ISSN 2219-9365
DOI: 10.31891/2219-9365

Міжнародний науково-технічний журнал

ВИМІРЮВАЛЬНА ТА ОБЧИСЛЮВАЛЬНА ТЕХНІКА В ТЕХНОЛОГІЧНИХ ПРОЦЕСАХ

2020, № 2

International scientific-technical journal

MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES

2020, Issue 2

Хмельницький 2020
Khmelnytskyi 2020

МІЖНАРОДНИЙ НАУКОВО-ТЕХНІЧНИЙ ЖУРНАЛ
ВИМІРЮВАЛЬНА ТА ОБЧИСЛЮВАЛЬНА ТЕХНІКА В ТЕХНОЛОГІЧНИХ ПРОЦЕСАХ

Затверджений як фахове видання (перереєстрація), група «Б»
Наказ МОН 28.12.2019 №1643

Засновано в травні 1997 р. ***Виходить 2 рази на рік***

Хмельницький, 2020, № 2 (66)

Засновник і видавець: **Хмельницький національний університет (до 2005 р. — Технологічний університет Поділля, м. Хмельницький)**

Наукова бібліотека України ім. В.І. Вернадського http://nbuv.gov.ua/j-tit/votт

Журнал включено до наукометричних баз:

Index Copernicus	http://jml2012.indexcopernicus.com/,p24781565,3.html h-індекс 49,97
Google Schoolar	http://scholar.google.com.ua/citations?user=nwN_nusAAAAJ&hl=uk - індекс 9
Національна бібліотека України ім. В.І. Вернадського	http://nbuv.gov.ua/j-tit/votт

Рекомендовано до друку рішенням Вченої ради Хмельницького національного університету, протокол № 5 від 26.11.2020

Адреса редакції: **Україна, 29016, м. Хмельницький, вул. Інститутська, 11, Хмельницький національний університет редакція журналу "Вимірювальна та обчислювальна техніка в технологічних процесах"**

☎ **067-347-74-57**

e-mail: **mscientificjournal@gmail.com**

web: **http://journals.khnu.km.ua/index.php/MeasComp**

Зареєстровано Міністерством України у справах преси та інформації.
Свідоцтво про державну реєстрацію друкованого засобу масової інформації
Серія КВ № 23279-13119ПР від 24 травня 2018 року (перереєстрація)

ЗМІСТ

МЕТРОЛОГІЯ, СТАНДАРТИЗАЦІЯ, СЕРТИФІКАЦІЯ ТА ВИМІРЮВАЛЬНА ТЕХНІКА В ТЕХНОЛОГІЧНИХ ПРОЦЕСАХ

ІНФОКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ, АВТОМАТИЗАЦІЯ ТА ОБЧИСЛЮВАЛЬНА ТЕХНІКА В ТЕХНОЛОГІЧНИХ ПРОЦЕСАХ

МЕТРОЛОГІЯ, СТАНДАРТИЗАЦІЯ, СЕРТИФІКАЦІЯ ТА ВИМІРЮВАЛЬНА ТЕХНІКА В ТЕХНОЛОГІЧНИХ ПРОЦЕСАХ

УДК 620.91
DOI: 10.31891/2219-9365-2020-66-2-1

СКИБА М. Є., МАРТИНЮК В. В.,
РАДЕЛЬЧУК Г. І., ТИМОЩУК Р. В.
Хмельницький національний університет

ПІДВИЩЕННЯ ДОСТОВІРНОСТІ АВТОМАТИЗОВАНОГО ДІАГНОСТУВАННЯ СТАНУ НАКОПИЧУВАЧІВ ЕЛЕКТРОЕНЕРГІЇ

У роботі запропонована автоматизована система діагностування стану накопичувачів електроенергії. Запропоновано підвищити достовірність діагностування стану накопичувачів електроенергії шляхом використання частотних та часових характеристик накопичувачів електроенергії. Встановлено, що достовірність процесу діагностування стану накопичувачів електроенергії буде максимальною, якщо математичні моделі перехідного опору та перехідної провідності накопичувачів електроенергії з високою описують їх виміряні характеристики перехідного опору та перехідної провідності.

Keywords: система діагностування стану накопичувачів електроенергії, частотні та часові характеристики, достовірність процесу діагностування стану накопичувачів електроенергії.

SKYBA M., MARTYNYUK V.,
RADELCHUK G., TYMOSCHUK R.
Khmelnitsky national university

INCREASING THE RELIABILITY OF AUTOMATED DIAGNOSIS OF ELECTRICITY ACCUMULATORS

Of all the secondary energy sources available for electric vehicles (EM), hybrid electric vehicles (GETs) and portable electronic devices such as smartphones and laptops, the use of lithium-ion (Li-ion) batteries is the most promising. Compared to other energy sources, lithium batteries have some unique advantages, for example, these batteries have a higher specific energy, have a minimal memory effect, provide the best ratio of energy to weight, and have a low self-discharge at idle.

The state of health (SOH) of electricity storage devices has recently become increasingly important, as electricity storage devices become obsolete over time and their parameters and characteristics deteriorate. The main consequences of the aging of electricity storage devices are a decrease over time in their capacity and an increase in their internal resistance.

Methods for diagnosing the level of charge and the level of efficiency of energy storage devices are similar. The difference between diagnosing the level of charge and diagnosing the level of efficiency of energy storage devices is that when the charge level decreases, it is necessary to react quickly and carry out the nucleation of the electrical energy storage device.

Instead, the process of aging (degradation) of drives is slower, but irreversible. The rate of aging (degradation) of electricity storage depends on various factors, such as operating conditions, charging and discharging modes, as well as the quality of electricity storage.

In the process of diagnosing the level of efficiency of electricity storage devices, measurements of capacity and active resistance of electricity storage losses are carried out. When building a system for diagnosing the condition of electricity storage, it is necessary to take into account the parameters that reflect their technical condition. The nominal indicators of the technical condition of electricity storage devices include their capacity C and active resistance R.

An automated system for diagnosing the state of electricity storage devices is proposed in the work. It is proposed to increase the reliability of diagnosing the state of electricity storage devices by using the frequency and time characteristics of electricity storage devices. It is established that the reliability of the process of diagnosing the state of electricity storage will be maximum if the mathematical models of transient resistance and transient conductivity of high energy storage describe their measured characteristics of transient resistance and transient conductivity.

Keywords: system for diagnosing the state of electric storage, frequency and time characteristics, the reliability of the process of diagnosing the state of electric storage.

Вступ. Серед усіх вторинних джерел енергії, доступних для електромобілів (ЕМ), гібридних електричних транспортних засобів (ГЕТЗ) та для портативних електронних пристроїв, таких як смартфони та ноутбуки, використання літій-іонних (Li-ion) батарей є найбільш перспективним. Порівняно з іншими варіантами джерел енергії, літієві батареї мають деякі унікальні переваги [1; 2], наприклад ці батареї мають вищу питому енергію, мають мінімальний ефект пам'яті, забезпечують найкраще співвідношення енергії до ваги, а також мають низький саморозряд при простої [3].

Рівень працездатності (англомовний термін state of health – SOH) накопичувачів електроенергії останнім часом стає все більш важливим, тому що накопичувачі електроенергії із часом старіють, а їх параметри і характеристики погіршуються. Основними наслідками старіння накопичувачів електроенергії є зменшення з часом їх ємності та зростання їх внутрішнього опору.

Методи діагностування рівня заряду та рівня працездатності накопичувачів електроенергії є подібними. Різниця між діагностуванням рівня заряду та діагностуванням рівня працездатності накопичувачів електроенергії полягає в тому, що при зменшенні рівня заряду необхідно швидко реагувати і здійснювати зароджування накопичувача електроенергії.

Натомість процес старіння (деградації) накопичувачів є більш повільним, але незворотнім. Швидкість старіння (деградації) накопичувачів електроенергії залежить від різних факторів, таких як умови експлуатації, режими заряджування та розряджування, а також якості накопичувачів електроенергії.

В процесі діагностування рівня працездатності накопичувачів електроенергії проводяться вимірювання ємності та активного опору втрат накопичувачів електроенергії. При побудові системи діагностування стану накопичувачів електроенергії необхідно враховувати параметри, які відображують їх технічний стан. До номінальних показників технічного стану накопичувачів електроенергії відноситься їх ємність C та активний опір R.

Загальна структурна схема автоматизованої системи діагностування стану накопичувачів електроенергії. В процесі діагностування стану накопичувачів електроенергії необхідно враховувати частотної дисперсію та не лінійність їх ємності $C(\omega, u)$ та активного опору $R(\omega, u)$. Загальна структурна схема системи діагностування стану накопичувачів електроенергії зображена на рис. 1.

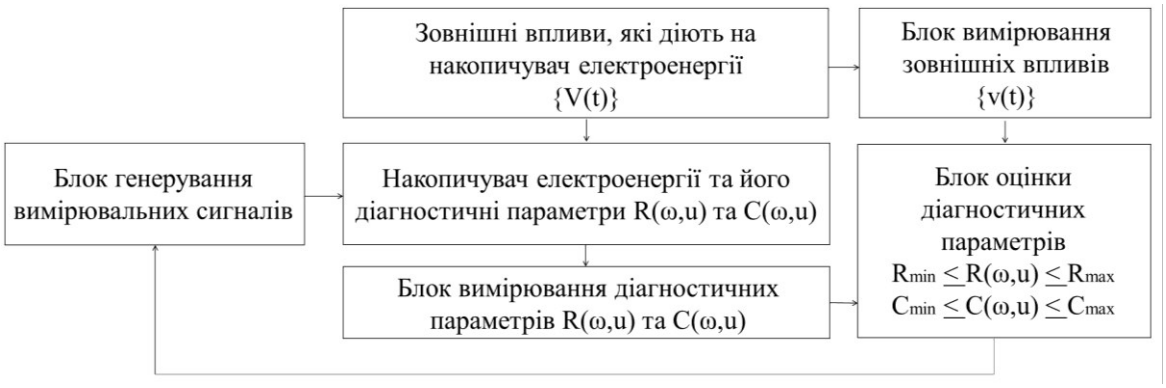


Рис. 1. Загальна структурна схема автоматизованої системи діагностування стану накопичувачів електроенергії

В процесі діагностування стану накопичувачів електроенергії блок генерування вимірювальних сигналів подає на накопичувач електроенергії вимірювальну напругу $u_в(t)$ або вимірювальний струм $i_в(t)$. Оточуюче середовище впливає на накопичувач електроенергії через зовнішні впливи $\{v(t)\}$.

Блок вимірювання діагностичних параметрів вимірює параметри накопичувача електроенергії ємності $c(\omega,u)$ та активного опору $r(\omega,u)$, відповідно. Блок вимірювання зовнішніх впливів, які діють на накопичувача електроенергії, вимірює множину зовнішніх впливів $\{v(t)\}$.

Виміряні діагностичні параметри накопичувача електроенергії $c(\omega, u)$ та $r(\omega, u)$ та множина зовнішніх впливів $\{v(t)\}$ поступають на блок оцінки діагностичних параметрів, який визначає оцінку Q (накопичувач електроенергії є справним або несправним). Процес діагностування стану накопичувачів електроенергії може відбуватись у стаціонарному режимі діагностування або у нестаціонарному режимі діагностування накопичувачів електроенергії.

Найпростіша математична модель процесу діагностування стану накопичувачів електроенергії у стаціонарному режимі діагностування побудована на вимірюванні ємності C та активного опору R накопичувача електроенергії один лише раз. В процесі діагностування стану накопичувачів електроенергії отримуємо вимірюванні ємності c та активного опору r.

В основі найпростішої математичної моделі процесу діагностування стану накопичувачів електроенергії лежить дві гіпотези.

1. Першою гіпотезою H_0 є гіпотеза, що в процесі діагностування стану накопичувачів електроенергії виявили його працездатний стан:

$$H_0: c \in [C_H, C_B] \cap r \in [R_H, R_B], \quad (1)$$

де C_H, C_B та R_H, R_B – нижня і верхня межі ємності та активного опору відповідно c і r.

2. Другою гіпотезою H_1 є гіпотеза, що в процесі діагностування стану накопичувачів електроенергії виявили його непрацездатний стан:

$$H_0: c \notin [C_H, C_B] \cap r \notin [R_H, R_B]. \quad (2)$$

Достовірність процесу діагностування стану накопичувачів електроенергії дорівнює добутку методичної достовірності процесу діагностування стану накопичувачів електроенергії на інструментальну достовірність процесу діагностування стану накопичувачів електроенергії.

Методична достовірність процесу діагностування стану накопичувачів електроенергії дорівнює відношенню кількості показників технічного стану, які визначаються в процесі діагностування стану накопичувачів електроенергії до загальної кількості показників діагностування стану накопичувачів електроенергії.

На основі аналізу найпростішої математичної моделі процесу діагностування технічного стану накопичувачів електроенергії у стаціонарному режимі можна зробити висновок, що вимірювання ємності C та активного опору R накопичувача електроенергії здійснюється один лише раз. Тому найпростішої математичної моделі процесу діагностування технічного стану накопичувачів електроенергії характеризується низькою методичною достовірністю діагностування. Низька методична достовірністю діагностування технічного стану накопичувачів електроенергії пояснюється зміною ємності $C \neq \text{const}$ та активного опору $R \neq \text{const}$ в процесі експлуатації накопичувачів електроенергії.

Для найпростішої математичної моделі процесу діагностування технічного стану накопичувачів електроенергії у стаціонарному режимі діагностування кількість показників дорівнює $N_1 = 2$ (ємність та активний опір).

В процесі експлуатації накопичувачів електроенергії частотна дисперсія та нелінійність ємності $C(\omega,u)$ та активного опору $R(\omega,u)$ накопичувачів електроенергії є аналогічним великій кількості параметрів, які характеризують технічний стан накопичувачів електроенергії.

В процесі діагностування стану накопичувачів електроенергії отримуємо $N \neq N_1$ і $N >> N_1$, тому методична достовірність діагностування стану накопичувачів електроенергії для найпростішої моделі діагностування стану накопичувачів електроенергії у стаціонарному режимі буде набагато меншою ніж одиниця:

$$D_M = \frac{2}{N} \ll 1. \tag{3}$$

До складу інструментальної достовірності діагностування стану накопичувачів електроенергії у стаціонарному режимі входить ймовірність помилки першого α, а також ймовірність помилки другого роду β. Вирази для визначення ймовірності помилки першого α та ймовірності помилки другого роду β описуються рівняннями (4) та (5). Необхідно відмітити, що ймовірності помилки першого α та ймовірності помилки другого роду β потрібно розраховувати для ємності C та активного опору R накопичувачів електроенергії:

$$\alpha_c = \int_{C_H}^{C_B} f(c)\left(\int_{-\infty}^{C_H - c} f(\delta_c)d\delta_c\right)dc + \int_{C_H}^{C_B} f(c)\left(\int_{C_B - c}^{\infty} f(\delta_c)d\delta_c\right)dc; \tag{4}$$

$$\beta_c = \int_{-\infty}^{C_H} f(c)\left(\int_{C_H - c}^{C_B - c} f(\delta_c)d\delta_c\right)dc + \int_{C_B}^{\infty} f(c)\left(\int_{C_H - I}^{C_B - I} f(\delta_c)d\delta_c\right)dc\ , \tag{5}$$

де C_B, C_H – верхня та нижня межі для ємності C накопичувачів електроенергії;

$f(c)$ – вираз щільності ймовірності для ємності C накопичувачів електроенергії;

$f(\delta_c)$ – вираз щільності ймовірності похибки вимірювання ємності C накопичувачів електроенергії.

Вирази для визначення ймовірності помилки першого α та ймовірності помилки другого роду β активного опору R накопичувачів електроенергії описуються рівняннями (6) та (7), відповідно:

$$\alpha_r = \int_{R_H}^{R_B} f(r)\left(\int_{-\infty}^{R_H - r} f(\delta_r)d\delta_r\right)dr + \int_{R_H}^{R_B} f(r)\left(\int_{R_B - r}^{\infty} f(\delta_r)d\delta_r\right)dr; \tag{6}$$

$$\beta_r = \int_{-\infty}^{R_H} f(r)\left(\int_{R_H - r}^{R_B - r} f(\delta_r)d\delta_r\right)dr + \int_{R_B}^{\infty} f(r)\left(\int_{R_H - r}^{R_B - r} f(\delta_r)d\delta_r\right)dr, \tag{7}$$

де R_B, R_H – верхня та нижня межі для активного опору R накопичувачів електроенергії;

$f(r)$ – вираз щільності ймовірності для активного опору R накопичувачів електроенергії;

$f(\delta_r)$ – вираз щільності ймовірності похибки вимірювання активного опору R накопичувачів електроенергії.

У процесі діагностування стану накопичувачів електроенергії отримуємо вираз загальної достовірності діагностування стану накопичувачів електроенергії у стаціонарному режимі, який записується у вигляді (8):

$$D_З = D_M \cdot D_I = \frac{2}{N} \cdot (1 - \alpha - \beta) \ll 1. \tag{8}$$

В процесі діагностування стану накопичувачів електроенергії оцінку якості діагностування стану накопичувачів електроенергії у стаціонарному режимі визначимо, використовуючи вираз середнього ризику діагностування стану накопичувачів електроенергії, який записується у вигляді (2.9):

$$\Psi \approx W_{1c}\alpha_c + W_{2c}\beta_c + W_{1r}\alpha_r + W_{2r}\beta_r, \quad (9)$$

де W_{1c}, та W_{1r} – коефіцієнти втрат, що виникають в процесі діагностування стану накопичувачів електроенергії та обумовлені помилками 1–го роду для ємності C та активного опору R накопичувачів електроенергії;

W_{2c}, та $W_{2к}$ – коефіцієнти втрат, що виникають в процесі діагностування стану накопичувачів електроенергії та обумовлені помилками 2-го роду для ємності C та активного опору R накопичувачів електроенергії;

α_c, та α_r – вирази імовірностей помилок 1-го роду для ємності C та активного опору R накопичувачів електроенергії;

β_c, та β_r – вирази імовірностей помилок 2-го роду для ємності C та активного опору R накопичувачів електроенергії;

Достовірність діагностування стану накопичувачів електроенергії можна підвищити, якщо використовувати їх частотні та часові характеристики.

Програмне забезпечення автоматизованої системи діагностування стану накопичувачів електроенергії. Програмне забезпечення автоматизованої системи діагностування стану накопичувачів електроенергії складається із трьох програм. Перша програма призначена для сигнального процесора. Стуктура програмного забезпечення автоматизованої системи діагностування стану накопичувачів електроенергії зображена на рис. 2. Програма для сигнального процесора виконує обробку даних, які отримуються від діагностуючих каналів у режимі реального часу.

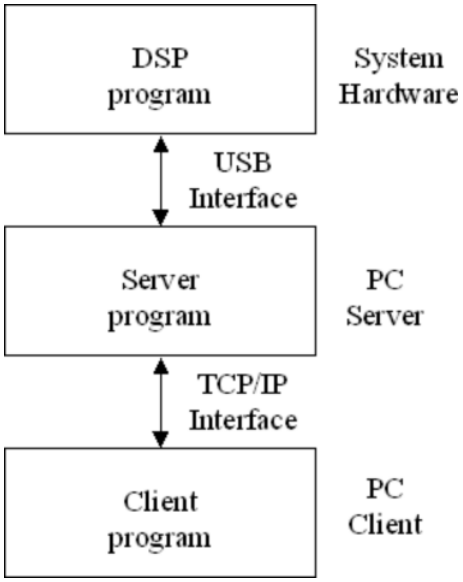


Рис. 2. Структура програмного забезпечення автоматизованої системи діагностування стану накопичувачів електроенергії

Друга програма виконує роль серверної програми. Ця програма дозволяє віддалене керування для багатьох користувачів через клієнтські програми, які здійснюють діагностування за допомогою незалежних каналів. Діагностуючі канали працюють незалежно і можуть керуватися за допомогою одного користувача.

Третя програма виконує роль клієнтської програми. Діагностування стану накопичувачів електроенергії виконується в автоматичному або в напівавтоматичному режимах. В автоматичному режимі модуль діагностуючих параметрів накопичувачів електроенергії виконує обробку даних без додаткових сигналів керування.

У напівавтоматичному режимі діагностування стану накопичувачів електроенергії програма здійснює цифрову обробку інформації під керівництвом оператора. Оператор системи може запускати або зупиняти незалежний діагностуючий канал.

У напівавтоматичному режимі можна перейти до наступного кроку програмного алгоритму процесу діагностування, використовуючи ручний режим роботи.

Висновки. В роботі запропоновано загальну структурну схема автоматизованої системи діагностування стану накопичувачів електроенергії, характеризується наступними перевагами:

а) в процесі діагностування стану накопичувачів електроенергії проводяться вимірювання ємності та активного опору втрат накопичувачів електроенергії;

б) діагностування стану накопичувачів електроенергії виконується в автоматичному або у напівавтоматичному режимах;

в) у автоматичному режимі модуль діагностуючих параметрів накопичувачів електроенергії виконує обробку даних без додаткових сигналів керування;

г) у напівавтоматичному режимі діагностування стану накопичувачів електроенергії програма здійснює цифрову обробку інформації під керівництвом оператора.

