2014. – С. 110-117.

[211] Писаренко Г. С. Сопротивление материалов: монография. 5-е изд. К.: Вища школа, 1986. 775 с.

[212] Підготовка докторів філософії (PhD) в умовах реформування вищої освіти: матеріали Всеукраїнської науково-практичної конференції (Запоріжжя, 5-6 жовтня 2017 р.). Запоріжжя: Запорізький національний університет, 2017. 216 с.

[213] Подгуренко В.С., Гетманец О.М., Терехов В.Е.. Повышение эффективности производства электроэнергии ветроэлектрической установкой на основе математического моделирования. Електрон. моделювання. 2020. Т.42, №2, с. 121 –127; doi:10.15407/emodel.42.02.121.

[214] Попов О.О. Математичне та комп'ютерне моделювання техногенних навантажень на атмосферу міста від стаціонарних точкових джерел забруднення [Текст] : автореф. дис. ... канд. техн. наук : 01.05.02 / О.О. Попов ; [Ін-т проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України]. – К., 2010. – 20 с.

[215] Попов, О. О., Яцишин, А. В., & Артемчук, В. О. (2014). Кількісний аналіз стану довкілля на техногенно забруднених територіях. Моделювання та інформаційні технології, (73), 3-16.

[216] Порядок купівлі гарантованим покупцем електричної енергії, виробленої з альтернативних джерел енергії. Постанова НКРЕКП 26 квітня 2019 року N 641 у редакції постанови НКРЕКП 13 грудня 2019 року N 2802.

[217] Постанова Кабінету Міністрів України від 5 червня 2019 р. № 483 в редакції постанови Кабінету Міністрів України від 9 грудня 2019 р. № 1003.

[218] Прийняття рішень оператором аеронавігаційної системи: монографія / В.П. Харченко, Т. Ф. Шмельова, Ю. В. Сікірда. – Кіровоград: КЛА НАУ, 2012. – 292 с.

[219] Применение IDS / IPS [Електронний ресурс] – https://xakep.ru/2012/10/29/ids-ips/

[220] Про затвердження Вимог з ядерної та радіаційної безпеки до інформаційних та керуючих систем, важливих для безпеки атомних станцій: наказ Державної інспекції ядерного регулювання від 22.07.2015 № 140, із змінами, внесеними згідно з Наказом Державної інспекції ядерного регулювання № 508 від 25.11.2019. URL: https://zakon.rada.gov.ua/laws/term/34229 (дата звернення: 26.03.2020).

[221] Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : постанова Кабінету міністрів України від 19.06.2019 № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF (дата звернення: 30.04.2020).

[222] Про основні засади забезпечення кібербезпеки України : Закон України від 08.07.2018 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 30.04.2020).

[223] Проект Закону про внесення змін до Податкового кодексу України щодо збільшення ставок екологічного податку та впровадження європейських принципів модернізації української промисловості № 2367-1 від 18.11.2019.

[224] Проект Закону про внесення змін до Податкового кодексу України щодо збільшення ставок екологічного податку з метою проведення додаткових заходів, що сприятимуть зміцненню здоров'я та покращенню медико-санітарного забезпечення громадян України № 2367 від 01.11.2019 р.

[225] Радиотехнические цепи и сигналі/ [И.С.Гоноровский] - М.: Радио и связь, 1986. – 512 с.

[226] Разработка систем цифровой обработки сигналов / [Д.С. Потехин, И.Е. Тарасов].– М.:Горячая Линия-Телеком, 2007.– 250 с.

[227] Результати аналізу порушень, які сталися протягом 2015 — першого півріччя 2016 років на АЕС України/ [С.В. Недбай, Д.В. Воронцов, О.М. Горпинченко, О.В. Печериця] - Ядерна та радіаційна безпека, 2016, Вип. 3(71). - с. 15-18.

[228] Рекомендації CERT-UA з безпеки вебресурсів. // CERT-UA. – URL: https://cert.gov.ua/recommendations/25

[229] С.В. Бушуев, А.Н. Попов Исследование точности измерений среднеквадратических значений электрических сигналов на ограниченных интервалах времени. Транспорт Урала №2(29)//2011 с. 46-50.

[230] С.В. Щербина, А.І. Фещенко, ОА. Владимирський, І.П. Криворучко, А.П. Іващенко, О.В. Адаменко. Сертифікована автоматизована цифрова система оцінки стану безпеки різних об'єктів. Моделювання та інформаційні технології. Вип. 86, Київ, 2019р.-с.36-41.

[231] Сетевая безопасность. Часть 2. Next-Generation Firewall [Електронний ресурс] – https://habr.com/ru/company/hpe/blog/262123.

[232] Симборський, А. І., & Станиціна, В. В. (2010). Потенціал енергозбереження у цементній промисловості. Проблеми загальної енергетики, (3), 25-29.

[233] Солоха М.А. Використання безпілотників при вирішенні екологічних задач / М.А. Солоха // Вісник ХНУ імені В.Н. Каразіна. Серія «Екологія». – 2013. – №1070. – Вип. 9. – С. 84-90.

[234] Спірін В.М. Якісні характеристики однофазного мостового випрямляча з активним навантаженням та ємнісним фільтром при живленні від джерела струму / Спірін В.М., Губаревич В.М., Маруня Ю.В., Салко С.В. // Технічна електродинаміка. 2020. Вип. 2. С. 23-27.