Література

1. B. Bilgin, P. Magne, P. Malysz, Y. Yang, V. Pantelic, M. Preindl, A. Korobkine, W. Jiang, S. Member, M. Lawford, S. Member, and A. Emadi, “Making the Case for Electrified Transportation,” IEEE Trans. Transp. Electrif., vol. 1, no. 1, pp. 4–17, 2015.

2. S. M. Lukic and A. Emadi, “Charging ahead,” IEEE Ind. Electron. Mag., vol. 2, no. 4, pp. 22–31, 2008.

3. J. Cao and A. Emadi, “Batteries need electronics,” Ind. Electron. Mag. IEEE, vol. 5, no. 1, pp. 27–35, 2011.

4. A. Emadi, “Transportation 2.0,” Power Energy Mag. IEEE, vol. 9, no. 4, pp. 18–29, 2011.

5. D. Fregosi, S. Bhattacharya, and S. Atcitty, “Empirical battery model characterizing a utility-scale carbon-enhanced VRLA battery,” 2011 IEEE Energy Convers. Congr. Expo., pp. 3541–3548, 2011.

6. X. Hu, S. Li, and H. Peng, “A comparative study of equivalent circuit models for Li-ion batteries,” J. Power Sources, vol. 198, pp. 359–367, 2012.

7. R. Ahmed, M. El Sayed, I. Arasaratnam, J. Tjong, and S. Habibi, “Reduced-Order Electrochemical Model Parameters Identification and SOC Estimation for Healthy and Aged Li-Ion Batteries. Part I: Parameterization Model Development for Healthy Batteryies,” IEEE J. Emerg. Sel. Top. Power Electron., vol. 2, no. 3, pp. 659–677, 2014.

8. W. Waag, C. Fleischer, and D. U. Sauer, “Critical review of the methods for monitoring of lithium-ion batteries in electric and hybrid vehicles”, J. Power Sources, vol. 258, pp. 321–339, 2014.

Надійшла / Paper received: 25.08.2020 Надрукована / Paper Printed : 01.12.2020

УДК 631.3.05
DOI: 10.31891/2219-9365-2020-66-2-2

КУЧЕРУК В. Ю., КУЛАКОВ П. І.
Вінницький національний технічний університет
ІВАНЕЦЬ О. Б.
Національний авіаційний університет
КУЛАКОВА А. П.
Вінницький національний технічний університет

ПІДХІД ДО КРИТЕРІАЛЬНОГО ОЦІНЮВАННЯ СТУПЕНЯ ВІДХИЛЕННЯ ВІД НОРМИ СТАНУ ОБ'ЄКТА

У статті наведено результати досліджень у галузі методів експерименту та запропоновано новий підхід до критеріального оцінювання ступеню відхилення від норми стану різнорідних об'єктів на основі результатів вимірювального контролю їх параметрів. Розроблений критерій може приймати значення в діапазоні від нуля до одиниці, чим більше чисельне значення критерію наближається до одиниці, тим менша ступінь відхилення стану об'єкта від норми. Наведено результати експериментальних досліджень та застосування запропонованої методики критеріального оцінювання. Результати досліджень, які наведено у статті, можуть бути використані для оцінювання ступеню відхилення від норми стану як технічних, так і біологічних об'єктів, у тому числі організму людей або тварин.

Ключові слова: критерій, вимірювальний контроль, оцінювання, контроль стану, ступінь відхилення.

KUCHERUK V., KULAKOV P.
Vinnytsia National Technical University
IVANETS O.
National Aviation University
KULAKOVA A.
Vinnytsia National Technical University

APPROACH TO CRITERION-BASED ASSESSMENT OF THE DEVIATION DEGREE OF THE OBJECTS FROM THE NORMAL STATE

Effective criteria-based assessment of the objects state and quality is important for various fields of industrie and science. The optimal quantitative indicator of the object state is the probability of a particular deviation type. Traditional methods of the probability determining of the presence of a particular type of deviation are an extremely difficult task that requires a very large amount of experimental research. Given the large number of industries in which criteria-based assessment of the objects state is used, an urgent task is to create a universal criterion suitable for use in various, even unrelated fields of science and technology, and relatively easy to use. The aim of the article is to develop the theory of criteria-based assessment, techniques and methods of experiment. As a result of the research, a new approach to criterial assessment of the various objects state was proposed, a universal criterion was developed for assessing the deviation degree from the norm of the objects state based on the measuring control results of their parameters. The convenience of using the developed criterion is ensured due to the fact that its numerical value is in the range from zero to one, and the smaller its numerical value, the greater the deviation degree of the object state from the norm. The results of experimental studies and the application of the proposed criteria-based assessment technique are presented. The effectiveness of using the developed approach to criteria-based assessment is confirmed by experimental results. The research results presented in the article can be used to assess the deviation degree from the norm of the state of both technical and biological objects, including the body of humans or animals.

Key words: measuring control, assessment, criterion, condition control, degree of deviation.

Вступ. Критеріальне оцінювання широко використовується у різних галузях науки і техніки для якісної та кількісної характеристики стану різноманітних об'єктів, як технічних, так і біологічних. Під час критеріального оцінювання стану складних об'єктів враховується значна кількість факторів впливу та показників стану, в тому числі результатів вимірювання та вимірювального контролю параметрів об'єктів. На основі теоретичних та експериментальних досліджень складних об'єктів встановлюються зв'язки між досліджуваним об'єктом і навколишнім середовищем, виявляються загальні закономірності, пояснюються, узагальнюються та формалізуються емпіричні закономірності. Враховуючи велику кількість галузей, у яких використовується критеріальне оцінювання стану об'єктів, важливим завданням є створення універсального критерію, придатного для використання у різних, навіть не споріднених галузях науки і техніки. Метою статті є розвиток теорії критеріального оцінювання, техніки та методів експерименту, розробка універсального критерію оцінювання ступеню відхилення від норми стану об'єкта та впровадження у практичне використання нових методів оперативного оцінювання стану різноманітних об'єктів.

Аналіз останніх досліджень та публікацій. Критеріальне оцінювання стану та якості об'єктів є важливим для різноманітних галузей промисловості та науки. У роботах [1, 2] розглянуто деякі критерії якості спеціалізованого програмного забезпечення, у роботі [3] розглянуто критерії, які характеризують

методики та якість навчання, певні методики критеріального оцінювання у галузі лінгвістики, медицини та соціальної інфраструктури розглянуто, відповідно, у роботах [4–6]. Деякі підходи до критеріального оцінювання стану механічних параметрів електричних машин розглянуто у [7], а певні підходи до критеріального оцінювання допустимого вмісту води у молоці та якості молока – в роботах [8–10]. У роботі [11] запропоновано універсальний критерій оцінювання ступеня відхилення від норми стану складових елементів технологічного процесу виробництва молока, який визначається на основі результатів вимірювального контролю його параметрів. Цей критерій має певну універсальність і може бути використаний для критеріального оцінювання стану інших різнорідних об'єктів. Недоліком цього критерію є незручність у використанні, тому що його значення змінюється в межах від певного мінімального значення до одиниці, а мінімальне значення залежить від коефіцієнтів кореляції між контрольованими параметрами об'єкта. Окрім того, наближення значення цього критерію до одиниці свідчить про збільшення ступеню відхилення стану об'єкта від норми, що на думку авторів, є незручним для сприйняття.

Постановка задачі. Для більшості варіантів відхилень стану складових елементів об'єкта оцінювання від норми можна виділити множину параметрів, значення яких, при наявності відхилення, не відповідає границям допуску. Оптимальним кількісним показником стану складових елементів об'єктів оцінювання є імовірність наявності того чи іншого варіанту відхилення. Теоретично, її можливо визначити на основі результатів встановлення відповідності значень параметрів об'єкта границям допуску, враховуючи їх взаємокорельованість, з використанням методів теорії імовірності. Але такий спосіб визначення імовірності являє собою надзвичайно складне завдання, яке потребує проведення дуже великої кількості експериментальних досліджень. Вирішити це завдання можна за допомогою універсального критерію оцінювання ступеня відхилення стану об'єкта від норми, який запропоновано у роботі [11], але цей критерій не є зручним для використання. Тому актуальним завданням є розробка універсального критерію оцінювання ступеню відхилення стану об'єкта від норми, зручного у використанні, чисельне значення якого знаходиться в діапазоні від нуля до одиниці і визначається на основі результатів вимірювального контролю параметрів об'єкта.

Вирішення поставленої задачі. Протягом функціонування практично будь-якого об'єкта виникають події, які негативно впливають на його ефективність. Результати вимірювального контролю параметрів об'єкта характеризують не тільки його стан в цілому, а і окремих складових елементів. Виходячи з цього, на основі результатів вимірювального контролю параметрів об'єкта можна здійснити оцінювання його стану в цілому, а також його окремих складових елементів, та виявити наявність певних подій, які негативно впливають на ефективність функціонування об'єкта. Основною ознакою виникнення певної події є негативний результат вимірювального контролю відповідного параметра об'єкта. Слід відзначити, що у багатьох випадках невідповідність значення певного параметра об'єкта межам допуску може виникнути внаслідок великої кількості різноманітних факторів, тобто ця обставина не гарантує наявності відповідної події. У багатьох випадках, відхилення стану об'єкта від норми, як правило, супроводжується одночасною зміною та знаходженням за межами допуску певної кількості його параметрів. Таким чином, у багатьох випадках, оцінити стан складових елементів об'єкта можливо на основі результатів вимірювального контролю декількох його параметрів.

Під контрольованим параметром першого рівня будемо розуміти такий параметр об'єкта, відхилення якого від норми є основною ознакою виникнення певного типу відхилення об'єкта від норми. Нехай для виявлення відхилення стану складового елементу об'єкта від норми здійснюється вимірювальний контроль N_K параметрів, які корельовані з контрольованим параметром першого рівня. Під контрольованим параметром другого рівня будемо розуміти той контрольований параметр, який має найбільше значення модуля коефіцієнту кореляції з контрольованим параметром першого рівня. Відповідно, під контрольованим параметром другого рівня, будемо розуміти той параметр, який має друге за величиною значення модуля коефіцієнту кореляції з контрольованим параметром першого рівня. Таким чином, контрольованим параметром *i*-го рівня є той контрольований параметр, який має *i*-те за величиною значення модуля коефіцієнту кореляції з контрольованим параметром першого рівня.

Позначимо через $P_{K1}, P_{K2} ... P_{Ki} ... P_{KN_K}$ – результати вимірювального контролю контрольованих параметрів $1,2...i...N_K$ рівня. Приймемо, що якщо значення контрольованого параметра *i*-го рівня не відповідає нормі, то $P_{Ki} = 1$, якщо відповідає нормі – $P_{Ki} = 0$.

Позначимо через $\rho_{K1}, \rho_{K2} ... \rho_{Ki} ... \rho_{KN_K}$ коефіцієнти кореляції між контрольованим параметром першого рівня та контрольованими параметрами $1,2...i...N_K$ рівня, які визначаються на основі серії експериментальних даних.

Розглянемо певний параметр K_{P0}, який визначається виразом:

$$K_{P0} = \frac{|\rho_{K1}| P_{K1} + |\rho_{K2}| P_{K2} + ... |\rho_{Ki}| P_{Ki} + ... + |\rho_{KN_K}| P_{KN_K}}{|\rho_{K1}| + |\rho_{K2}| + ... + |\rho_{Ki}| + |\rho_{KN_K}|}. \quad (1)$$

З урахуванням того, що оцінювати стан об'єкта на основі результатів вимірювального контролю його параметрів є сенс тільки тоді, коли $P_{K1}=1$, вираз (1) набуде вигляду:

$$K_{P0}=\frac{|\rho_{K1}|+\sum_{i=2}^{N_K}|\rho_{Ki}|P_{Ki}}{\sum_{i=1}^{N_K}|\rho_{Ki}|}. \tag{2}$$

Параметр K_{P0}, як слідує з виразу (2), може приймати значення в межах від мінімального значення K_{P0MIN} до одиниці, при умові, що $P_{K1}=1$. У цьому випадку мінімальне значення параметра K_{P0} визначається за виразом

$$K_{P0MIN}=\frac{|\rho_{K1}|}{\sum_{i=1}^{N_K}|\rho_{Ki}|}. \tag{3}$$

Теоретично, мінімальне значення параметра K_{P0MIN} може знаходитись в межах, які визначається співвідношенням:

$$K_{P0MIN}\in(0;1]. \tag{4}$$

З виразів (1) та (2) слідує, що чим більше значення параметра K_{P0} наближається до одиниці, тим більша імовірність наявності відхилення стану об'єкта від норми, тобто чисельне значення параметра K_{P0} певним чином характеризує стан об'єкта і може бути використано для критеріальної оцінки його стану. Але чисельне значення параметра K_{P0} у діапазоні $[K_{P0MIN};1]$ є незручним для сприйняття, більш інформативним є значення критерію, яке змінюється в діапазоні від нуля до одиниці, при умові, що наближення чисельного значення критерію до одиниці свідчить про зменшення ступеню відхилення стану об'єкта від норми.

Відповідно, з урахуванням того, що наближення чисельного значення критерію до одиниці повинно свідчити про зменшення ступеню відхилення стану об'єкта від норми, критерій оцінювання ступеню відхилення стану об'єкта від норми на основі результатів вимірювального контролю його параметрів пропонується визначати за виразом:

$$K_S=1-K_{P0}=1-\frac{\sum_{i=1}^{N_K}|\rho_{Ki}|P_{Ki}}{\sum_{i=1}^{N_K}|\rho_{Ki}|}. \tag{5}$$

Чисельне значення критерію K_S змінюється в межах від нуля до одиниці. Якщо чисельне значення K_S дорівнює одиниці, тобто $P_{K1},P_{K2}...P_{Ki}...P_{KN_K}=0$, це свідчить про повну відсутність будь-яких відхилень від норми. Чим вище значення критерію K_S, тим більше стан об'єкта наближений до нормального стану, і навпаки. Якщо чисельне значення критерію K_S дорівнює нулю, тобто $P_{K1},P_{K2}...P_{Ki}...P_{KN_K}=1$, це свідчить про те, що усі контрольовані параметри знаходяться за границями допуску і ступінь відхилення стану об'єкта від норми максимальна.

Від чисельного значення критерію залежить прийняття рішення стосовно дій, спрямованих на усунення подій, що спричинили відхилення стану. У випадку, якщо критерій оцінювання стану має значення наближене до нуля, то дії, спрямовані на усунення причин відхилення контрольованих параметрів від норми, треба провести негайно. Слід відзначити, що корельованість параметрів, які характеризують стан об'єкта, для різних варіантів відхилень від норми необхідно визначати окремо для кожного типу об'єктів. Ефективність використання запропонованого критерію зумовлена наочністю користування та простотою проведення розрахунків.

Експериментальне дослідження розробленого критерію проводилося авторами шляхом критеріального оцінювання ступеня відхилення від норми стану біологічного об'єкта - дійної тварини, у якій виявлено захворюваність маститом. При захворюваності тварини маститом, основною ознакою цієї події, при проведенні експрес-діагностики, є збільшення електропровідності молока вище межі допуску [12 - 14], тобто електропровідність молока, у даному випадку, є контрольованим параметром першого рівню. Із збільшенням електропровідності поступово зменшується разовий удій тварини, який у даному випадку є контрольованим параметром другого рівню. Внаслідок погіршення самопочуття тварини починає зменшуватись активність, яка є контрольованим параметром третього рівня, та збільшується температура тіла, яка є контрольованим параметром четвертого рівня. Типові експериментальні залежності зоотехнічних параметрів дійної тварини від дня спостереження при виникненні маститу наведено на рис. 1.

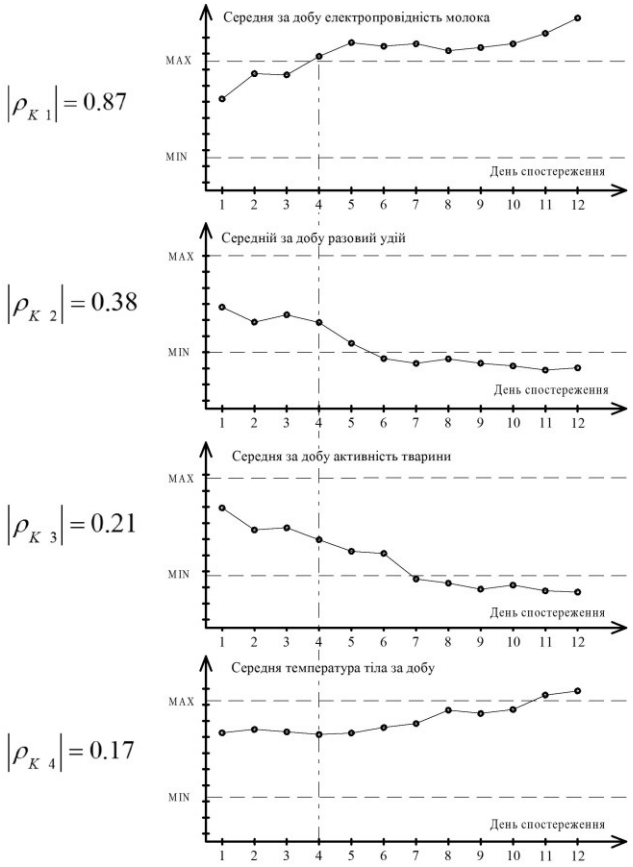


Рис. 1. Типові експериментальні залежності зоотехнічних параметрів тварини від дня спостереження при виникненні маститу

В результаті експериментальних досліджень, та відповідно до [12–14], встановлено значення коефіцієнтів кореляції між наявністю мастита та контрольованими параметрами першого, другого, третього та четвертого рівнів: $|\rho_{K1}| = 0{,}87$, $|\rho_{K2}| = 0{,}38$, $|\rho_{K\,3}| = 0{,}21$, $|\rho_{K4}| = 0{,}17$. Розраховане значення критерію ступеню відхилення від норми стану тварини, яка хвора на мастит, для кожного дня, протягом дванадцяти днів спостереження, наведено у таблиці 1. Як слідує з таблиці 1, протягом перших трьох днів спостереження усі контрольовані параметри, у тому числі і параметр першого рівню, були в границях допуску. Відповідно, чисельне значення критерію протягом цих днів дорівнювало одиниці. Протягом четвертого і п'ятого дня середня електропровідність молока (параметр першого рівня) збільшилася вище максимально допустимого значення, відповідно, чисельне значення критерію зменшилося до 0,47. На шостий день, внаслідок розвитку захворювання, середній за добу разовий удій тварини знизився нижче мінімального значення, відповідно, чисельне значення критерію зменшилося до 0,23. З сьомого по десятий день, у зв'язку з погіршенням стану тварини, її активність зменшилася нижче допустимого рівня, відповідно, чисельне значення критерію зменшилося до 0,10.

Таблиця 1

Значення критерію ступеню відхилення стану тварини захворілої маститом від норми протягом десяти днів спостереження

День спостереження	$P_{K\,1}$	$P_{K\,2}$	$P_{K\,3}$	$P_{K\,4}$	K_S
1	0	0	0	0	1
2	0	0	0	0	1
3	0	0	0	0	1
4	1	0	0	0	0.47
5	1	0	0	0	0.47
6	1	1	0	0	0.23
7	1	1	1	0	0.10
8	1	1	1	0	0.10
9	1	1	1	0	0.10
10	1	1	1	0	0.10
11	1	1	1	1	0
12	1	1	1	1	0

Протягом одинадцятого та дванадцятого дня спостереження, вище допустимого значення збільшилася температура тіла тварини. Відповідно, чисельне значення критерію зменшилося до нуля, тому як усі контрольовані параметри тварини не відповідають границям допуску. Нульове значення критерію свідчить про дуже високу імовірність того, що тварина хвора на мастит. Слід відзначити, що остаточний висновок про наявність маститу та його ступінь можна зробити тільки після проведення відповідних лабораторних досліджень молока та вимені тварини.

Більша частина експериментальних результатів була отримана за допомогою інформаційної системи для доїльної установки з молокопроводом «ІС-Молокопровід» [15], для розробки критерію ступеню відхилення стану від норми та розрахунку його чисельних значень використовувалося програмне забезпечення Maple V.

Слід відзначити, що розроблений критерій можна використовувати для оцінювання ступеня відхилення стану тварини від норми і при інших типах відхилень. Так, наприклад, збільшення температури тіла тварини вище верхньої границі допуску одночасно із збільшенням тривалості латентного періоду, збільшенням тривалості доїння, зменшення середньої інтенсивності молоковіддачі та інтенсивності молоковіддачі протягом першого, другого, та третього тридцятисекундного часового інтервалу після початку доїння, є певною ознакою наявності запалювального процесу або інфекційного захворювання. Збільшення тривалості латентного періоду та тривалості доїння одночасно із зменшенням середньої інтенсивності молоковіддачі та інтенсивності молоковіддачі протягом першого, другого, та третього тридцятисекундного часового інтервалу після початку доїння може бути ознакою неякісної підготовки тварини до доїння, або наявністю стресового стану, який може виникнути внаслідок великої кількості причин. Одночасне зменшення активності, румінації, разового удою та добового удою є ознакою наявності стресового стану або травмованості тварини.

Висновки. В результаті проведених досліджень розроблено універсальний критерій оцінювання ступеню відхилення від норми стану різноманітних об’єктів на основі результатів вимірювального контролю їх параметрів. Розроблений критерій зручний у використанні, його чисельне значення знаходиться в діапазоні від нуля до одиниці, чим вище його чисельне значення, тим більше стан об’єкта наближений до нормального. Ефективність використання розробленого критерію підтверджено результатами експериментальних досліджень. Результати досліджень, які наведено у статті, можуть бути використані для оцінювання ступеню відхилення від норми стану як технічних, так і біологічних об’єктів.

Література

1. A. Rawashdeh and B. Matalkah, “A new software quality model for evaluating COTS components,” Journal of Computer Science, vol. 2, pp. 373–381, 2006.

2. S. Liu and T. A. Moughal, “A novel method for dynamic multicriteria decision making with hybrid evaluation information,” Journal of Applied Mathematics, vol. 2014, Article ID 864628, 11 pages, 2014.

3. Sadler, D. Royce. "Interpretations of criteriabased assessment and grading in higher education." Assessment & evaluation in higher education 30.2 (2005): 175-194.

4. Van Trijp, R. (2013). Linguistic Assessment Criteria for Explaining Language Change: A Case Study on Syncretism in German Definite Articles, Language Dynamics and Change, 3(1), 105-132. doi: https://doi.org/10.1163/22105832-13030106

5. Rhodes V. A. Criteria for assessment of nausea, vomiting, and retching. Oncology Nursing Forum. 1997 Aug; 24 (7 Suppl): 13-19.

6. Sierra, Leonardo A., Víctor Yepes, and Eugenio Pellicer. "A review of multi-criteria assessment of the social sustainability of infrastructures." Journal of Cleaner Production 187 (2018): 496-513.

7. Vasilevskyi O. M., "Advanced mathematical model of measuring the starting torque motors," Tehnichna elektrodinamika 6, 76-81 (2013).

8. R. Tsenkova, S. Atanassova, K. Toyoda, Y. Ozaki, K. Itoh, T. Fearn, Near-Infrared Spectroscopy for Dairy Management: Measurement of Unhomogenized Milk Composition, Journal of Dairy Science, Volume 82, Issue 11, 1999, Pages 2344-2351, ISSN 0022-0302, https://doi.org/10.3168/jds.S0022-0302(99)75484-6.

9. Kucheruk, V. Mathematical model of the visible range optical radiation passing through a water-milk solution / V. Kucheruk, I. P. Kurytnik, P. Kulakov, A. N. Vasilevskyi, D. Zh. Karabekova, D. Mostovyi, A. Kulakova // Bulletin of the Karaganda University. «Physics» series., ISSN 2518-7198, № 1(89) / 2018, p. 24 – 31, URI: rep.ksu.kz/handle/data/2937

10. Volodymyr Kucheruk, Pavlo Kulakov, Oleksandr Vasilevskyi, Dmytro Mostovyi, Anna Kulakova, Iryna M. Kobylyanska, Gaini Karnakova, and Piotr Kisala “Optical method to determine the quantity of water in milk using the visible radiation range”, Proc. SPIE 10808, Photonics Applications in Astronomy, Communications, Industry, and High Energy Physics Experiments 2018, 108080Y (1 October 2018); https://doi.org/10.1117/12.2501605

11. Кулаков, П. І. Елементи теорії вимірювального контролю параметрів біотехнічної системи доїння / П. І. Кулаков. – Вінниця : ВНТУ, 2015. – 220 с. - ISBN 978-966-641-641-7.

12. Rasmussen, M. D. Detection and separation of abnormal milk in automatic milking systems / M. D. Rasmussen, A. Meijering, H. Hogeveen, C. J. A. M. de Koning // Automatic Milking – A Better Understanding. Wageningen Academic Publishers. –2004. – P. 189–197.

13. Chagunda, M. G. A model for detection of individual cow mastitis based on an indicator measured in milk / M. G. Chagunda, N. C. Friggens, M. D. Rasmussen, T. Larsen. // Journal of Dairy Science. – 2006. – V. 89. – P. 2980–2998.

14. Hamann, J. Diagnosis of mastitis and indicators of milk quality / J. Hamann, Krömker V. // Mastitis in Dairy Production: Current Knowledge and Future Solutions. – Wageningen Academic Publishers. – 2005. – P. 82–91.

15. Офіційний веб-сайт компанії «АГРО-ПРОМСЕРВІС». – [Електронний ресурс]. – Режим доступу: https://agropro/mservis.net.ua/.

References

1. A. Rawashdeh and B. Matalkah, “A new software quality model for evaluating COTS components,” Journal of Computer Science, vol. 2, pp. 373–381, 2006.

2. S. Liu and T. A. Moughal, “A novel method for dynamic multicriteria decision making with hybrid evaluation information,” Journal of Applied Mathematics, vol. 2014, Article ID 864628, 11 pages, 2014.

3. Sadler, D. Royce. "Interpretations of criteria-based assessment and grading in higher education." Assessment & evaluation in higher education 30.2 (2005): 175-194.

4. Van Trijp, R. (2013). Linguistic Assessment Criteria for Explaining Language Change: A Case Study on Syncretism in German Definite Articles, Language Dynamics and Change, 3(1), 105-132. doi: https://doi.org/10.1163/22105832-13030106

5. Rhodes V. A. Criteria for assessment of nausea, vomiting, and retching. Oncology Nursing Forum. 1997 Aug; 24 (7 Suppl): 13-19.

6. Sierra, Leonardo A., Víctor Yepes, and Eugenio Pellicer. "A review of multi-criteria assessment of the social sustainability of infrastructures." Journal of Cleaner Production 187 (2018): 496-513.

7. Vasilevskyi O. M., "Advanced mathematical model of measuring the starting torque motors," Tehnichna elektrodinamika 6, 76-81 (2013).

8. R. Tsenkova, S. Atanassova, K. Toyoda, Y. Ozaki, K. Itoh, T. Fearn, Near-Infrared Spectroscopy for Dairy Management: Measurement of Unhomogenized Milk Composition, Journal of Dairy Science, Volume 82, Issue 11, 1999, Pages 2344-2351, ISSN 0022-0302, https://doi.org/10.3168/jds.S0022-0302(99)75484-6.

9. Kucheruk, V. Mathematical model of the visible range optical radiation passing through a water-milk solution / V. Kucheruk, I. P. Kurytnik, P. Kulakov, A. N. Vasilevskyi, D. Zh. Karabekova, D. Mostovyi, A. Kulakova // Bulletin of the Karaganda University. «Physics» series., ISSN 2518-7198, № 1(89) / 2018, p. 24 – 31, URI: rep.ksu.kz/handle/data/2937

10. Volodymyr Kucheruk, Pavlo Kulakov, Oleksandr Vasilevskyi, Dmytro Mostovyi, Anna Kulakova, Iryna M. Kobylyanska, Gaini Karnakova, and Piotr Kisala “Optical method to determine the quantity of water in milk using the visible radiation range”, Proc. SPIE 10808, Photonics Applications in Astronomy, Communications, Industry, and High Energy Physics Experiments 2018, 108080Y (1 October 2018); https://doi.org/10.1117/12.2501605

11. Kulakov, P. I. Elementy teoriyi vymiryuvalnogo kontrolyu parametriv biotehnichnoyi systemy doyinnya / P. I. Kulakov. – Vinnytsia : VNTU, 2015. – 220 p. - ISBN 978-966-641-641-7.

12. Rasmussen, M. D. Detection and separation of abnormal milk in automatic milking systems / M. D. Rasmussen, A. Meijering, H. Hogeveen, C. J. A. M. de Koning // Automatic Milking – A Better Understanding. Wageningen Academic Publishers. –2004. – P. 189–197.

13. Chagunda, M. G. A model for detection of individual cow mastitis based on an indicator measured in milk / M. G. Chagunda, N. C. Friggens, M. D. Rasmussen, T. Larsen. // Journal of Dairy Science. – 2006. – V. 89. – P. 2980–2998.

14. Hamann, J. Diagnosis of mastitis and indicators of milk quality / J. Hamann, Krömker V. // Mastitis in Dairy Production: Current Knowledge and Future Solutions. – Wageningen Academic Publishers. – 2005. – P. 82–91.

15. Official web site of «AGRO-PROMSERVIS LTD». – [Electronic resource]. – Access mode: https://agropromservis.net.ua/.

Надійшла / Paper received: 17.09.2020 Надрукована / Paper Printed : 02.12.2020

УДК 519.25
DOI: 10.31891/2219-9365-2020-66-2-3

ГОРОШКО А. В., КОВТУН І. І., КРУШИНСЬКИЙ Д. О.
Хмельницький національний університет

РОЗРАХУНКОВО-ЕКСПЕРИМЕНТАЛЬНІ МЕТОДИ ОЦІНЮВАННЯ МІЦНОСТІ МЕТАЛОСКЛЯНИХ ВИРОБІВ РЕА

У статті представлені результати досліджень міцності склоспаїв у виробах електронної техніки. Проведено розрахунок допустиму розкиду фізико-механічних характеристик матеріалів вузла склоспаю, що забезпечують виконання умови міцності склоспая, і запропоновано здійснюючи вхідний контроль фізико-механічних характеристик використаних матеріалів з подальшим погодженням їх партій. Запропонована методика проектного розрахунку на міцність вузлів металоскляних фотодатчиків РЕА.

Ключові слова: склоспай, фотодатчик, міцність, електронні вироби.

GOROSHKO A., KOVTUN I., KRUSHYNSKYI D.
Khmelnytskyi National University

CALCULATION AND EXPERIMENTAL METHODS ASSESSING THE STRENGTH OF GLASS-TO-METAL PRODUCTS OF ELECTRONIC EQUIPMENT

The experience of using metal-glass electronics products indicates their low reliability due to mechanical destruction. As a rule, failure is caused by the insufficient ability of incandescent glass to wet the metal to form a tight bond, as well as by the inconsistent thermal expansion of glass and metal, which can cause a decrease in strength and depressurization of the seal when the assembly is cooled. The paper presents the results of studies of the strength of glass-sealed in electronic products. It is shown that the theory of thick-walled Lamé cylinders can be used for the calculation. The calculation of the permissible scatter of the physical and mechanical characteristics of the materials of the glass-weld assembly, ensuring the fulfillment of the strength condition of the glass-weld, was carried out, and it was proposed to carry out the incoming control of the physical and mechanical characteristics of the materials used with the subsequent approval of their batches. A method of design calculation for the strength of units of metal-glass photosensors of electronic equipment is proposed.

In, a new design and technological concept of sealing electronic modules in aluminum alloy housings using a multifunctional coating based on Ni and Si, obtained by pulsed laser surfacing. A formula for determining the mobility of surfacing of one layer, taking into account which find the total duration of laser surfacing and the formation of a multifunctional coating. In it is noted that indium and some of its alloys can be used as a solder capable of wetting glass, ceramics and metals and connecting them together. Indium has a low melting point and is very mild; softness allows it to plastically deform and absorb stress due to the mismatch of thermal expansion. Due to the very low pressure, indium vapor is used in glass-metal seals used in vacuum technology and cryogenic applications.

Keywords: Glass-to-metal seal, Photosensor, Strength, Electronic Products.

Постановка проблеми. Склоспаї (Glass-to-metal seal), які є герметичним щільним з’єднанням скла і металу, є важливим елементом конструкції вакуумних трубок, електричних розрядних трубок, ламп розжарювання, герметичних напівпровідникових діодів, герконів, герметичних скляних вікон в металевих корпусах і металевих або керамічних корпусів електронних компонентів. Досвід експлуатації виробів РЕА, виготовлених за технологією склоспаю показує, що значна частина з них виходить з ладу через механічне руйнування. Як правило, воно викликане недостатньою здатністю розпеченого скла змочувати метал для утворення щільного зв’язку, а також неузгодженим температурним розширенням скла і металу, що може викликати зниження міцності і розгерметизацію ущільнення при охолодженні складання.

Аналіз останніх досліджень і публікацій.

У роботі [1] розроблено нову конструкторсько-технологічну концепцію герметизації радіоелектронних модулів в корпусах з алюмінієвих сплавів з використанням багатофункціонального покриття на основі Ni і Si, що отримується імпульсною лазерною наплавкою. Отримано формулу для визначення рухливості наплавлення одного шару, з урахуванням якої знаходять загальну тривалість лазерного наплавлення і утворення багатофункціонального покриття. У роботі [2] відзначається, що індій і деякі його сплави можуть використовуватися в якості припою, здатного змочувати скло, кераміку і метали і з'єднувати їх разом. Індій має низьку температуру плавлення і дуже м'який; м'якість дозволяє йому пластично деформуватися і поглинати напруження через невідповідність теплового розширення. Через дуже низький тиск пара індій знаходить застосування в скло-металевих ущільненнях, що використовуються у вакуумній технології [3] і кріогенних застосуваннях [4].

Експериментально встановлено, що руйнування реальних матеріалів відбувається при навантаженнях в 10–100 разів менших, ніж передбачають теоретичні дані. На сьогодні різниця реальної міцності від теоретичної пояснюється за допомогою уявлення про існування різних типів дефектів [5]. Для зменшення концентрації напружень, створюваних дефектами, використовуються різні методи: травлення поверхні скла плавиковою кислотою, «зализування» поверхні скла за допомогою вогневого полірування тощо.

Виділення невирішених раніше частин загальної проблеми. У роботі [6] обґрунтована можливість використання теорії Ляме-Гадоліна для розрахунку напружень в електронних елементах, що мають форму тіл обертання, зокрема таких металоскляних виробів РЕА, як фотодатчики СФ-2-5, СФ-2-6, СФ-2-9, СФ-2-12, СФ-2-16, ФРЗ-11 (рис. 1). Ці фотодатчики (ФД) є мікроприладами РЕА, що змінюють свої електричні параметри в залежності від освітленості навколишнього середовища або певної інтенсивності світлового потоку, що реєструють наявність випромінювання певної довжини хвилі. Досвід виробництва і експлуатації ФД показав ненадійність конструкції через її недостатню міцність.

СФ-2-5 СФ-2-6 СФ-2-12 СФ-2-16 ФРЗ-11

Рис. 1. Фотодатчики типу СФ

У роботі представлені деякі результати проведених авторами досліджень, метою яких було оцінювання напружень, що виникають при виробництві і експлуатації ФД, вибір значення коефіцієнта запасу міцності і конструкторські і технологічні рекомендації щодо їх виробництва.

Результати досліджень. Розглянемо, наприклад, скляну деталь, що має форму тіла обертання, спаяну з іншою, наприклад, металевої деталлю, яка охоплює скляну. Введемо наступні припущення: не враховуємо напруження, що виникають внаслідок зміни розмірів при склованні, тобто усадку; закон Гука виконується; справедливою є гіпотеза плоских перерізів.

На рис. 2 представлений переріз вузла виведення через намистинковий склоспай. Скляний циліндр (середній) знаходиться під дією контактного тиску з боку оточуючих його металевих частин. В інших випадках, як наприклад, в діодах, можна вважати, що стінки циліндра знаходяться під дією контактного тиску з боку компаунду і газу, що знаходиться всередині виробу: компаундний циліндр знаходиться під впливом контактних тисків зі боку скляної частини і навколишнього середовища. Таким чином, для всіх випадків слід розглянути розрахунок тіла обертання, що знаходиться під дією контактних тисків по обидва боки.

Розглянемо загальний випадок навантаження циліндрів внутрішнім контактним тиском P_1 і зовнішнім – P_2. Позначимо r_1 і r_2 – внутрішній і зовнішній радіуси зовнішнього (металевого) циліндра. У тих випадках, коли задовільною є точність розрахунків 5–6 %, циліндр з відношенням $R_2 / r_2 > 4$ можна розглядати таким, що має нескінченно товсту стінку, при цьому величина контактного тиску q зростає, асимптотично наближаючись до деякого значення. Отже, при інженерних розрахунках можна розглядати навколишню деталь як циліндр з нескінченно великим радіусом.

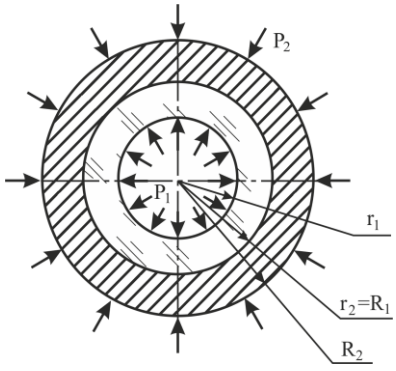


Рис. 2. Розрахункова схема типового вузла РЕА

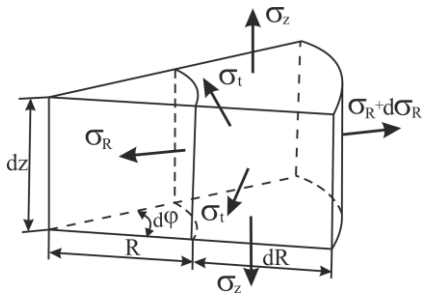


Рис. 3. Рівновага нескінченно малого елементу

Нехай зовнішній циліндр буде навантажений внутрішнім контактним тиском q (з боку деталі, яку він стискує) і зовнішнім P_2. Якщо розглянути рівновагу нескінченно малого елемента циліндра, утвореного двома поперечними площинами з відстанню dz між ними, двома осьовими площинами, з кутом $d\varphi$ між ними і двома циліндрами радіусів R и $(R+dR)$, то можна прийти до відомих формул Ляме:

– для зовнішнього металічного циліндра

$$U_M = \frac{1-2\mu_м}{E_м}\cdot\frac{R_1^2 q - R_2^2 P_2}{R_2^2 - R_1^2} R + \frac{1+\mu_м}{E_м}\cdot\frac{R_1^2 R_2^2 (q-P_2)}{R_2^2 - R_1^2}\frac{1}{R}, \quad (1)$$

$$\sigma_R = \frac{R_1^2 q - R_2^2 P_2}{R_2^2 - R_1^2} - \frac{R_1^2 R_2^2 (q-P_2)}{R_2^2 - R_1^2}\frac{1}{R^2}, \quad \sigma_t = \frac{R_1^2 q - R_2^2 P_2}{R_2^2 - R_1^2} + \frac{R_1^2 R_2^2 (q-P_2)}{R_2^2 - R_1^2}\frac{1}{R^2}, \quad \sigma_z = \frac{qR_1^2 - P_2 R_2^2}{R_2^2 - R_1^2}; \quad (2)$$

– для внутрішнього скляного циліндра

$$U_c = \frac{1-2\mu_c}{E_c}\cdot\frac{r_1^2 P_1 - r_2^2 q}{r_2^2 - r_1^2} r + \frac{1+\mu_c}{E_c}\cdot\frac{r_1^2 r_2^2 (P_1-q)}{r_2^2 - r_1^2}\cdot\frac{1}{r}, \quad (3)$$

$$\sigma_r = \frac{r_1^2 P_1 - r_2^2 q}{r_2^2 - r_1^2} - \frac{r_1^2 r_2^2 (P_1-q)}{r_2^2 - r_1^2}\cdot\frac{1}{r}, \quad \sigma_t = \frac{r_1^2 P_1 - r_2^2 q}{r_2^2 - r_1^2} + \frac{r_1^2 r_2^2 (P_1-q)}{r_2^2 - r_1^2}\cdot\frac{1}{r^2}, \quad \sigma_z = \frac{P_1 r_1^2 - q r_2^2}{r_2^2 - r_1^2}, \quad (4)$$

де σ_R – радіальне напруження; σ_t – тангенціальне напруження; σ_z – осьове напруження; $U_м$ – радіальне переміщення зовнішнього металічного циліндра; U_c – радіальне переміщення внутрішнього скляного циліндра.

Аналіз результатів розрахунків показав, що у розглянутих конструкціях значення як контактних тисків на границях матеріалів, так і напружень в елементах конструкції більші при використанні скла марки С48-2, ніж при використанні скла марки С52-1. Тому запас міцності елементів конструкції більше в останньому випадку.

Встановлено, що окружні напруження $\sigma_{t_{R_2}}$ в кришках ФД можуть перебувати в інтервалі, що охоплює значний діапазон величин в залежності від фізико-механічних характеристик сполучних матеріалів і законів зміни температури.

Для оцінювання температурних напружень по радіусу виробу використовувалися викладені у роботі [6] методики і математичні моделі. З їх використанням розрахували температурні поля при склоспаї вікончатого вузла кришок ФД на індукційній установці (рис. 2, 3). Результати розрахунків доводять, що при виготовленні намистинкових склоспаїв для зменшення внутрішніх напружень ефективніше використовувати скло марки С52-1 замість скла С48-2.