[235] Станиціна В.В. Артемчук В.О. Врахування екологічної складової у середній вартості теплової енергії за життєвий цикл. Зб. тез конференції «Безпека енергетики в епоху цифрової трансформації», м. Київ, 20 грудня 2019 р. ІПМЕ ім. Г.Є. Пухова НАН України. 2019. С. 86-89.

[236] Станиціна В.В. Визначення середньої вартості теплової енергії за життєвий цикл теплонасосної станції на артезіанських водах. Зб. тез XXXVII науково-технічної конференції молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України (2019). С.67-68.

[237] Станиціна, В. В. (2012). Врахування екологічних витрат при визначенні показників енергетичної ефективності та потенціалів енергозбереження в галузях та регіонах. Проблеми загальної енергетики, (1), 62-68.

[238] Стогній, О. В., Каплін, М. І., & Білан, Т. Р. (2012). Економіко-математична модель імпортування вугілля в Україну. Проблеми загальної енергетики, (1), 29-34.

[239] Стогній, О. В., Каплін, М. І., & Білан, Т. Р. (2012). Особливості моделі виробничого типу системи паливозабезпечення для розрахунку перспективних обсягів заміщення видів палива в економіці країни. Проблеми загальної енергетики, (3), 30-36.

[240] Стогній, О. В., Макаров, В. М., Каплін, М. І., & Білан, Т. Р. (2013). Визначення оптимальної марки вугілля ТЕЦ при переведенні їх котлоагрегатів на пиловугільне спалювання. Проблеми загальної енергетики, (1), 28-37.

[241] Тарасов В.И. Нелинейные методы минимизации для расчета установившихся режимов электроэнергетических систем. – Новосибирск: Наука, 2001. – 214 с.

[242] Теоретические основы радиотехники/ [Б.Р. Левин] – М.: Радио и связь, 1989– 656 с.

[243] Теоретичні та прикладні основи економічного, екологічного та технологічного функціонування об'єктів енергетики / [В.О. Артемчук, Т.Р. Білан, та ін.; за ред. А.О. Запорожця, Т.Р. Білан]. – Київ, 2017. – 312 с.

[244] Теория нейронных сетей. / [А.И. Галушкин] - М.: ИПРЖР, 2010. – 348 с.

[245] Теория упругости / [В.В.Новожилов]. – Ленинград, 1952. – 381 с.

[246] Технология Software Defined Radio/[А.Силин] - Беспроводные технологии, №2, 2007-22 с.

[247] Ткаченко В.В. / Основні аспекти кібербезпеки в Smart Grid системах: матеріали наук.-практ. конф. «Безпека енергетики в епоху цифрової трансформації» - Київ: Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національна академія наук України, 2019. – 21 с.

[248] Ткаченко В.В., Щебланін Ю.М. / Основні аспекти інформаційної безпеки в Smart Grid системах на основі стандартів ISO/IES 27001 та 27005: Сучасний захист інформації - № 3(39), 2019. - 36 - 41 с.

[249] Требования к содержанию отчета по анализу безопасности действующих на Украине энергоблоков АЭС с реакторами типа ВВЭР. Руководящий документ. Киев, 1995

[250] Феликсон Е. И. Упругие элементы приборов : монография. М.: Машиностроение, 1977. 311 с.

[251] Флеминг У., Ришел Р. Оптимальное управление детерминированными и стохастическими системами / У. Флеминг, Р. Ришел .-М.:Мир,1978.-312с.

[252] Холмский В.Г. Расчет и оптимизация режимов электрических сетей (специальные вопросы): учебное пособие для вузов / В. Г. Холмский. –М.: Высшая школа, 1975. –280 с.

[253] Цифровая обработка изображений / [Яне Б.] - М.: Техносфера, 2007. - 584 с.

[254] Черненко П.О., Мірошник В.О. Короткострокове прогнозування електричного навантаження електропостачальної компанії з використанням штучної нейронної мережі глибинного навчання. Праці інституту електродинаміки НАН України. 2018р. № 50. С. 5-11.

[255] Чим захищають сайти, або Навіщо потрібен WAF? [Електронний ресурс] – https://habr.com/ru/company/pt/blog/269165.

[256] Чио К., Фримен Д. Машинное обучение и безопасность / пер. с анг. А.В. Снастина. – М.: ДМК Пресс, 2020, 388 с.

[257] Электрические системы. Электрические сети: Учеб. для электро-энерг. спец. вузов / В.А. Веников, А.А. Глазунов, Л.А. Жуков и др.: Под ред. В.А. Веникова, В.А. Строева. – 2-е изд., перераб и доп. – М.: Высш. шк., 1998. – 511с.: ил.

[258] Яцишин А.В., Куцан Ю.Г., Артемчук В.О., Каменева І.П., Попов О.О., Ковач В.О. Принципи та методи управління екологічною безпекою на основі інтелектуального аналізу даних мережі моніторингу атмосферного повітря // Електронне моделювання. 2019. № 4(41). С. 85-101.

[259] Яцишин, А. В., Попов, О. О., & Артемчук, В. О. (2009). Комп’ютерні засоби прогнозування техногенних навантажень на атмосферу. Восточно-Европейский журнал передовых технологий, 5(2), 33-36.

[260] Яцишин, А. В., Попов, О. О., Ковач, В. О., & Артемчук, В. О. (2018). Методика навчання майбутніх фахівців у галузі екології методам і засобам екологічного моніторингу приземного шару атмосфери. Інформаційні технології і засоби навчання, (66,№ 4), 217-230.