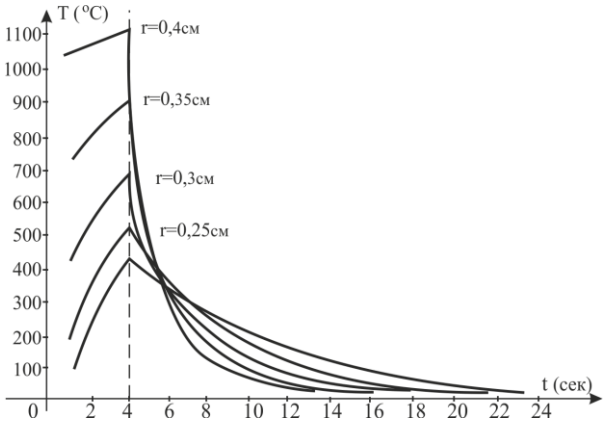


Рис. 2. Зміна температури по радіусу вікончатого склоспаю залежно від часу

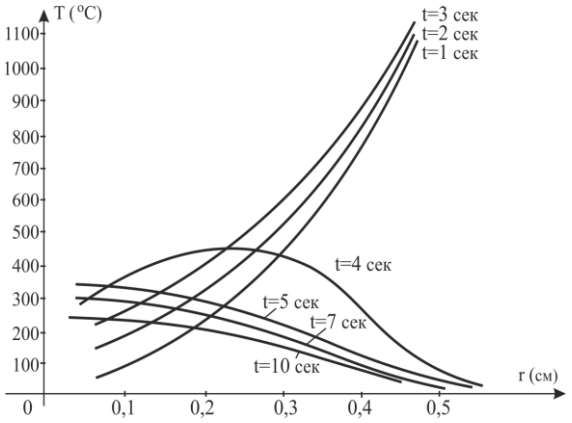


Рис. 3 Зміна температури по радіусу вікончатого склоспаю

Аналіз отриманих даних на рис. 2 і 3 показує, що за перші три секунди температура зовнішньої кромки скла, що з'єднується з металом, досягає 1000°С і відбувається розплав, в той час як в центрі температура не перевищує 200 °С. Після відключення індуктора (на четвертій секунді) видно хвильової процес поширення тепла від краю до центру і назад, що характеризується все ще досить великим градієнтом температур між центром скла і периферією. Необхідно звернути увагу на ту обставину, що при змінах радіусу на 1,5 мм перепад температури лежить в межах лише від 5 °С до 50 °С, що на порядок менше, ніж при зміні радіуса на 5 мм. Результати контрольних розрахунків для вікончатого скла ФД дають величини напружень $\sigma = (-509{,}6\ldots49)\cdot10^5$ Па, порівнюваних зі значеннями руйнівних напружень для скла С52-1. Якщо врахувати при цьому можливий розкид фізико-механічних характеристик (ФМХ) з'єднувальних матеріалів,

що призводить до збільшення напружень на 20–25 %, мікродефекти і концентратори напружень, то стає зрозумілим 86 % вихід бракованої продукції [6].

Звідси можна зробити практичний висновок: для вікончатого скла ФД, радіус яких сягає 4–5 мм, доцільно відмовитися від індукційного способу розігріву і віддати перевагу іншому, що забезпечує істотно менший перепад температур.

На підставі зазначених розрахунків заводу-виробнику ФД було рекомендовано змінити технологічний процес створення вікончатих склоспаїв таким чином, щоб зменшити градієнт температури по радіусу виробу. Для цієї мети на початку був використаний багатовитковий обертальний кондуктор, що дозволив дещо вирівняти температурне поле і це зменшило кількість дефектів на склі. Надалі операція склоспаювання здійснювалась з використанням графітових касет, які розміщені в муфельні печі, що дозволило збільшити кількість виробів, що проходять цю технологічну операцію одночасно, і домогтися ще більш рівномірного розподілу температури по радіусу ФД.

Як показують розрахункові дані, напруження в цьому випадку становлять: $\sigma = -47{,}4\cdot10^5$ Па. Економічний ефект від впровадження рекомендації по вирівнюванню температурного поля в процесі операції склоспаювання за рахунок використання муфельній печі і графітових касет склав більше мільйона гривень [6]. Для вузлів іншого класу, наприклад, намистинкових склоспаїв, у яких радіус знаходиться в межах 0,8–1,7 мм, причому розігрів йде як з внутрішньої, так і зовнішньої поверхні, індукційний спосіб розігріву є прийнятним.

Був проведений розрахунок допустиму розкиду ФМХ матеріалів, що використовуються при виготовленні ФД. Такими матеріалами є скло С52-1 і сплав ковар 29НК. Величини допустимих напружень приймалися наступними: на розтяг $[\sigma]_P = +98\cdot10^5$ Па, на стиск – $[\sigma]_{cm} = -441\cdot10^5$ Па. Розрахунок напружень проведено для випадку рівномірного розподілу перепаду температури по радіусу виробу: T = const = 20 °С. Результати розрахунків зведені в таблиці 1.

Таблиця 1.

Розкид фізико-механічних характеристик

ФМХ	Одиниця вимірювання	Існуючий розкид	Рекомендований розкид
α_c	град$^{-1}$	$(46–52)\cdot10^{-7}$	$(46–49)\cdot10^{-7}$
$\alpha_м$		$(46–48)\cdot10^{-7}$	$(46–47)\cdot10^{-7}$
E_c	Па	$(0{,}5–0{,}64)\cdot10^{11}$	$(0{,}53–0{,}59)\cdot10^{11}$
$E_м$		$(1{,}47–1{,}86)\cdot10^{11}$	$(1{,}47–1{,}7)\cdot10^{11}$
μ_c	–	0,24–0,26	0,25–0,26
$\mu_м$		0,28–0,32	0,29–0,31

Порівняння отриманих значень допустимого розкиду ФМХ, що забезпечують виконання умови міцності склоспая, з ДСТУ, показує, що отримані розрахунковим шляхом значення перекривають менші, у порівнянні з існуючими, діапазони значень. Отже, використання матеріалів з ФМХ, величина яких знаходиться в області значень, близькою до краю допуску, може призвести до виникнення у виробах руйнувальних напружень. Уникнути цього явища можна, наприклад, здійснюючи вхідний контроль ФМХ використаних матеріалів з подальшим погодженням їх партій.

У результаті проведених досліджень була розроблена методика проектного розрахунку на міцність вузлів металоскляних фотодатчиків РЕА, що герметизується компаундами. Методика може бути практично використана конструкторами і технологами. Методика передбачає:

– розрахунок розподілу температури;

– розрахунок температурних напружень для отриманого закону або по одному зі спрощених законів;

– розрахунок контактних тисків і сумарних напружень з урахуванням одночасного впливу тиску і температури;

– визначення напружень, які виникають від експлуатаційних навантажень;

– пошук сумарних напружень в небезпечній точці;

– визначення граничних напружень з урахуванням стану поверхні скла;

– отримання умови міцності.

Висновки та перспективи подальшого розвитку в цьому напрямі. Отримані результати у вигляді практичних конструкторських і технологічних рекомендацій і методик можуть використовуватися при виробництві металоскляних виробів РЕА, що дасть змогу підвищити міцність склоспаїв і підвищити надійність РЕА.

Література

1. Замирец Н. В. и др. Конструкторско технологическая концепция механизма образования лазерного сварного соединения в узлах герметизации радиоэлектронных модулей для изделий космической и специальной техники //Восточно-Европейский журнал передовых технологий. – 2003. – №. 2. – С. 34-41

2. Richard B. Belser (1954). "A Technique of Soldering to Thin Metal Films". Rev. Sci. Instrum. 25 (2): 180–183. doi:10.1063/1.1771017

3. Weissler, G. L., and Robert Warner Carlson. Vacuum physics and technology. Academic Press, 1980.

4. Döge, Stefan, and Jürgen Hingerl. "A hydrogen leak-tight, transparent cryogenic sample container for ultracold-neutron transmission measurements." Review of Scientific Instruments 89.3 (2018): 033903.

5. Abedi, Reza, Robert B. Haber, and Philip L. Clarke. "Effect of random defects on dynamic fracture in quasi-brittle materials." International Journal of Fracture 208.1-2 (2017): 241-268.

6. Механика в электронике. Монография: [в 3 т.] Т. 1: Статическая прочность / Ройзман В. П. - Хмельницкий : ХНУ – 2015. - 313 с

References

1. Zamirets N. V. i dr. Konstruktorsko tekhnologicheskaya kontseptsiya mekhanizma obrazovaniya lazernogo svarnogo soyedineniya v uzlakh germetizatsii radioelektronnykh moduley dlya izdeliy kosmicheskoy i spetsial'noy tekhniki //Vostochno-Yevropeyskiy zhurnal peredovykh tekhnologiy. – 2003. – №. 2. – S. 34-41

2. Richard B. Belser (1954). "A Technique of Soldering to Thin Metal Films". Rev. Sci. Instrum. 25 (2): 180–183. doi:10.1063/1.1771017

3. Weissler, G. L., and Robert Warner Carlson. Vacuum physics and technology. Academic Press, 1980.

4. Döge, Stefan, and Jürgen Hingerl. "A hydrogen leak-tight, transparent cryogenic sample container for ultracold-neutron transmission measurements." Review of Scientific Instruments 89.3 (2018): 033903.

5. Abedi, Reza, Robert B. Haber, and Philip L. Clarke. "Effect of random defects on dynamic fracture in quasi-brittle materials. "International Journal of Fracture 208.1-2 (2017): 241-268.

6. Mekhanika v elektronike. Monografiya: [v 3 t.] T. 1: Staticheskaya prochnost' / Royzman V. P. Khmel'nitskiy : KHNU – 2015. 313 s

Надійшла / Paper received: 28.10.2020 Надрукована / Paper Printed : 01.12.2020

УДК 631.3.05
DOI: 10.31891/2219-9365-2020-66-2-4

ІВАНЕЦЬ О. Б., МЕЛЬНИКОВ О. В.,
АРХИРЕЙ М. В., ЯКИМЕЦЬ І. В.
Національний авіаційний університет

МОДЕЛЬ ПРИЙНЯТТЯ РІШЕНЬ ЩОДО ФУНКЦІОНАЛЬНОГО СТАНУ СКЛАДНИХ ОБ"ЄКТІВ

У статті наведено результати досліджень у галузі методів експерименту та запропоновано новий підхід до оцінювання функціонального стану складних об'єктів на основі обробки результатів вимірювального контролю їх параметрів. В роботі запропонована формалізація процесу прийняття рішення при оцінюванні функціонального стану, такого складного об'єкту як організм людини, з використання статистичного методу. Запропонована можливість оцінювання стану організму, як багато параметричної системи при кореляції її показників, використання Т2 – статистика Хотелінга, яка дозволяє за рахунок визначення індивідуальних особливостей перетворення інформативних параметрів, надавати більш достовірні результати про зміну стабільності організму порівняно з традиційним підходом визначення норми з урахуванням тільки статі та віку. Проведені розрахунки медичних показників 12 операторів, що виконують професійні обов'язки, у яких проведені дослідження аналізу крові впродовж одного року. Наведені особливості використання персоналізованої медицини в рамках «концепції ЗП». Та запропоновано використання Т2 – статистики Хотелінга, що дає змогу визначати границі контрольованих значень на заданому рівні значущості за таблицею квантилів розподілу хи-квадрат.

Ключові слова: багато параметрична система, кореляція показників, статистичні методи, критерії оцінювання, медичні показники.

IVANETS O., MELNIKOV O.,
ARKHYREI M., YAKIMETS I.
National Aviation University

DECISION-MAKING MODEL ON THE FUNCTIONAL STATE OF COMPLEX OBJECT

Effective assessment of the condition of complex objects is important for various industries and science. Almost all characteristics of a biological object are characterized by variability - a specific and distinctive feature of all biomedical measurements. Variation of the trait occurs if its values vary from individual to individual or for one individual over time, which makes it impossible to repeat control measurements of the parameters of the same biological object, as is usually accepted in the art, which leads to great difficulties in estimating random variables. measurement and, as a consequence, diagnostic errors. The aim of the work is to formalize the decision-making process in assessing the functional state, such a complex object as the human body, using a statistical method. The possibility of estimating the state of the organism as a lot of parametric system in the correlation of its indicators, the use of T2 – Hotelling statistics, which allows by determining the individual characteristics of the transformation of informative parameters, to provide more reliable results on changes in body stability compared to the traditional approach and age. The effectiveness of using the developed approach to assessing the state of the organism is confirmed by experimental results. The results of the research presented in the article can be used to assess the degree of deviation from the norm of both technical and biological objects, including the body of humans or animals.

The article presents the results of research in the field of experimental methods and proposes a new approach to assessing the functional state of complex objects based on the processing of the results of measuring control of their parameters. The paper proposes the formalization of the decision-making process in assessing the functional state, such a complex object as the human body, using a statistical method. The possibility of estimating the state of the organism as a lot of parametric system in the correlation of its indicators, the use of T2 – Hotelling statistics, which allows by determining the individual characteristics of the transformation of informative parameters, to provide more reliable results on changes in body stability compared to the traditional approach and age. Medical indicators of 12 operators performing professional duties, in which blood tests were performed during one year, were calculated. Peculiarities of using personalized medicine within the framework of the "3P concept" are given. However, the use of T2 – Hotelling statistics is proposed, which makes it possible to determine the limits of controlled values at a given level of significance according to the chi-square distribution quantile table.

Key words: multi-parametric system, correlation of indicators, statistical methods, evaluation criteria, medical indicators.

Вступ. В останні десятиріччя технічні методи та засоби оцінювання складних об'єктів все більше впроваджуються в галузі економіки, біології, медицини екології та інших. Необхідність побудови функціональних моделей для опису структур складних об'єктів є актуальною задачею, яка дозволяє вирішувати питання оцінювання як поточного стану даних систем так і прогнозувати їхній стан при зміні факторів впливу. При визначенні функціонального стану такого складного об'єкту як організм людини необхідно провести аналіз всіх етапів прийняття рішень щодо його оцінювання. Розробка функціональної моделі прийняття рішень для оцінювання стану організму надасть змогу забезпечити повноту отримання інформації про параметри об'єкта, що контролюються. Первинна інформація після перетворення набуває форми кількісних суджень про стан об'єкта. Але обов'язковою умовою є операція порівняння зі значеннями норми. На сьогодні при прийнятті рішень щодо стану біологічних об'єктів такою нормою є референтні

значення які характеризуються достатньо широким діапазоном та не враховують унікальні особливості як самого організму та його адаптації та реакцій на зовнішні умови перебування.

Аналіз останніх досліджень та публікацій. Оцінювання складних об'єктів є важливим питанням для різноманітних галузей промисловості та науки. У роботах [1–3] розглянуто певні методики оцінювання у галузі лінгвістики, медицини та соціальної інфраструктури. розглянуто, а певні підходи до критеріального оцінювання біологічних об'єктів запропоновані – в роботах [4, 5]. Оцінювання та прогнозування різних функціональних станів організму людини розглянуті у роботах [6, 7]. Але майже всім характеристикам біологічного об'єкта притаманна варіабельність – специфічна і відмінна ознака всіх біомедичних вимірювань. Варіація ознаки виникає, якщо її значення змінюються від індивідууму до індивідууму або для одного індивідуума в часі. Майже завжди унеможливлюється проведення повторних контрольних вимірювань параметрів того самого біологічного об'єкту, як це прийнято зазвичай в техніці, що призводить до великих труднощів в оцінці випадкових величин при вимірюванні і, як наслідок, помилок діагностування. Мінливість та індивідуальний розкид параметрів біологічного об'єкту, їх взаємозв'язок, нелінійність цих зв'язків, наявність високого рівня перешкод, робить завдання об'єктивної оцінки стану біологічного об'єкту досить складним. У біологічному експерименті немає поняття «істинного значення», тільки середнє, а розкид даних, внаслідок індивідуальної реакції організму, може сильно варіювати.

Постановка задачі. Біологічний об'єкт як особливий об'єкт досліджень описується комплексом медико-біологічних показників – групами фізичних, біохімічних, психологічних параметрів, що визначаються в процесі досліджень [8, 9]. Через недостатню вивченість біологічного об'єкту ускладнено отримання адекватних математичних моделей між реєстрованими параметрами і відповідними їм біологічними показниками, що характеризують часово-просторовий стан біологічного об'єкта [10, 11]. Тому в роботі пропонується підхід який дозволяє при прийняття діагностичних рішень враховувати індивідуальні особливості меж норми для кожного окремого об'єкту на основі його ретроспективних даних.

Вирішення поставленої задачі. В роботі запропоновано представити складний об'єкт (наприклад організм людини), що характеризується параметром Y а $X_1,..X_k$ – вимірювальні величини (величини що контролюються) які відображають властивості об'єкта. Y – випадкова величина в тому сенсі що відсутня можливість точного обґрунтованого метрологічного відтворення будь-якого заданого значення в діапазоні Ау усіх її можливих змін. Але дисперсія величини Y в будь-якій точці діапазону кінцева та постійна $\sigma_y^2 = const$, а для математичних очікувань Y та $\{X_i\}_l^k$ існує функціональна, але апріорі невідома залежність:

$$M[Y] = F(M[X_1], \dots M[X_k]).$$

Узагальнена структурна схема отримання і перетворення вимірювальної інформації про значення показників системи організму за результатами вимірювального контролю його показників подана на рис.1 [12].

В якості первинної вимірювальної інформації про стан об'єкту обрані значення показників крові, а саме: значення параметрів лейкоцитів, еритроцитів та гемоглобіну Блок В (вимірювання) здійснює перетворення виміряних значень $X_1^*,..X_k^*$ контрольованих величин, а саме, X_1 – кількість лейкоцитів, X_2 – кількість еритроцитів, X_3 – кількість гемоглобіну, в оцінку Y^* значення параметра Y математичної моделі перетворення $M[Y] = F(M[X_1], \dots M[X_k])$.

Блок П (прийняття рішень) здійснює вибір $\{a_l, b_c\}_1^m$ одного $y_j\{a_l, b_c\}_1^m$ із багатьох $\{y_l\}_1^m$ рішень про значення Y (рис. 2), після порівняння Y^* з нормою $(a_l, b_l), l = \overline{1, m}$ відповідно до правила вибору рішення $\forall Y^*[Y^* \in (a_i, b_i) \rightarrow Y^* \in Y_i]$.

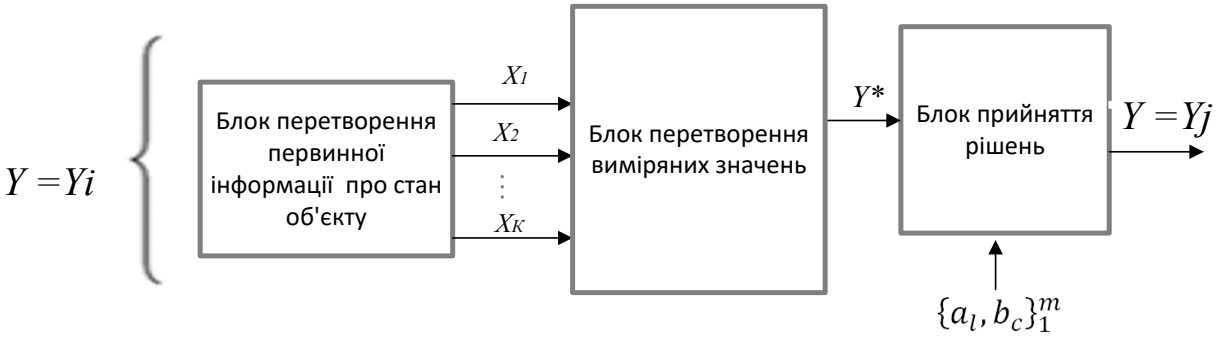


Рис. 1. Структурна схема інформаційної перетворень в системі прийняття рішень

Особливістю підходу запропонованого в даній роботі є визначення індивідуального підходу при формуванні значень норми. Це пов'язано з унікальними особливостями кожного окремого організму, який підтримує стійкість свого функціонування з огляду на фактори дестабілізації: кліматичні, соціальні,

демографічні, екологічні, спадкові та хронічні хвороби, шкідливі звички. В той час як традиційний підхід формує межі референтної норми для даних показників згідно доволі широких границь вікового ранжування та статі, так, наприклад, норми для значень лейкоцитів для дорослого чоловіка тільки 2 (табл. 1).

Таблиця 1.

Референтні значення згідно традиційного підходу оцінювання

Вік	Стать	Еритроцити, *10^12/л	Гемоглобін, г/л	Лейкоцити, *10^9/л
18–45 років	Чоловіча	4,3–5,7	132–173	4–5
	Жіноча	3,8–5,1	117–155	4–9
45–65 років	Чоловіча	4,2–5,6	131–172	3–9
	Жіноча	3,8–5,3	117–160	3,3–8,8
> 65 років	Чоловіча	3,8–5,8	126–174	3–9
	Жіноча	3,8–5,2	117–161	3,1–7,58

Якщо визначення оцінки кількості інформації про параметр *Y*, вважаючи, що ширина Δ допускових інтервалів $(a_i, b_i), j = \overline{1,k}$ однакова [13], а загальна кількість дорівнює *k*. В такому вигляді кількість інформації визначається різницею вихідної H(Y) і умовної $H(Y \mid Y_j)$ ентропії $I = H(Y) - H(Y \mid Y_j)$,

$$\text{де, } H(Y) = -\sum_{j=1}^{k}\left[\int_{a_j}^{b_j} f(y)dy\right]\ln\left[\int_{a_j}^{b_j} f(y)dy\right];$$

де *f*(*y*) – щільність розподілу величини Y в діапазоні Ay.

Умовну ентропію може бути знайдена через умовну ймовірність $P(Y_i \mid Y_j)$ того, що істинне значення $M[Y] = Y_j$, в той час як результат контролю (рішення y_j) дав значення $Y = Y_j$:

$$H(Y|Y_j) = -\sum_{i=1}^{k} P(Y_i|Y_j)\ln P(Y_i|Y_j).$$

При рівноймовірному розподілі значень Y1,…Yк і нормальному закону розподілу відхилення Y^* від дійсного значення M[Y]= const , якщо дисперсія цього відхилення дорівнює σ_y^2 маємо:

$$H(Y) = \ln\frac{A_y}{\Lambda};$$

$$H(Y|Y_j) = \ln\frac{\sigma_y\sqrt{2\pi e}}{\Delta}$$

Оцінка кількості інформації, з врахуванням двох останніх виразів, має вигляд:

$$I = \ln\frac{A_y}{\sigma_y\sqrt{2\pi e}}$$

Вираз можна розглядати, як кількість очікуваної вимірюваної інформації про функціональний стан організму Y при дисперсії σ_X^2 вхідних вимірюваних величин $X_1,\ldots X_к$ [12]. В якості вимірюваної первинної інформації про такий складний об'єкт як організм людини обрані контрольовані показники аналізу крові. Але традиційний підхід визначення допускових інтервалів на основі прийняти значень норми для відповідної групи згідно віку, статі та антропометричних особливостей знаходиться в протиріччі з новим курсом прийнятим галуззю охорони здоров'я так званою «концепцією 3П». Предиктивна медицини в якості раннього виявлення спадкової схильності людини до захворювань, що може дозволити своєчасно проводити профілактичні заходи для попередження їх розвитку, поліпшити стан здоров'я, підвищити якість і збільшити тривалість активного періоду життя. Превентивна медицина як особливий аспект медицини профілактичної, принципами якої є не пасивне очікування хвороби, а проведення застережливих і коригуючих заходів задовго до розвитку хвороби. Ця медицина орієнтована, насамперед, на підтримку здоров'я, поліпшення його якості, на попередження процесів передчасного старіння організму. Та нарешті персоналізована медицина є спробою перейти від наукових досліджень і терапевтичної практики, в значній мірі орієнтованих на середньостатистичного пацієнта, до досліджень і практики, які були б чутливими до унікальних біологічних і особистісних особливостей конкретного пацієнта. Але на сьогодні не існую

формалізованих методів для визначення таких «персоналізованих норм» тобто допускових інтервалів. Тому в якості прикладу в роботі запропоновано використання T^2 – статистики Хотелінга для контролю стабільності функціонального стану організму на основі синтезу інформаційних показників аналізу крові. Були визначені показники аналізу крові 12 дорослих чоловіків, що виконують професійні обов'язки операторів зібраних впродовж року. В якості показників обрані значення кількості гемоглобіну, еритроцитів, лейкоцитів в крові операторів, що діагностуються. Для проведення розрахунків була використана T^2 – статистика Хотелінга яка дозволяє виявити, які саме показники або їх поєднання, можуть вказати на порушення в організмі.

Для використання T^2 – статистика Хотелінга в одновимірному випадку за вибіркою обсягом n при відомій дисперсії генеральної сукупності використовується статистика:

$$z = \frac{\left(\bar{x} - \mu_0\right)}{\sigma/\sqrt{n}}. \tag{1}$$

При розгляді багатовимірної випадкової величини, якщо звести ліву і праву частини виразу (1) до другого степеня, отримаємо вираз:

$$z^2 = n\left(\bar{x} - \mu_0\right)^2 \left(\sigma\right)^{-1}, \tag{2}$$

яке в матричної формі можна представити як:

$$T_H^2 = n\left(\bar{\boldsymbol{X}} - \boldsymbol{\mu_0}\right)^T \boldsymbol{\Sigma^{-1}} \left(\bar{\boldsymbol{X}} - \boldsymbol{\mu_0}\right). \tag{3}$$

Отриманий вираз є узагальненою характеристикою Хотелінга (T^2-статистика Хотелінга), яка застосовується при оцінюванні якості багатопараметричного контролю при наявності кореляції його показників [14].

Багатовимірної випадкової величини відповідає коваріаційна матриця:

$$\boldsymbol{\Sigma} = \begin{vmatrix} \sigma_1^2 & \rho_{12}\sigma_1\sigma_2 & \dots & \rho_{1p}\sigma_1\sigma_p \\ \rho_{21}\sigma_2\sigma_1 & \sigma_2^2 & \dots & \rho_{2p}\sigma_2\sigma_p \\ \dots & \dots & \dots & \dots \\ \rho_{p1}\sigma_p\sigma_1 & \rho_{p2}\sigma_p\sigma_2 & \dots & \sigma_p^2 \end{vmatrix}, \tag{4}$$

де ρ_{ij}– коефіцієнт кореляції між величинами $\bar{x}_i$ та $\bar{x}_j$ $(i, j = 1, \dots, \rho_i)$ – число випадкових величин – контролюючих параметрів).

При відомій коваріаційній матриці Σ статистика Хотелінга має χ^2-розподілення. В цьому випадку при статистичному контролі багатопараметричного об'єкта положення контрольованої кордону на заданому рівні значимості α визначається безпосередньо по таблиці квантиль розподілу χ^2т, тобто:

$$T_{kp}^2 = \chi_{(1-\alpha),p}^2. \tag{5}$$

Слід також відзначити особливість застосування критерію T^2-Хотелінга – на підставі відомої коваріаційної матриці можна розраховувати «точкові» значення T_H^2.

Потім, відповідно до виразу (3), необхідно для кожної підгрупи спостережень розрахувати T_H^2.

У багатовимірному випадку обчислюється незміщена оцінка $\boldsymbol{S}$ матриці Σ. В такому випадку статистика T_H^2-Хотелінга задається формулою:

$$T_H^2 = n\left(\bar{\boldsymbol{X}} - \boldsymbol{\mu}_0\right)^T \boldsymbol{S}^{-1} \left(\bar{\boldsymbol{X}} - \boldsymbol{\mu}_0\right). \tag{6}$$

Отримане на основі виразу (5) значення T_H^2 зіставляється з критичним значенням для заданого рівня статистичної значущості α та чисел степенів свободи $\nu_1 = p$ і $\nu_2 = n - p$ $(n - 1 \geq p)$. Критичне значення статистики Хотелінга визначається як:

$$T_{\alpha,p,(n-p)}^2 = \frac{p\left(n-1\right)}{n-p} F_{\alpha,p,(n-p)}. \tag{7}$$

При цьому незміщена оцінка коваріаційної матриці визначається на підставі виразу:

$$\boldsymbol{S} = \frac{1}{n-1}\begin{vmatrix} x_{11}-\mu_{01} & x_{21}-\mu_{02} & \dots & x_{p1}-\mu_{0p} \\ x_{12}-\mu_{01} & x_{22}-\mu_{02} & \dots & x_{p2}-\mu_{0p} \\ \dots & \dots & \dots & \dots \\ x_{1n}-\mu_{01} & x_{2n}-\mu_{02} & \dots & x_{pn}-\mu_{0p} \end{vmatrix} \times \begin{vmatrix} x_{11}-\mu_{01} & x_{12}-\mu_{01} & \dots & x_{1n}-\mu_{01} \\ x_{21}-\mu_{02} & x_{22}-\mu_{02} & \dots & x_{2n}-\mu_{01} \\ \dots & \dots & \dots & \dots \\ x_{p1}-\mu_{0p} & x_{p2}-\mu_{0p} & \dots & x_{pn}-\mu_{0p} \end{vmatrix}$$

де n – число точок в вибірці/підгрупі.

Розрахункове значення статистики Хотелінга, певне на підставі виразу (7), порівнюється з критичним значенням $\mathrm{T}^2_{\alpha,p,(n-p)}$. якщо T^2_H більше критичного значення, то гіпотеза H_0 про стабільність організму не приймається. Таким чином, при відомих (заданих) середньоквадратичних відхиленнях показників організму можна, обчислюючи статистику Хотелінга T_{Hi}, виявляти розладнаність процесів в організмі в реальному масштабі часу. При невідомих же СКВ оцінюється статистична керованість процесами в організмі за певний період.

В якості прикладу на основі запропонованого підходу проведений розрахунок ретроспективних даних операторів, що виконують професійні обов'язки, у яких проведені дослідження аналізу крові впродовж одного року. Наведені розрахунки двох операторів у яких значення $\mathrm{T}^2_{\mathrm{H}}$ менше та більше $\mathrm{T}^2_{\mathrm{KP}}$ відповідно для проведення порівняльної характеристики.

Таблиця 2.

Показники клінічного аналізу крові оператора 1

Показники	Оператор 1												Сред.знач
	Квітень	Травень	Червень	Липень	Серпень	Вересень	Жовтень	Листопад	Грудень	Січень	Лютий	Березень	
Гемоглобін	14,8	15,3	15,7	15,2	14,8	14,5	15,2	14,8	14,4	13,8	13,2	12,7	14,5
Еритроцити	4,4	5	5,1	5,1	5,1	5,3	5,2	5,1	5,1	4,9	4,3	4	4,9
Лейкоцити	4,3	6,2	6,3	6,5	6,4	6,5	6,5	6,5	5,2	6,5	5,2	6,7	6,1

На основі наявних даних отримуємо оцінку коваріаційної матриці для першого оператора:

$$S1 = \frac{1}{n-1} * \begin{vmatrix} 14{,}8-14{,}5 & 15{,}3-14{,}5 & 15{,}7-14{,}5 & \dots & 13{,}8-14{,}5 & 13{,}2-14{,}5 & 12{,}7-14{,}5 \\ 4{,}4-4{,}9 & 5{,}0-4{,}9 & 5{,}1-4{,}9 & \dots & 4{,}9-4{,}9 & 4{,}3-4{,}9 & 4{,}0-4{,}9 \\ 4{,}3-6{,}1 & 6{,}2-6{,}1 & 6{,}3-6{,}1 & \dots & 6{,}5-6{,}1 & 5{,}2-6{,}1 & 6{,}7-6{,}1 \end{vmatrix} *$$

$$* \begin{vmatrix} 14{,}8-14{,}5 & 4{,}4-4{,}9 & 4{,}3-6{,}1 \\ 15{,}3-14{,}5 & 5{,}0-4{,}9 & 6{,}2-6{,}1 \\ 15{,}7-14{,}5 & 5{,}1-4{,}9 & 6{,}2-6{,}1 \\ \dots & \dots & \dots \\ 13{,}8-14{,}5 & 4{,}9-4{,}9 & 6{,}5-6{,}1 \\ 13{,}2-14{,}5 & 4{,}3-4{,}9 & 5{,}2-6{,}1 \\ 12{,}7-14{,}5 & 4{,}0-4{,}9 & 6{,}7-6{,}1 \end{vmatrix} = \frac{1}{11} * \begin{vmatrix} 8{,}76 & 3{,}02 & 0{,}45 \\ 3{,}02 & 1{,}88 & 1{,}27 \\ 0{,}45 & 1{,}27 & 6{,}16 \end{vmatrix} = \begin{vmatrix} 0{,}79 & 0{,}27 & 0{,}04 \\ 0{,}27 & 0{,}17 & 0{,}11 \\ 0{,}04 & 0{,}11 & 0{,}55 \end{vmatrix} = 0{,}025$$

На підставі вихідних даних, наведених в таблиці 1, розраховуємо T^2-критерій Хотелінга:

$$\mathrm{T}^2_{\mathrm{H}} = 12 * |14{,}5-14{,}8 \quad 4{,}9-5{,}1 \quad 6{,}1-6{,}5| * \begin{vmatrix} 3{,}09 & -5{,}47 & 0{,}87 \\ -5{,}47 & 16{,}4 & -2{,}90 \\ 0{,}87 & -2{,}90 & 2{,}33 \end{vmatrix} * \begin{vmatrix} 14{,}5-14{,}8 \\ 4{,}9-5{,}1 \\ 6{,}1-6{,}5 \end{vmatrix} = 4.74$$

Критичне значення T^2-критерію для заданого рівня значущості $\alpha = 0{,}05$ буде дорівнювати:

$$\mathrm{T}^2_{\mathrm{кр}} = (2(12-1)/12-2)) * 4{,}459 = 9{,}8$$

Таким чином, $\mathrm{T}^2_{\mathrm{H}} = 4{,}74 < \mathrm{T}^2_{\mathrm{кр}} = 9{,}8$, а це означає, що функціональний стан організму стабільний.

Аналогічно проведений розрахунок для всіх операторів. В якості прикладу наведені розрахунки оператора 7.

Таблиця 3.

Показники клінічного аналізу крові оператора 7

Показники	Оператор 7												Сред.знач
	Квітень	Травень	Червень	Липень	Серпень	Вересень	Жовтень	Листопад	Грудень	Січень	Лютий	Березень	
Гемоглобін	16,7	15	15,3	15	15,5	15,3	15,2	15,3	14,9	14,8	15	14,8	15,2
Еритроцити	5,3	4,9	5	5	5,3	4,9	5,3	5,1	5,3	5,4	5	5,1	5,1
Лейкоцити	4,7	7,4	7,3	7,8	7,6	7,8	7,4	6,4	5,8	5,1	5	4,8	6,4

На основі наявних даних можна отримати оцінку коваріаційної матриці:

$$S7 = \frac{1}{n-1} * \begin{vmatrix} 16,7-15,2 & 15,0-15,2 & 15,3-15,2 & \dots & 14,8-15,2 & 15,0-15,2 & 14,8-15,2 \\ 5,3-5,1 & 4,9-5,1 & 5,0-5,1 & \dots & 5,4-5,1 & 5,0-5,1 & 5,1-5,1 \\ 4,7-6,4 & 7,4-6,4 & 7,3-6,4 & \dots & 5,1-6,4 & 5,0-6,4 & 4,8-6,4 \end{vmatrix} *$$

$$* \begin{vmatrix} 16,7-15,2 & 5,3-5,1 & 4,7-6,4 \\ 15,0-15,2 & 4,9-5,1 & 7,4-6,4 \\ 15,3-15,2 & 5,0-5,1 & 7,3-6,4 \\ \dots & \dots & \dots \\ 14,8-15,2 & 5,4-5,1 & 5,1-6,4 \\ 15,0-15,2 & 5,0-5,1 & 5,0-6,4 \\ 14,8-15,2 & 5,1-5,1 & 4,8-6,4 \end{vmatrix} = \frac{1}{11} * \begin{vmatrix} 2,9 & 0,23 & -0,82 \\ 0,23 & 0,36 & -0,98 \\ -0,82 & -0,98 & 17,63 \end{vmatrix} = \begin{vmatrix} 0,26 & 0,02 & -0,07 \\ 0,02 & 0,03 & -0,09 \\ -0,07 & -0,09 & 1,59 \end{vmatrix} = 0.011$$

Розраховуємо T^2-критерій Хотелінга:

$$T_H^2 = 12 * |15,2-15,0 \quad 5,1-5,3 \quad 6,4-7,4| * \begin{vmatrix} 4,05 & -2,61 & 0,03 \\ -2,61 & 41,8 & 2,25 \\ 0,03 & 2,25 & 0,75 \end{vmatrix} * \begin{vmatrix} 15,2-15,0 \\ 5,1-5,3 \\ 6,4-7,4 \end{vmatrix} = 22,96$$

На основі розрахунків отримуємо, $T_H^2 = 22,96 > T_{кр}^2 = 9,8$, це вказує на те, що є порушення функціонального стану організму, а також говорить про те, що організм був схильний до дестабілізації за рахунок впливу зовнішніх факторів. Використання статистики Хотелінга також надає можливість провести додаткові розрахунки за кожним показником.

Розраховуємо окремо значення коефіцієнта Хотелінга для гемоглобіну:

$$T_{H1}^2 = \frac{12 * |1 \quad 0 \quad 0| * \begin{vmatrix} 0,2 \\ -0,2 \\ 1,0 \end{vmatrix}^2}{|1 \quad 0 \quad 0| * \begin{vmatrix} 0,26 & 0,02 & -0,07 \\ 0,02 & 0,03 & -0,09 \\ -0,07 & -0,09 & 1,59 \end{vmatrix} * \begin{vmatrix} 1 \\ 0 \\ 0 \end{vmatrix}} = \frac{0,48}{0,26} = 1,84$$

Аналогічно розраховуємо коефіцієнт для еритроцитів:

$$T_{H2}^2 = \frac{12 * |0 \quad 1 \quad 0| * \begin{vmatrix} 0,2 \\ -0,2 \\ 1,0 \end{vmatrix}^2}{|0 \quad 1 \quad 0| * \begin{vmatrix} 0,26 & 0,02 & -0,07 \\ 0,02 & 0,03 & -0,09 \\ -0,07 & -0,09 & 1,59 \end{vmatrix} * \begin{vmatrix} 0 \\ 1 \\ 0 \end{vmatrix}} = \frac{0,48}{0,03} = 16$$

Також, визначаємо коефіцієнт Хотелінга і для тертого показника крові – лейкоцитів:

$$T_{H3}^2 = \frac{12 * |0 \quad 0 \quad 1| * \begin{vmatrix} 0,2 \\ -0,2 \\ 1,0 \end{vmatrix}^2}{|0 \quad 0 \quad 1| * \begin{vmatrix} 0,26 & 0,02 & -0,07 \\ 0,02 & 0,03 & -0,09 \\ -0,07 & -0,09 & 1,59 \end{vmatrix} * \begin{vmatrix} 0 \\ 0 \\ 1 \end{vmatrix}} = \frac{12}{1,59} = 7,54$$

Оскільки $T_{H2}^2 > T_{кр}^2$, то можна зробити висновок, що показник еритроцитів був нестабільним впродовж вимірювального конструолю. Суттєві зміни в організмі є наслідком того, що на показник еритроцитів впливали зовнішні фактори дестабілізації. Це означає, що функціональний стан організму оператора був не стабільний протягом року але як видно з таблиці 1 значення його показників крові не

виходять за межі прийнятої норми. Таким чином можна зробити висновок що використання карт Хотелінга є більш чутливим методом порівняно з традиційним [5].

Аналогічним чином були розраховані показники клінічного аналізу всіх операторів. Результати розрахунків та порівняльного аналізу подані на рис. 1.

Розрахункові значення порівняні з критичними значеннями. Якщо значення $T^2_н$ перевищує значення $T^2_{кр}$, тобто контрольної границі, то можна зробити висновок про порушення функціонального стану організму в тому числі виходу за межі норми гомеостазису. Результати порівняльного аналізу подані в графічному вигляді на рис. 1.

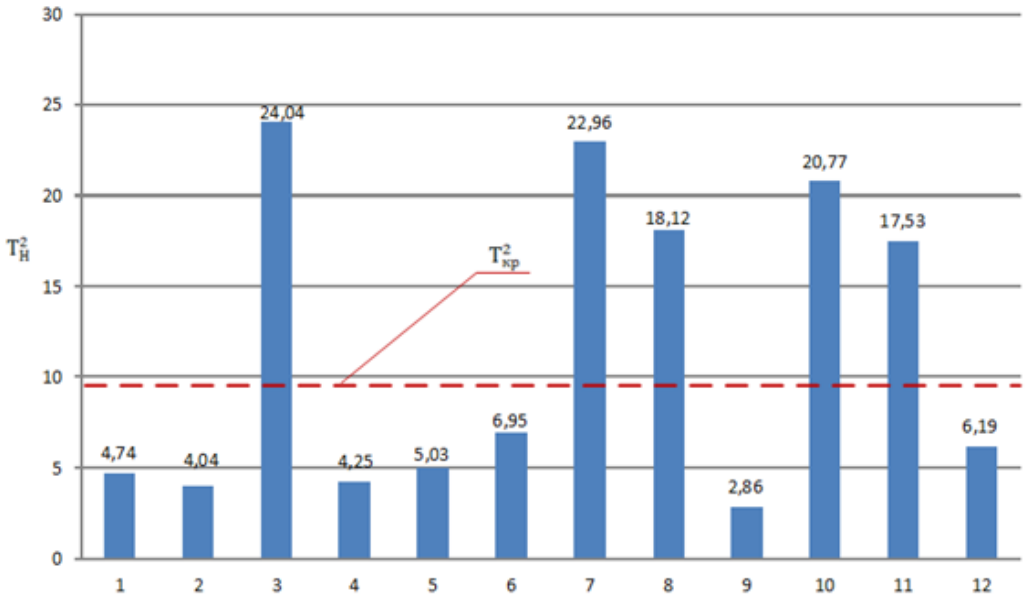


Рис. 1. Результати порівняльного аналізу розрахункових значень з критичним значенням

Червоною лінією встановлене критичне значення. Всі значення, які знаходяться вище червоної лінії свідчать про порушення функціонального стану організму [6]. Можна зробити висновок, що параметри крові п'ятьох операторів виходять за межі критичного значення, що свідчить порушення функціонального стану та потребує подальших діагностичних процедур.

За результатами розрахунків, порушення функціонального стану організму було визначено у п'ятьох операторів, в той час як за традиційним підходом наявних відхилень не було виявлено. Таким чином, застосування статистики Хотелінга для оцінювання змін в системі організму людини, дає більш достовірні результати порівняно з традиційним підходом.

До останнього часу застосування многопараметрических критеріїв було обмежено складністю обчислень. Однак широке поширення сучасних засобів обчислювальної техніки зняло ці обмеження.

Висновки. В результаті проведених досліджень запропоновано модель прийняття рішень на основі порівняльної характеристики з індивідуальними межами норми. Для визначення стабільності функціонування організму запропоновано використання T^2-статистики Хотелінга, яка на основі визначення μ_0 як найчастішого значення, що і характеризую індивідуальне значення гомеостазу дозволяє підвищити рівень достовірності прийняття рішення в порівнянні з традиційним підходом. Даний підхід дозволяє урахувати особливості концепції персоналізованого підходу в галузі охорони здоров'я і може бути використаний при професійному відборі, прогнозуванні поточного стану та в задачах страхової медицини.

Література

1. Van Trijp, R. (2013). Linguistic Assessment Criteria for Explaining Language Change: A Case Study on Syncretism in German Definite Articles, Language Dynamics and Change, 3(1), 105-132. doi: https://doi.org/10.1163/22105832-13030106

2. Rhodes V. A. Criteria for assessment of nausea, vomiting, and retching. Oncology Nursing Forum. 1997 Aug; 24 (7 Suppl): 13-19.

3. Sierra, Leonardo A., Víctor Yepes, and Eugenio Pellicer. "A review of multi-criteria assessment of the social sustainability of infrastructures." Journal of Cleaner Production 187 (2018): 496-513.

4. Kucheruk, V. Mathematical model of the visible range optical radiation passing through a water-milk solution / V. Kucheruk, I. P. Kurytnik, P. Kulakov, A. N. Vasilevskyi, D. Zh. Karabekova, D. Mostovyi, A. Kulakova // Bulletin of the Karaganda University. «Physics» series., ISSN 2518-7198, № 1(89) / 2018, p. 24 – 31, URI: rep.ksu.kz/handle/data/2937

5. Volodymyr Kucheruk, Pavlo Kulakov, Oleksandr Vasilevskyi, Dmytro Mostovyi, Anna Kulakova, Iryna M. Kobylyanska, Gaini Karnakova, and Piotr Kisala "Optical method to determine the quantity of water in milk using the visible radiation range", Proc. SPIE 10808,

Photonics Applications in Astronomy, Communications, Industry, and High Energy Physics Experiments 2018, 108080Y (1 October 2018); https://doi.org/10.1117/12.2501605

6. Bemmel J. H. Handbook of medical informatics / J. H. van Bemmel, M. A. Musen. – Houten : Springer-Verlag, – 628 p., (2002).

7. Bronzino J. D. Medical Devices and Human Engineering Four Volume Set / J. D. Bronzino, D. R. Peterson. – Boca Raton : CRC Press. – 563 p. , (2014).

8. Family Medicine: Principles and practice / R. B. Taylor, J. L. Buckingham, E. P. Donatelle, T. A. Johnson, Jr., J. E. Scherger. – New York : Springer-Verlag. – 743 p., (1988).

9. Pisanelli D. M. Ontologies in Medicine / D. M. Pisanelli. – Amsterdam : IOS Press. – 165 p., (2004)

10. Webster J. G. Medical instrumentation. Application and design / J. G. Webster – New York : John Wiley & Sons. – 675 p., (2009).

11. Ledzhevich, U. (ets.) Mathematical Methods and Models in biomedicine. – Springer, (2013).

12. Ivanets O., Kosheva L.O. Approach to the Evaluation of the Functional State of the Human Body Taking into Account the Variability of Medical and Biological Indicators. CAOL*2019 International Conference on Advanced Optoelectronics and Lasers C.661-665. #978-1-7281-1814-7/19/31.00 c 2019 IEEE

13. Іванець О. Б., Кулаков П. І., Шкіндер Г. П., Кулакова А. П. Оцінювання функціонального стану організму на основі критерію небезпеки відхилення. Наукоємні технології. - 2019. - № 4(44). - с. 441 - 448. DOI: 10.18372/2310-5461.44.14320

14. Іванець О.Б., Бурiченко М.Ю., Еременко В.С. «Method of processing the results of measurements of medical indicators». Наукоємні технології. - 2020. - № 3(47). - с. 392 - 398. DOI: 10.18372/2310-5461.47.1493715.

References

1. Van Trijp, R. (2013). Linguistic Assessment Criteria for Explaining Language Change: A Case Study on Syncretism in German Definite Articles, Language Dynamics and Change, 3(1), 105-132. doi: https://doi.org/10.1163/22105832-13030106

2. Rhodes V. A. Criteria for assessment of nausea, vomiting, and retching. Oncology Nursing Forum. 1997 Aug; 24 (7 Suppl): 13-19.

3. Sierra, Leonardo A., Víctor Yepes, and Eugenio Pellicer. "A review of multi-criteria assessment of the social sustainability of infrastructures." Journal of Cleaner Production 187 (2018): 496-513.

4. Kucheruk, V. Mathematical model of the visible range optical radiation passing through a water-milk solution / V. Kucheruk, I. P. Kurytnik, P. Kulakov, A. N. Vasilevskyi, D. Zh. Karabekova, D. Mostovyi, A. Kulakova // Bulletin of the Karaganda University. «Physics» series., ISSN 2518-7198, № 1(89) / 2018, p. 24 – 31, URI: rep.ksu.kz/handle/data/2937

5. Volodymyr Kucheruk, Pavlo Kulakov, Oleksandr Vasilevskyi, Dmytro Mostovyi, Anna Kulakova, Iryna M. Kobylyanska, Gaini Karnakova, and Piotr Kisala “Optical method to determine the quantity of water in milk using the visible radiation range”, Proc. SPIE 10808, Photonics Applications in Astronomy, Communications, Industry, and High Energy Physics Experiments 2018, 108080Y (1 October 2018); https://doi.org/10.1117/12.2501605

6. Bemmel J. H. Handbook of medical informatics / J. H. van Bemmel, M. A. Musen. – Houten : Springer-Verlag, – 628 p., (2002).

7. Bronzino J. D. Medical Devices and Human Engineering Four Volume Set / J. D. Bronzino, D. R. Peterson. – Boca Raton : CRC Press. – 563 p. (2014).

8. Family Medicine: Principles and practice / R. B. Taylor, J. L. Buckingham, E. P. Donatelle, T. A. Johnson, Jr., J. E. Scherger. – New York : Springer-Verlag. – 743 p., (1988).

9. Pisanelli D. M. Ontologies in Medicine / D. M. Pisanelli. – Amsterdam : IOS Press. – 165 p., (2004)

10. Webster J. G. Medical instrumentation. Application and design / J. G. Webster – New York : John Wiley & Sons. – 675 p., (2009).

11. Ledzhevich, U. (ets.) Mathematical Methods and Models in biomedicine. – Springer, (2013).

12. Ivanets O., Kosheva L.O. Approach to the Evaluation of the Functional State of the Human Body Taking into Account the Variability of Medical and Biological Indicators. CAOL*2019 International Conference on Advanced Optoelectronics and Lasers C.661-665. #978-1-7281-1814-7/19/31.00 c 2019 IEEE

13. Ivanets OB, Kulakov PI, Shkinder GP, Kulakova AP Estimation of a functional condition of an organism on the basis of criterion of danger of deviation. Science-Based Technologies. - 2019. - № 4 (44). - with. 441 - 448. DOI: 10.18372 / 2310-5461.44.14320

14. Ivanets OB, Burichenko M.Yu., Eremenko VS "Method of processing the results of measurements of medical indicators". Science-Based Technologies. - 2020. - № 3 (47). - with. 392 - 398. DOI: 10.18372/2310-5461.47.1493715.

Надійшла / Paper received: 11.07.2020 Надрукована / Paper Printed : 01.12.2020

УДК 681.391
DOI: 10.31891/2219-9365-2020-66-2-5

ПЯТІН І. С., МІШАН В. В., РЕЗНИЧУК Р. В.
Хмельницький національний університет

МЕТОДИ ГЕНЕРАЦІЇ ПЕРЕВІРОЧНИХ МАТРИЦЬ LDPC КОДУ

LDPC коди - це лінійні блокові коди, де перевірочні біти додаються в кінець інформаційного повідомлення. Стаття присвячена проблемі побудови перевірочних матриць коду з низькою щільністю перевірок на парність для заданих характеристик швидкості і довжини коду. Розглянуто метод генерації перевірочних матриць на основі випадкової перестановочної підматриці (квазіциклічне регулярне кодування), і структурований метод генерації матриці на основі евклідово-геометричного коду з можливістю видалення рядків і розподілу стовпців. Виконано моделювання кодів.

Ключові слова:коди LDPC, перевірочна матриця, квазіциклічний LDPC код.

PYATIN I., MISHAN V., REZNICHUCK R.
Khmelnytskyi National University

METHODS OF GENERATION OF LDPC CODE VERIFICATION MATRIXES

LDPC codes are linear block codes, where check bits are added to the end of the information message. The coding procedure is the multiplication of the information message vector of length K by the generating matrix G. The generating matrix is associated with the parity check matrix. The parity check matrix has (N–K) rows and N columns, where N corresponds to the required length of the codeword, K corresponds to the length of the message. The article is devoted to the problem of construction of code verification matrices with low density of parity checks for given characteristics of code speed and length. A method for generating test matrices based on a random permutation submatrix, known as quasicyclic regular coding, and a structured method for generating a matrix based on a Euclidean geometric code with the ability to delete rows and distribute columns are considered. An important characteristic of the LDPC code matrix is the absence of cycles of a certain size. Under the cycle of length 4 means the formation in the test matrix of a rectangle in the corners of which are units. The absence of a cycle of length 4 can also be determined by the scalar product of the columns (or rows) of the matrix. If each pairwise scalar product of all columns (or rows) of the matrix is not more than 1, this indicates the absence of a cycle of length 4. Cycles of greater length (6, 8, 10, etc.) can be determined by constructing a graph in the test matrix, vertices of which there are units, and the edges are all possible connections of vertices parallel to the sides of the matrix (ie vertical or horizontal lines). The minimum cycle in this graph will be the minimum cycle in the LDPC code check matrix. Code simulation performed.

Keywords: LDPC codes, verification matrix, QC-LDPC code, permutation matrix.

Вступ. Проблема побудови, адаптації та модифікації відомих кодів є актуальним завданням в області телекомунікацій. Висока продуктивність і коригувальна здатність, що отримується при ітеративному декодуванні турбокодів, стимулювали активні дослідження щодо застосування даного методу до декодування інших видів кодів. Зокрема, виявилося, що можливо отримати на порядок кращі характеристики при використанні кодів низької щільності (low density parity check – LDPC). Коди LDPC сьогодні все ширше застосовуються на практиці: їх використовують стандарти DVB-T2, DVB-S2, DVB-C2, WiFi, WiMax, IEEE 802.15.3. Також передбачено передавання даних користувача транспортного каналу за допомогою кодів LDPC у системах зв'язку 5G. Коди LDPC пропонують кращу спектральну ефективність ніж турбо-коди, і підтримують високу пропускну здатність [1].

Одним із завдань, пов'язаних з побудовою кодів низької щільності, є генерація перевірочних матриць із заданими властивостями. LDPC код задається перевірочною матрицею *H*, що має властивість розрідженої, тобто її рядки і стовпці містять малу кількість ненульових елементів в порівнянні з розмірністю матриці. Перевірочна *H* і генераторна *G* матриці повинні задовольняти наступній умові:

$$GH^T = 0.$$

Кодування послідовності ($m_1, m_2, ..., m_k$) полягає в отриманні кодованої послідовності ($c_1, c_2, ..., c_n$):

$$C = (m_1, m_{2,...}, m_k)G = (c_1, c_{2,...}, c_n)$$

за умови, що:

$$H(c_1, c_{2,...}, c_n)^T = 0.$$

Перевірочна матриця LDPC-коду. Використовуються два принципи побудови перевірочних матриць. Перший заснований на генерації початкової перевірочної матриці за допомогою псевдовипадкового генератора. Коди, отримані таким методом, називають випадковими (random-like codes). Основні недоліки випадкових кодів – необхідність застосування алгоритмів видалення коротких циклів і нестабільні робочі характеристики коду. Другий базується на використанні спеціальних структурованих методів, заснованих на групах, кінцевих полях, тощо. Краще виправлення помилок забезпечують випадкові

LDPC-коди. Структуровані методи дозволяють використовувати оптимізацію процедур зберігання, кодування і декодування, а також отримувати коди з більш передбачуваними і стійкими характеристиками.

Галлагером була запропонована наступна структура перевірочної матриці H з параметрами (n , λ , ρ), де n – кількість стовпців матриці, яка має λ одиниць в кожному стовпці і ρ одиниць в кожному рядку (інші нулі). Приклад матриці для (20, 3, 4) LDPC-коду представлений виразом:

$$H=\begin{pmatrix}H_1\\H_2\\H_3\end{pmatrix}=\begin{pmatrix}
1&1&1&1&&&&&&&&&&&&&&&&\\
&&&&1&1&1&1&&&&&&&&&&&&\\
&&&&&&&&1&1&1&1&&&&&&&&\\
&&&&&&&&&&&&1&1&1&1&&&&\\
1&&&&1&&&&1&&&&1&&&&&&&\\
&1&&&&1&&&&1&&&&&&&1&&&\\
&&1&&&&1&&&&&&&1&&&&1&&\\
&&&1&&&&&1&&&&1&&&&1&&&\\
&&&&&&&1&&&1&&&1&&&&&1&\\
1&&&&1&&&&&&1&&&&&1&&&&\\
&1&&&&1&&&1&&&&1&&&&&&&\\
&&1&&&&1&&&&1&&&&&1&&&&\\
&&&1&&&&1&&&&1&&&1&&&&&\\
&&&&1&&&&1&&&&1&&&1&&&&
\end{pmatrix}$$

Як видно, структурно вона складається з трьох підматриць, в кожній з яких міститься тільки одна одиниця в стовпці: в H_1 кожний *i*-й рядок містить одиниці в стовпці від $(i-1)k+1$ до ik ; H_2 і H_3 отримані шляхом випадкової перестановки стовпців матриці H_1. Всі рядки і стовпці матриці H мають однакові ваги, що робить код регулярним.

Оскільки використовувалася випадкова перестановка і немає чітко визначеного правила, то в подальшому необхідно проведення комп'ютерного пошуку для вибору з потенційної множини кодів з найкращими характеристиками. Більш універсальним є структурований метод побудови коду на основі евклідово-геометричних кодів $EG(m,2^k)$ [2]. Даний метод дозволяє наблизитися до границі Шеннона при BER (Bit Error Rate), що дорівнює 10^{-4}.

Евклідово-геометричні коди будуються як система кодів $EG(m,p^s)$. Код має наступні характеристики: довжина кодового слова – $n=2^{2s}-1$; довжина інформаційного повідомлення – $k=2^{2s}-3^s$; кількість надлишкових біт – $n-k=3^s-1$; мінімальна відстань – $d_{\min}=2^s+1$. Оскільки число одиниць в перевірочній матриці евклідово-геометричного коду мало в порівнянні з розміром матриці, то такий код можна розглядати як LDPC-код. Перевірочна матриця H_{EG} будується наступним чином: рядки перевірочної матриці відповідають лініям евклідової геометрії, стовпці – ненульовим точкам в $EG(m,p^s)$. Елементи матриці H_{EG} визначаються з векторів геометрії Евкліда:

$$H_{EG}(i,j)=\begin{cases}1, \text{ якщо точка на прямій } i,\\ 0, \quad\quad \text{в іншому випадку.}\end{cases}$$

Якщо ввести позначення $q=p^s$, то матриця H_{EG} має $n=q^m$ стовпців і $r=q^{m-1}(q^m-1)/(q-1)$ рядків. Кожен стовпець матриці містить $\lambda=q^{m-1}(q^m-1)/(q-1)$ одиниць, кожен рядок містить $\rho=p^s$ одиниць. Наприклад, евклідово-геометричний код $EG(2,2^2)$ буде мати перевірочну матрицю, що відповідає структурі регулярного коду LDPC (15, 4, 4). Нерегулярні LDPC-коди (ваги стовпців і рядків описуються за допомогою функцій $\lambda(i)$ і $\rho(i)$, які задають частку стовпців і рядків з вагою *i*) мають кращі характеристики, ніж регулярні.

Розглянемо метод побудови LDPC-кодів, в основі якого лежить властивість – будь-який циклічний зсув кодового слова є також кодове слово. Такий блоковий код називається квазіциклічним (QC-LDPC) [3].

Перевірочна матриця коду являє собою поєднання $H = [H_1, H_2, \ldots, H_P]$ циклічних матриць:

$$H_{QC} = \begin{bmatrix} P_{a1,1} & P_{a1,2} & \cdots & P_{a1,c-1} & P_{a1,c} \\ P_{a2,1} & P_{a2,2} & \cdots & P_{a2,c-1} & P_{a2,c} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ P_{am,1} & P_{am,2} & \cdots & P_{am,c-1} & P_{am,c} \end{bmatrix},$$

де $a_{j,k}$ являє собою циклічний зсув стовпців матриці на i розрядів. Таким чином, P_j – перестановочна матриця розміром $L \times L$, яка утворюється в результаті циклічного зсуву стовпців на i позицій. У реальних системах L вибирається досить великим, наприклад, $L = 101$. Вибір одиничної матриці в якості P_0 не є обов'язковим, наприклад, для $L = 5P_0$, одинична матриця може бути наступною:

$$P_0 = \begin{bmatrix} 1 & & 1 & 1 & \\ & 1 & & 1 & 1 \\ 1 & & 1 & & 1 \\ 1 & 1 & & 1 & \\ & 1 & 1 & & 1 \end{bmatrix}$$

Генерація перевірочної матриці. У загальному випадку циклічна матриця описується асоційованим полиномом:

$$p_i(x) = \sum_{j=0}^{L-1} (P_i)_{oj} \, x^j$$

Перший спосіб генерації перевірочної матриці квазіциклічного LDPC-коду заснований на випадковому розподілі перестановочних матриць із заданим розподілом ρ(x) і λ(x) (залежно від їх вибору можуть бути побудовані регулярні і нерегулярні коди). Якщо L = 47, m = 6, j = 12, то загальний розмір матриці QC-LDPC коду H буде $L_m \times L_j$ або 250×450. Приклад структури перевірочної матриці показаний на рис. 1.

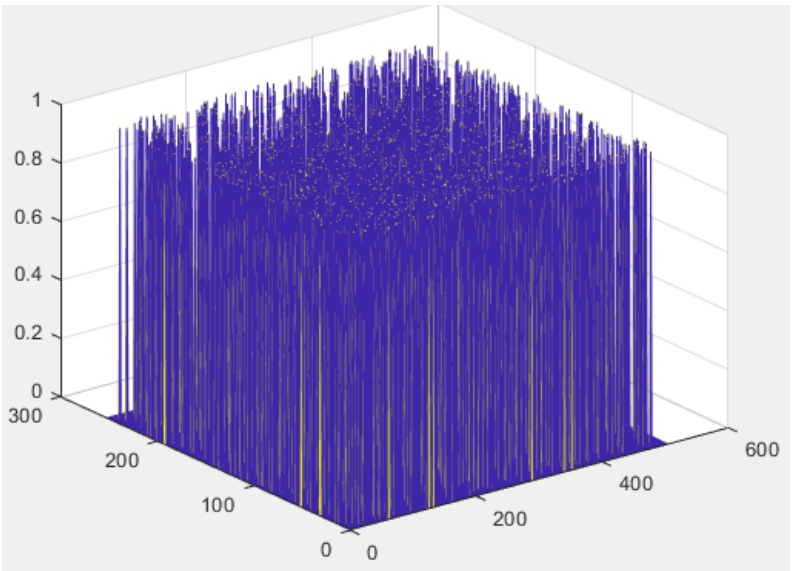


Рис. 1. Приклад будови перевірочної матриці QC-LDPC коду

Другий спосіб отримання перевірочної матриці заснований на виборі двох чисел a і b, що належать ненульовим елементам поля Галуа $GF(L)$, де L – просте число. Тоді заповнення матриці H розміром $L_m \times L_j$ – розстановка перестановочних матриць.

Отримуємо регулярний квазіциклічний LDPC-код з λ = m – 1, σ = j – 1 і швидкістю $r \geq 1 - (m/j)$. Для даної матриці довжина найкоротшого циклу буде 8 (що значно більше, ніж у LDPC-кодів, побудованих на

основі евклідово-геометричних кодів). Велика величина довжини циклу дозволяє ефективно використовувати декодування з поширенням довіри.

Декодування кодів LDPC. Алгоритм декодування LDPC кодів базується на логарифмічному відношенні правдоподібності (log-likelihood ratio – LLR), що визначається виразом:

$$LLR(x \mid y) = \ln\left[\frac{p(y \mid x=0)}{p(y \mid x=1)}\right]$$

Припустимо, $x = [x_1, x_2, \ldots, x_n]$ позначає кодове слово, яке модулюється при використанні двійкової фазової модуляції, і модульовані значення x передаються по каналу з адитивним білим гаусовим шумом (АБГШ). Припустимо $y = [y_1, y_2, \ldots, y_n]$ позначає вхідну послідовність прийнятих сигналів (символів). Демодулятор приймає вхідну послідовність сигналів і обчислює відповідні LLR значення для: $j = 1, 2, \ldots, n$.

$$\lambda_j = LLR(y_j \mid x_j) = \ln\left[\frac{p(y_j \mid x_j = 0)}{p(y_j \mid x_j = 1)}\right].$$

При двійковій біполярній передачі по каналу LLR значення обчислюються за допомогою виразу:

$$\lambda_j = \frac{2}{\sigma^2} \cdot y_j,$$

де σ^2 – дисперсія шуму у каналі зв'язку.

На рис. 2 показана залежність ймовірності помилки на біт (BER) від відношення сигнал/шум (E_b/N_0) для системи зв'язку з LDPC-кодом та модуляцією.

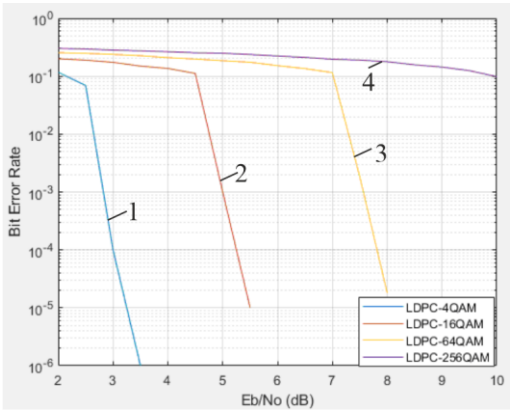


Рис. 2. Залежність ймовірності помилки на біт (BER) від відношення сигнал/шум (Eb/N0) для системи зв'язку з LDPC кодом та модуляцією (*1* – QPSK; *2* – 16QAM; *3* – 64-QAM; *4* – 256QAM)

З аналізу отриманої залежності можна зробити висновок, що найбільшу енергетичну ефективність забезпечує використання LDPC коду з модуляцією QPSK. Модуляція QPSK на 2 дБ ефективніше модуляції 16QAM і на 5 дБ ефективніше модуляції 64QAM.

Висновки. За результатами синтезу коди з перевірочними квазіциклічними матрицями низької щільності, отриманими на основі випадкових перестановок, мають вищу продуктивність, ніж коди з матрицями на основі структурованих евклідово-геометричних кодів при однаковій швидкості коду (0,5), при однаковій кількості перевірочних і інформаційних розрядів (283, 564). Однак коригувальна здатність кодів на основі квазіциклічних матриць нестабільна і змінюється в діапазоні від 10^{-3} до 10^{-5} (SNR = 6 dB).

Література

1. H. Li, B. Bai, X. Mu, J. Zhang and H. Xu, "Algebra-Assisted Construction of Quasi-Cyclic LDPC Codes for 5G New Radio," in IEEE Access, vol. 6, pp. 50229-50244, 2018, doi: 10.1109/ACCESS.2018.2868963.

2. S. K. Chilappagari, D. V. Nguyen, B. Vasic and M. W. Marcellin, "Girth of the Tanner graph and error correction capability of LDPC codes," 2008 46th Annual Allerton Conference on Communication, Control, and Computing, Urbana-Champaign, IL, 2008, pp. 1238-1245, doi: 10.1109/ALLERTON.2008.4797702.

3. Yige Wang, J. S. Yedidia and S. C. Draper, "Construction of high-girth QC-LDPC codes," 2008 5th International Symposium on Turbo Codes and Related Topics, Lausanne, 2008, pp. 180-185, doi: 10.1109/TURBOCODING.2008.4658694.

Надійшла / Paper received: 12.09.2020 Надрукована / Paper Printed : 02.12.2020

УДК 621.396.12
DOI: 10.31891/2219-9365-2020-66-2-6

ЛУЖАНСЬКИЙ В. І., ФОРКУН І. В., ФОРКУН Ю. В., КЛЬОЦ Ю.П.
Хмельницький національний університет

ВПЛИВ ПРОЦЕСУ АВТОМАТИЗАЦІЇ РІВНЕМ ПОТУЖНОСТІ СИГНАЛУ ПЕРЕДАВАЧІВ БАЗОВОЇ ТА МОБІЛЬНИХ СТАНЦІЙ МЕРЕЖІ РУХОМОГО ЗВ'ЯЗКУ СТАНДАРТУ CDMA

Мета наукової статі полягає в досліджені впливу процесу автоматизації рівнем потужності сигналу передавачів базової та мобільних станцій мережі рухомого зв'язку стандарту CDMA . Також наведені розрахунки максимальної кількості активних мобільних абонентів в комірці, потужності сигналу, яка припадає на одного абонента мережі мобільного зв'язку, ймовірності бітової помилки в залежності від потужності шумів на вході приймача та швидкості передачі цифрової інформації.

Ключові слова: автоматизація рівня потужності приймача ,мобільний зв'язок, стандарт CDMA, мобільна станція (МС), базова станція(БС), внутрішньосистемні завади, співвідношення сигнал/завада, ймовірність бітової помилки.

LUZHANSKY V., FORKUN I., FORKUN Y., KLOTS Y.
Khmelnitsky National University

THE INFLUENCE OF THE AUTOMATION PROCESS ON THE LEVEL OF THE SIGNAL POWER OF THE TRANSMITTERS OF THE BASE AND MOBILE STATIONS OF THE MOBILE NETWORK OF THE CDMA STANDARD

The purpose of the scientific article is to study the effects of the process of automation of the signal power level of transmitters of base and mobile stations of the mobile network of the CDMA standard. Calculations of the maximum number of active mobile subscribers in a cell, signal strength per mobile subscriber, probability of bit error depending on the power of noise at the receiver input and digital data rate are also given.

In the process of development of mobile communication networks, the issues of their planning and optimization are important. We will study that before the automated control of the signal power level of transmitters of base and mobile stations of the CDMA mobile network on the number of active subscribers in the cell, the signal-to-noise ratio at the input of base and mobile station receivers, the impact of intra-system interference in the mobile network, the effect of receiver noise and the rate of transmission of digital information on the probability of bit error.

CDMA mobile networks have a high noise immunity to signal interference, which is achieved through a special coding algorithm, which allows to transmit the signal almost without distortion, and the CDMA standard allows to achieve a minimum amount of harmful radiation during operation and low cost of cellular tariffs standard.Therefore, further research on CDMA mobile networks is relevant.

Keywords: receiver traffic level automation, mobile communication, CDMA standard, mobile station (MS), base station (BS), internal system interference, signal-to-noise ratio, bit error probability.

Вступ. В процесі розвитку мереж мобільного зв'язку важливими є питання їх планування і оптимізації. Проведемо дослідження, що до автоматизованого регулювання рівня потужності сигналу передавачів базової та мобільних станцій мережі рухомого зв'язку стандарту CDMA на кількість активних абонентів в комірці, на співвідношення сигнал/завада на вході приймачів базової та мобільних станцій, на вплив внутрішньосистемних завади в мережі мобільного зв'язку при заданій якості, впливу шумів приймача та швидкості передачі цифрової інформації на ймовірність бітової помилки.

Аналіз стану досліджень та публікацій. Мережі мобільного зв'язку стандарту CDMA мають високу завадостійкість перед перешкодами сигналів, що досягається завдяки спеціальним алгоритмом кодування, що дозволило домогтися передачі сигналу практично без спотворення, також стандарт CDMA дозволяє домогтися мінімальної кількості шкідливого випромінювання при роботі обладнання і низької вартість тарифів стільникового зв'язку стандарту. Тому подальше дослідження мереж мобільного зв'язку стандарту CDMA є актуальним.

Формування мети. Мета наукової статі полягає в досліджені впливу процесу автоматизації рівнем потужності сигналу передавачів базової та мобільних станцій мережі рухомого зв'язку стандарту CDMA . Також наведені розрахунки максимальної кількості активних мобільних абонентів в комірці, потужності сигналу, яка припадає на одного абонента мережі мобільного зв'язку, ймовірності бітової помилки в залежності від потужності шумів на вході приймача та швидкості передачі цифрової інформації.

Результати дослідження. Контролер базових станцій (КБС) або BSC (Base Station Controller) здійснюють автоматичне керування декількома (10-15) базовими станціями (БС). Один контролер може керувати до 1020 приймачами та передавачами БС . Контролер базової станції з'єднується з центром комутації рухомого зв'язку шляхом цифрової радіорелейної лінії (ЦРРЛ) в діапазонах 11,13…23 ГГц, пропускаючи цифровий потік зі швидкістю 64 кбіт/с.

Контролер базової станції виконує наступні функції:

– встановлює з'єднання між двома мобільними станціями (МС), які знаходяться в одній комірці;

– встановлює з'єднання між двома мобільними станціями, які знаходяться в зоні дії різних БС, але які контролюються одним і тим же контролером базових станцій;

– передає обслуговування мобільної станції(МС) від однієї БС до іншої при перетині мобільною станцією межі між комірками, як що обидві БС контролюються одним і тим же контролером базових станцій;

– організує радіовимірювання в радіотракті співвідношення сигнал/шум для автоматичного оперативного регулювання вихідної потужності передавачів БС та МС .

Центральним елементом коміркової системи рухомого радіозв'язку є центр управління та обслуговування (ЦУО) або ОМС (Operations and Maintanance Center), який забезпечує автоматичне керування всіма елементами системи, а також здійснює контроль якості функціонування мережі в основному.

Потужності передавачів МС в одній комірці встановлюється таким чином, що б на вході приймача БС потужності сигналів, які приходять, автоматично регулювались з точністю $\pm$, 0,2 дБ для стандарту CDMA.

В стандарті CDMA потужність передавачів БС регулюється дискретно кроком $\pm$0,2 дБ. Автоматичне регулювання потужності передавача БС зменшує рівень внутрішньосистемних завад, що дозволяє збільшити ємність мережі (число активних мобільних абонентів). Точність автоматичного регулювання потужності передавача МС кроком $\pm$0,5 дБ. В технології CDMA IS-95 на кожній несучій частоті можна організувати до 55 цифрових мовних каналів. Автоматизоване управління потужностями передавачів МС і БС забезпечує ефективну боротьбу з швидкими та повільними завмираннями сигналів, зменшує дію завад, компенсує затухання сигналів та економить електроенергію БС та МС та забезпечує максимальну кількість активних абонентів в комірці БС, зменшує вартість послуг та зменшує дію електромагнітних хвиль на організм людини.

Автоматичне вирівнювання рівнів сигналів активних МС на вході приймача БС реалізує схема з замкнутою петлею пілот-сигналу, в якому знаходиться інформація про співвідношення сигнал/завада. Потужність пілотного сигналу на 4-6дБ перевищує потужність в каналі трафіку. Проведемо розрахунок числа активних абонентів в коміркових системах рухомого радіозв'язку з кодовим поділом каналів. Особливості розрахунку ємності стільника при номінальному плануванні мережі UMTS (Universal Mobile Telecommunications System). Ємність стільники визначається числом абонентів, що обслуговуються одночасно на одному частотному каналі. Так як точне визначення цього числа є складним завданням, залежить від багатьох чинників. Розглянемо наближену методику розрахунку, засновану на наступних припущеннях – всі МС: в комірці знаходяться на рівній відстані від антени базової станції; мають однакову потужність передавачів радіосигналів; мають однакову швидкість передачі даних.

Введено поняття виграшу G у відношенні сигнал/шум за рахунок широкосмуговості використовуваного радіосигналу ($B >> 1$). З урахуванням прийнятих допущень всі абоненти мають однаковий виграш G. При цьому швидкість передачі елементарних символів в соті фіксована (3,84 Мбіт/с), а G визначається швидкістю передачі даних R в каналі.

Фізичний механізм підвищення відношення сигнал/завада ґрунтується на тому, що для k-го сигналу в кореляторі використовується відповідний йому опорний сигнал, і спектр корисного сигналу стискається. В результаті операції стиснення енергія корисного сигналу виявляється зосереджене в смузі частот вихідного цифрового сигналу. Для всіх інших сигналів використовувана в корелятор псевдо випадкової послідовності який не є опорним сигналом. Тому після обробки в кореляторі їх спектри залишаються широкосмуговими, а доля енергії в основній смузі є незначною. Ступінь розширення (стиснення) спектра залежить від бази сигналу, яка визначається наступним чином:

$$B = FT, \tag{1}$$

де F – ширина спектру цифрового сигналу на вході модулятора передавача; T – тривалість символу інформаційної послідовності, наприклад, для стандарту cdmaOne F = 1,2288 МГц і T = 1/9,6 мс, тому $B = FT = 1{,}2288 \cdot 10^6 / 9{,}6 \cdot 10^3 = 128$. База є однією з найважливіших характеристик сигналу з розширеним спектром, вона визначає виграш при кореляції обробці або просто виграш обробки.

Відповідно співвідношення потужностей сигналу і шуму на вході приймача визначається виразом:

$$\frac{P_C}{P_{N_0}} = \frac{E_B + N_0}{G}. \tag{2}$$

Припустимо, що в комірці є N активних абонентів. Тоді для кожного абонента потужність шуму визначається сумою потужностей радіосигналів від інших абонентів $P_{N_0} = (N-1)P_C$. У цьому випадку (3) набуде вигляду:

$$\frac{P_C}{P_{N_0}} = \frac{P_C}{P_C(N-1)} = \frac{1}{N-1}. \quad (3)$$

При великому числі активних абонентів вираз (3) можна спростити, таким чином, $(E_b / N_0)/G \approx 1/N$, або число активних абонентів в комірці:

$$N = \frac{G}{E_b / N_0}. \quad (4)$$

Припустимо, що база радіосигналів, що використовуються в комірці, дорівнює 128, необхідне відношення сигнал / шум на вході приймача базової станції становить 3 дБ (2 рази). За формулою (4) виводимо:

$$N \approx \frac{G}{E_b / N_0} \approx \frac{128}{2} = 64 \text{ (àáî í åí òè)}. \quad (5)$$

Теоретично 64 – максимальне число активних абонентів в комірці при G = 128. При розрахунку враховувався лише вплив перешкод всередині комірки. Якщо врахувати вплив внутрішньо системних завад від сусідніх комірок, то число абонентів, що обслуговуються зменшиться. Так, при рівному впливу сусідніх комірок число абонентів, що обслуговуються, зменшиться вдвічі: 64/2 = 32.

Необхідне співвідношення E_b / N_0 є головним чинником при розрахунку ємності комірки, пов'язаного зі швидкістю передачі даних в частотному каналі. Відношення сигнал/шум характеризується наступними фізичними принципами:

– спектральна щільність теплових шумів є постійною величиною і характеристикою приймача;

– зі збільшенням бази радіосигналу (виграшу G) необхідне значення енергії радіосигналу для передачі одного біта повідомлення зменшується;

– збільшення швидкості передачі даних вимагає великого значення енергії;

Розрахунок потужності передавача базової станції, випромінюваної на одну мобільну станцію. У системах стандарту CDMA на кожну МС доводиться певна частка сумарної потужності передавача БС. Більшість виробників обладнання CDMA рекомендує використовувати такі значення потужності передавача, що припадають на одного абонента: 0,46...2,19 Вт (–3,3...–3,4 дБВт), залежно від віддаленості МС від БС. Згідно з моделлю Окамури–Хати потужність сигналу, яка припадає на одного абонента визначається співвідношенням:

$$P_{ÁÑ} = \left[69{,}55 + P_{Ì Ñ} + 26{,}16\lg \mathrm{f} - 13{,}82\lg \mathrm{h} b_{ÁÑ} - \alpha - G_{ÁÑ} + (44{,}9 - 6{,}55\lg h_{ÁÑ})\lg R + k_\tau \sigma_0\right], \quad (6)$$

$$\text{де } \alpha = (1{,}1\lg \mathrm{f} - 0{,}7)h_{Ì Ñ} - (1{,}56\lg \mathrm{f} - 0{,}8); \quad (7)$$

P_{MC} – чутливість приймача мобільної станції, дБВт;

f – частота, на якій здійснюється передача сигналів в мережі, МГц;

R_0 – радіус стільника, км;

$G_{БС}$ – коефіцієнт підсилення антени базової станції, дБ;

$h_{БС}$ – висота підвісу антени БС, м;

h_{MC} – висота підвісу антени МС, м.

Якщо прийняти значення $P_{БС}$ = –154 дБВт, f = 2,1 ГГц, $G_{БС}$ = 21 дБ, $h_{БС}$ = 32 м, h_{MC} = 1,7 м, R_0 = 8 км, $k_\tau \sigma_0$ =1,645 $k_\tau \sigma_0 \cdot 1{,}39 = 2{,}3$.

Підставемо числові значення в формулу (5) і отримаємо:

$$P_{ÁÑ} = \left[69{,}55 - 154 + 26{,}16\lg 2100 - 13{,}82\lg 32 - 0{,}606 - 21 + (44{,}9 - 6{,}55\lg 32)\lg 8 + 2{,}3\right] = -1{,}65 \text{ äÁÂò (0,7 Âò)}.$$

Останній член цього виразу визначає запас потужності сигналу для забезпечення заданої надійності радіоканалу. Цей запас в системах CDMA виявляється менше, ніж в інших системах, так як МС здійснює вибір тієї БС, яка забезпечує найбільший рівень сигналу.

Повна потужність сигналу, що випромінюється антеною БС з урахуванням регулювання потужності БС, визначається формулою:

$$P_t = \frac{1{,}09\alpha 0{,}3 n_0}{1-\lambda}, \quad (8)$$

де n_0 – для прийнятних значень (50…60); λ – середня довжина електромагнітної хвилі (0,14 м).

$$P_t = \frac{1,09 \cdot 0,606 \cdot 0,3 \cdot (50...60)}{1-0,14} = (11,5...13,8) Âò.$$

Отриманий результат вказує на те, що в системах CDMA значення випромінюваної потужності базовою станцією істотно нижче, ніж в системах TDMA (GSM-900, GSM-1800 та ін.)

У цифровій системі передачі інформації по каналу зв'язку з білим гауссівським шумом використовують двійкову фазову маніпуляцію ФМ-2 (BPSK).

Швидкість передачі інформації дорівнює R = 10 Мбіт/с. У приймальнику сигнали обробляються когерентно з використанням узгодженого фільтра. Рівень потужності сигналу на вході приймача базової станції становить $P_c =$ 112дБВт. Коефіцієнт шуму приймача дорівнює n = 9 дБ. Визначимо ймовірність бітової помилки при чотирьох заданих даних 12,15,18 та 20 МБ/с.

Розв'язання. Перш за все визначимо потужність сигналу на вході приймача:

$$P_{ñ} = 10^{0,1 \cdot P_c} = 10^{-11,2} = 6,3 \cdot 10^{-12} Âò = 6,3ï \ Âò.$$

Відповідно продовжимо наші розрахунки і знайдемо тривалість одного біта при 12, 15, 18 та 20 МБ/с, відповідно:

$$T_{12} = \frac{1}{R} = \frac{1}{12 \ Ì \ á³ò/ñ} = \frac{1}{12 \cdot 10^6 \ á³å/ñ} = 0,083 \cdot 10^{-6} c;$$

$$T_{15} = \frac{1}{R} = \frac{1}{15 \ Ì \ á³ò/ñ} = \frac{1}{15 \cdot 10^6 \ á³å/ñ} = 0,067 \cdot 10^{-7} c;$$

$$T_{18} = \frac{1}{R} = \frac{1}{18 \ Ì \ á³ò/ñ} = \frac{1}{18 \cdot 10^6 \ á³å/ñ} = 0,056 \cdot 10^{-6} c;$$

$$T_{20} = \frac{1}{R} = \frac{1}{20 \ Ì \ á³ò/ñ} = \frac{1}{20 \cdot 10^6 \ á³å/ñ} = 0,05 \cdot 10^{-6} c.$$

Відповідно знайдемо енергію, що витрачається на передачу одного біта:

$$E_{b12} = P_C \cdot T = 6,3 \cdot 10^{-12} \cdot 0,083 \cdot 10^{-6} = 0,52 \cdot 10^{-18} Äæ;$$

$$E_{b15} = P_C \cdot T = 6,3 \cdot 10^{-12} \cdot 0,067 \cdot 10^{-6} = 0,42 \cdot 10^{-18} Äæ;$$

$$E_{b18} = P_C \cdot T = 6,3 \cdot 10^{-12} \cdot 0,056 \cdot 10^{-6} = 0,35 \cdot 10^{-18} Äæ;$$

$$E_{b20} = P_C \cdot T = 6,3 \cdot 10^{-12} \cdot 0,05 \cdot 10^{-6} = 0,32 \cdot 10^{-18} Äæ.$$

Потужність шумів на вході приймача можна визначити за формулою (9):

$$P_{Ш \ ПР} = nkT_0 \Delta f_{ПР}, Bm, \tag{9}$$

де n – коефіцієнт шуму приймача; $k = 1,38 \cdot 10^{-23} Âò/(Ãö \cdot ãðàä)$ – постійна Больцмана; T_0 = 290 К – шумова температура в градусах Кельвіна; $\Delta f_{ПР}$ – смуга пропускання високочастотного тракту приймача. Звідси одностороння спектральна щільність потужність білого шуму може бути представлена як:

$$N_0 = nkT_0, Bm/Гц, \quad N_0 = -195 \ \ дБВт/Гц = 3,16 \cdot 10^{-20}, Bm/Гц.$$

Тепер можна знайти співвідношення сигнал/шум на вході приймача:

$$E_{b12}/N_0 = \frac{0,52 \cdot 10^{-18}}{3,16 \cdot 10^{-20}} = 16,45 \text{ дБ};$$

$$E_{b15}/N_0 = \frac{0,42 \cdot 10^{-18}}{3,16 \cdot 10^{-20}} = 13,3 \text{ дБ};$$

$$E_{b18}/N_0 = \frac{0,35 \cdot 10^{-18}}{3,16 \cdot 10^{-20}} = 11 \text{ дБ}.$$

$$E_{b20}/N_0 = \frac{0,32 \cdot 10^{-18}}{3,16 \cdot 10^{-20}} = 10 \text{ дБ};$$

Тепер вирахуємо ймовірність помилки:

$$P_{b12} = Q\left(\sqrt{\frac{2E_b}{N_0}}\right) = Q\left(\sqrt{\frac{2\cdot 0{,}52\cdot 10^{-18}}{3{,}16\cdot 10^{-20}}}\right) = Q(5{,}73) = 0{,}5\cdot 10^{-8}$$

$$P_{b15} = Q\left(\sqrt{\frac{2\cdot 0{,}42\cdot 10^{-18}}{3{,}16\cdot 10^{-20}}}\right) = Q(5{,}15) = 1{,}3\cdot 10^{-7}$$

$$P_{b18} = Q\left(\sqrt{\frac{2\cdot 0{,}35\cdot 10^{-18}}{3{,}16\cdot 10^{-20}}}\right) = Q(4{,}7) = 1{,}3\cdot 10^{-6}$$

$$P_{b20} = Q\left(\sqrt{\frac{2\cdot 0{,}32\cdot 10^{-18}}{3{,}16\cdot 10^{-20}}}\right) = Q(4{,}5) = 3{,}3\cdot 10^{-6}$$

Ймовірність бітової помилки від швидкості передачі цифрової інформації наведено в таблиці 1:

Таблиця 1

Залежність ймовірності бітової помилки від швидкості передачі цифрової інформації

R, Мбіт/с	12	15	18	20
P_b	$0{,}5\cdot 10^{-8}$	$1{,}3\cdot 10^{-7}$	$1{,}3\cdot 10^{-7}$	$1{,}3\cdot 10^{-6}$

Висновки

1. Процес автоматизації рівнем потужності сигналу передавачів базової та мобільних станцій мережі рухомого зв'язку стандарту CDMA забезпечує задане співвідношення сигнал/завада на вході приймачів базових та мобільних станцій при заданій якості зв'язку, зменшує внутрішньо/системні завади мережі, забезпечує економне споживання приймально/передавального обладнання систем мобільного зв'язку, забезпечує максимальну максимальну кількість активних абонентів в мережі та забезпечує мінімальну кількість шкідливого впливу електромагнітного випромінювання на організм людини.

2. Максимальна кількість активних користувачів в комірці мереж мобільного зв'язку стандарту CDMA при заданих умовах буде складати 64 абонента.

3. Згідно з моделлю Окамури–Хати потужність сигналу, яка припадає на одного абонента буде складати $-1{,}65 дБВт. (0{,}7 Вт)$.

4. При збільшені швидкості передачі цифрової інформації імовірність бітової помилки зростає. Так при швидкості 12 Мбіт/с імовірність бітової помилки $P_b = 0{,}5\cdot 10^{-8}$ а при швидкості 20 Мбіт/с буде $P_b = 1{,}3\cdot 10^{-6}$.

Література

1. Сукачов Е. А. Стільникові мережі радіозв'язку з рухомими об'єктами: навч. посібник / Е. А. Сукачов: [3-е вид, випр. і доп.]. – Одеса: ОНАЗ ім. А. С. Попова, 2013. – 256 с.

2. Маковєєва М. М. Системи зв'язку з рухомими об'єктами: навч. посібник для вузів / М. М. Маковєєва, Ю. С. Шінаков. – М .: Радио и связь, 2002. – 440 с.

3.Смирнов Н. І. Оцінка пропускної спроможності базових станцій систем МДКР при зміні щільності їх розташування / Н. І. Смирнов, Ю. А. Караваєв, В. А. Сівов // Електросвязь. – 2001.- № 10. – С. 30-33

References

1. Sukachov E. A. Stil'nykovi merezhi radiozv'jazku z ruhomymy ob'jektamy: navch. posibnyk / E. A. Sukachov: [3-e vyd, vypr. i dop.] . – Odesa: ONAZ im. A. S. Popova, 2013. – 256 s.

2. Makovjejeva M. M. Systemy zv'jazku z ruhomymy ob'jektamy: navch. posibnyk dlja vuziv / M. M. Makovjejeva, Ju. S. Shinakov. – M .: Radyo y svjaz', 2002. – 440 s.

3.Smyrnov N. I. Ocinka propusknoi' spromozhnosti bazovyh stancij system MDKR pry zmini shhil'nosti i'h roztashuvannja / N. I. Smyrnov, Ju. A. Karavajev, V. A. Sivov // Elektrosvjaz'. – 2001.- № 10. – S. 30-33

Надійшла / Paper received: 16.10.2020 Надрукована / Paper Printed : 01.12.2020

ІНФОКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ, АВТОМАТИЗАЦІЯ ТА ОБЧИСЛЮВАЛЬНА ТЕХНІКА В ТЕХНОЛОГІЧНИХ ПРОЦЕСАХ

УДК 004.891
DOI: 10.31891/2219-9365-2020-66-2-7

АНДРОЩУК О. С., ДЖУЛІЙ В. М.,
КЛЬОЦ Ю. П., МУЛЯР І. В.
Хмельницький національний університет

МОДЕЛЬ НЕЛЕГІТИМНОГО АБОНЕНТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ IP-ТЕЛЕФОНІЇ

У роботі запропонована імовірнісна модель виявлення нелегітимного абонента на основі алгоритму Діффі–Хелмана. Вирішує наступні задачі: надає можливість виявити активного нелегітимного абонента, який використовує програмне забезпечення синтезу голосу; визначити активного нелегітимного абонента IP-протоколів в каналах зв'язку Інтернет-телефонії при відсутності попередньо розподіленої секретної ключової інформації між кореспондентами, довіреного центру. Модель нелегітимного абонента може використовуватися при оцінці методів контролю рівня захищеності потоку даних з пакетною комутацією в Інтернет-телефонії, що надасть можливість забезпечення надійності IP-телефонії та підвищення захищеності.

Ключові слова: імовірнісна модель, нелегітимний абонент, інформаційна взаємодія, криптографічний захист, канали зв'язку.

ANDROSHCHUK O., DZHULIY V.,
KLOTS Y., MULYAR I.
Khmelnytsky National University

MODEL OF ILLEGAL SUBSCRIBER OF IP-TELEPHONY SECURITY PROVISION

The purpose of the work is cryptographic protection of information in IP telephony sessions, which will increase the level of security of voice flow over Internet networks and, based on the use of software key distribution, reduce the time of the session to establish a secure connection.

An analysis of possible active successful attacks (threats) and a study to identify their possible sources. Knowing the vulnerabilities and security level of the object for which protection is required, an active illegitimate subscriber can perform a combination of attacks, which can lead to unauthorized access to the data of the object.

Based on the analysis of algorithms of behavior of illegitimate subscribers, a model of the violator is proposed, which will take into account the level of capabilities of violators. The model of an illegitimate subscriber takes into account illegitimate operators who have the appropriate level of access to secure IP-telephony services: employees of this organization; software developers or suppliers of technical means, employees who provide improvement, maintenance, repair of means at the object on which protection of information resources is necessary. The purposes of illegitimate subscribers at carrying out active attack for the purpose of receiving unauthorized access to a stream of data of IP-telephony are defined. The ultimate goal of each active attack is to gain unauthorized access to the IP telephony data stream.

The illegitimate subscriber model can be used to evaluate methods of controlling the level of security of packet-switched data streams in Internet telephony, which provide the ability to ensure the reliability of IP telephony and increase security.

Keywords: probabilistic model, illegitimate subscriber, information interaction, cryptographic protection, communication channels.

Вступ. Поширення телефонії через Internet мережі поставило під загрозу прибутки операторів телефонних мереж. Проте, оператори AT&T, British Telecomunications, Deutsche Telecom, починають надавати послуги Internet-телефонії. Deutsche Telecom придбала частину Vocal Tec. Послугами передачі голосу через Internet мережі можна скористатися в багатьох містах і країнах. Аналогічні послуги передачі голосу через Internet мережі надають компанії Lucent, WorldPort, ITXC та ін. Найперспективнішими ринками передачі голосу через IP-мережі для IP-телефонії вважаються Австралія, США та Японія.

Поширенню IP-телефонії в Україні перешкоджає кілька факторів: не достатньо надійна інфраструктура Internet мереж каналів зв‘язку; не зацікавлені організації в розвитку IP-телефонії, які забезпечують телефонні мережі послугами зв‘язку. Таким чином, великі корпоративні компанії найбільш інтенсивно використовують IP-телефонію всередині. Лише кілька провайдерів надають послуги IP-телефонії – Infocom, IP Telecom, Sovam Teleport. Перевагою Internet-телефонії є низька вартість міжміських і міжнародних переговорів, дозволяє зменшити витрати на послуги передачі факсів і мультимедіа зв'язку, за рахунок цифрування і стиснення голосового потоку. Internet-телефонія не використовує на шляху передачі інформації пакетів з голосовим сигналом дороге устаткування. IP-телефонія – високоякісна технологія, не використовує дорогі комутатори-маршрутизатори.

Постановка задачі. Проведені дослідження показують існування декілька моделей нелегітимного абонента в IP-телефонії в Інтернет мережах. Імовірнісна модель нелегітимного абонента показує які дії та з використанням якого інструменту проводить нелегітимний абонент атаки при експлуатації захищеної IP-телефонії в Інтернет мережах. Імовірнісна модель нелегітимного абонента проводить аналіз та враховує різновиди атак, а також враховує особливості та характер атак на операційну систему Windows, з врахуванням використання операційною системою засобів захисту. Імовірнісна модель нелегітимного абонента не враховує програмний розподіл загальної секретної інформації (закритих ключів), з використанням IP – протоколів рознесення ключів IP-телефонії в Інтернет мережах[3]. Розглянута імовірнісна модель використовує попередній розподіл секретної інформації, тобто завчасна установка секрету учасникам сеансу. При застосуванні імовірнісної моделі нелегітимного абонента для здійснення атаки, задача якої отримання несанкціонований доступу до голосової інформації IP-технології в Інтернет мережах, вирішується тільки задача дешифрування переданого потоку даних при цьому використовується «атака в лоб» (метод перебору), вірогідність успішного завершення даної атаки достатньо низька при правильному вибору ключів сесії. Таким чином модифікація пакетів інформації можлива в разі успішної атаки, результатом якої є підбір пароля для реалізації процесу дешифрування перехоплених потоків даних.

Модель нелегітимного абонента наведена та описана в стандарті по питанням технічного та експортного контролю [1, 2]. У запропонованому стандарті наведений опис загальної моделі нелегітимного абонента. Описана в стандарті модель не враховує також особливостей роботи в Інтернет мережах захищеної IP-телефонії. Технологія IP-телефонії має в своєму розпорядженні в застосуванні IP – протоколи, які призначенні для підвищення ефективності та забезпечення безпеки IP-телефонії, сюди можна віднести захист сигналізації, розподіл загальної секретної інформації між учасниками сеансу зв'язку, захист голосової інформації, при цьому не наведено інформації про здійснення атак на IP-протоколи IP-телефонії. В проведеному аналізу робіт [7] рекомендуються загальні вимог, які ждуть бути запропонування до мережі IP-телефонії в Інтернет мережах, також наводиться опис загальних характеристик та виконуваних дій при здійсненні атак на мережу IP-телефонії. Рівень описаних атак відповідає діям середньостатистичного хакера при проведенні атак на сервіси IP-телефонії. На основі проведеного дослідження та аналізу відповідних робіт можна зробити наступний висновок: в розглянутих роботах не наводиться декомпозиція IP-протоколів Інтернет мереж безпечної IP-телефонії на відповідні складові, також не наведено опис успішних атак на IP-протоколи Інтернет мереж які безпосередньо використовуються в безпечній IP-телефонії. В розглянутих роботах [6] використовуються та описуються загальні підходи та принципи забезпечення підвищення надійності та захисту сервісів IP-телефонії, а також загальні підходи та принципи можливих дії нелегітимного абонента при атаках на сервіси IP-телефонії. В роботах не приділяється належної уваги атакам на протоколи розподілу загальної секретної інформації між учасниками сеансу зв'язку, захисту голосової інформації, при цьому не приводиться інформації про здійснення атак на IP-протоколи використовувані в IP-телефонії. Таким чином виникає необхідність розробки моделі нелегітимного абонента яка буде враховувати дії нелегітимного абонента, які були не враховані в розглянутих роботах, в існуючих моделях нелегітимного абонента, в першу чергу виникає необхідність прийняти до уваги декомпозиція IP-протоколів Інтернет-мереж, які використовуються безпечною IP-телефонії, запропонована модель має враховувати вказані особливості.

Основна частина. Моделі які описані в розглянутих роботах [1, 3] не дозволяють визначити імовірність успішної атаки на отримання несанкціонованою доступу до потоку даних в мережі захищеної IP-телефонії, яка працює в режимі за схемою точка – точка, також не надають механізмів виявлення та захисту від атак типу «зустріч по середині», розглянуті моделі не враховують даний тип атак. В запропоновану модель нелегітимного абонента необхідно включити додаткові механізми, такі як: виявлення імовірність успішної атаки на отримання несанкціонованого доступу до потоку даних захищеної IP-телефонії, яка працює в режимі за схемою точка – точка; також механізми виявлення та захисту від атак типу «зустріч по середині». Виникнення загроз в Інтернет мережах безпеки голосової інформації в IP-телефонії може проявитися в результаті виникнення додаткового каналу потоку інформації в Інтернет мережах між нелегітимним абонентом (джерелом загрози) і кореспондентом носієм інформації, при цьому необхідно створення відповідних умов, які сприяють для виникнення порушення захищеності та безпеки голосової інформації. Наскільки актуальна загроза порушення захищеності та безпеки голосової інформації буде оцінюватися, також, типом джерела загрози – рівнем атаки, рівнем захищеності джерела голосової інформації та наявністю вразливостей, а також рівнем захищеності середовища поширення голосового інформаційного сигналу.

Залежно від типу інформації на яку виконується атака можна виділити наступні джерела загроз: загрози, які пов'язані з діяльністю конкретної організації, організації які володіють оснащеністю і мотивацією, високим потенціалом; загрози що направлені і зумовлені економічними, політичними, військовими та іншими цілями іноземних держав; також загрози, пов'язані з діяльністю організацій, що володіють мотивацією, обумовленої їх економічними, інформаційними та іншими цілями; загрози, пов'язані з діяльністю окремих фізичних осіб (злочинних елементів).

Рівень впливу на закриту інформацію, яку необхідно захистити, визначається можливостями джерела загроз, наскільки джерело загроз володіє інформацією про сервіси захисту IP-телефонії, також рівень впливу на закриту інформацію визначається рівнем механізмів якими володіє джерело загроз. Джерело загроз, яке

здійснює дії (атаку) або займається підготовкою до дій (атаки) результатом яких є отримання несанкціонованого доступу до інформації з подальшим впливом на закриту інформацію є зловмисником інформаційної безпеки. В якості нелегітимного абонента будемо визначати фізичну особу, яка випадково чи не випадково здійснює дії (атаки) в своїх інтересах чи в інтересах даної організацій, чи в інтересах інших організацій (можливо іноземних організацій) результатом яких є порушення захищеності та безпеки інформаційних ресурсів при її обробці програмно-апаратними, технічними та іншими сервісами в інформаційних системах.

При розробці уточненої модель нелегітимного кореспондента більш доцільно розглядати зловмисників з точки зору рівня їх можливостей а також наявності прав несанкціонованого доступу до інформації, одноразового чи постійного. Таким чином модель нелегітимного кореспондента буде враховувати рівень можливостей зловмисників, до першого рівня віднесемо нелегітимних операторів які мають відповідний рівень доступу до сервісів безпечної IP-телефонії. До другого рівня віднесемо нелегітимних абонентів які не мають відповідного рівня доступу до сервісів безпечної IP-телефонії.

Таким чином нелегітимними операторами (перший рівень) можуть в даному випадку можуть виступати: працівники даної організації; розробники програмного забезпечення або постачальники технічних засобів, працівники які забезпечують удосконалення, супровід, ремонт засобів на об'єкті, на якому необхідний захист інформаційних ресурсів. До нелегітимних абонентів (другий рівень) можуть в даному випадку бути віднесені: сторонні особи; особи іноземних держав; представники іноземних розвідувальних служб; терористичні і кримінальні структури.

Одним з напрямів забезпечення безпеки передачі голосової інформації в Інтернет мережах захищеної IP-телефонії це використання криптографічних IP-протоколів SRTP. Протокол SRTP реалізує функції криптографічного захисту потоку даних. Також для забезпечення безпеки передачі голосової інформації в Інтернет мережах захищеної IP-телефонії виникає необхідність використання IP-протоколів програмного розподілу загальної секретної інформації (ключів) для сесій SRTP.

Враховуючи те, що передача голосової інформації в Інтернет мережах безпечної IP-телефонії здійснюється з використанням загального доступу, а монітори VoIP практично доступні будь-якій сторонній особі, як і легальний доступ до Інтернет-мереж – таким чином на основі сказаного можливо зробити висновок про актуальність виникнення загроз віддаленого доступу і можливості їх реалізації нелегітимними абонентами, як першого так і другого рівнів.

Реалізація моделі нелегітимного кореспондента безпечної IP-телефонії повинна бути конкретної, враховувати поведінку, властивості також характеристики конкретного об'єкту захисту VoIP. Виходячи з проведеного аналізу модель нелегітимного кореспондента безпечної IP-телефонії має враховувати структуру системи, сервіси безпеки також варіанти і способи використання ресурсів.

Існуючі моделі не враховують атаки на IP-протоколи розподілу загальної секретної інформації між учасниками сеансу зв'язку, захисту голосової інформації, відсутня інформації про здійснення атак на IP-протоколи використовувані в IP-телефонії, що складаються в застосуванні декількох протоколів для забезпечення безпеки, а також не описують атаки безпосередньо на ці протоколи.

Отже виникає необхідність розробки моделі нелегітимного абонента яка буде враховувати дії нелегітимного абонента, які були не враховані в розглянутих роботах, в існуючих моделях, в першу чергу виникає необхідність прийняти до уваги декомпозиція IP – протоколів Інтернет мереж, які використовуються безпечною IP-телефонії, модель повинна враховувати вказані особливості, мати механізми виявлення та захисту від атак типу «зустріч по середині». Для врахування в моделі вказаних недоліків розглянемо схему взаємодії кореспондентів захищеної IP-телефонії клієнт–клієнт, при відсутності попереднього програмного розподілення загального секретного матеріалу (закритого ключа сесії), і також розглянемо можливі варіанти дій нелегітимного абонента в схемі клієнт–клієнт (див. рис. 1).

Нелегітимний абонента може використовувати наступні сценарії виконання атак: здійснення пасивної атаки, при цьому використовує перехоплення переданих даних, без їх подальшої зміни; здійснення активної атаки, при цьому знаючи рівень системи захисту її вразливості, недоліки а також використовуючи штатні засоби системи захисту для проведення атаки з метою несанкціонованого доступу до даних з подальшою їх модифікацією, або отримання додаткових засобів для впливу на систему з метою подальшого виконання атаки.

Розглянемо модель нелегітимний абонента, який Інтернет мережах IP-телефонії буде використовувати сценарій активної атаки, направлену використанні вразливості IP - протоколу Діффі–Хелмана. IP-протокол Діффі-Хелмана схильний до атаки «зустріч посередині» що є суттєвим недоліком цих протоколів. Так як, IP-протокол Діффі–Хелмана лежить в основі більшості протоколів програмного розподілу секретного матеріалу (закритих ключів) то виникає необхідність більш детального приділення їм уваги. IP-протокол Діффі–Хелмана протокол захищає від атаки пасивного нелегітимного абонента, однак, він нестійкий до атаки активного нелегітимний абонента.

При здійсненні активної атаки нелегітимним абонентом необхідно враховувати можливий рівень прав порушника, так порушник може знаходитися в одній підмережі з об'єктом на який направлена атака, в даному випадку може мати достатньо прав для виконання успішної атаки, в іншому випадку порушник

може знаходитися не в одній підмережі з об'єктом на який направлена атака, в даному випадку може не мати достатньо прав для виконання успішної атаки.

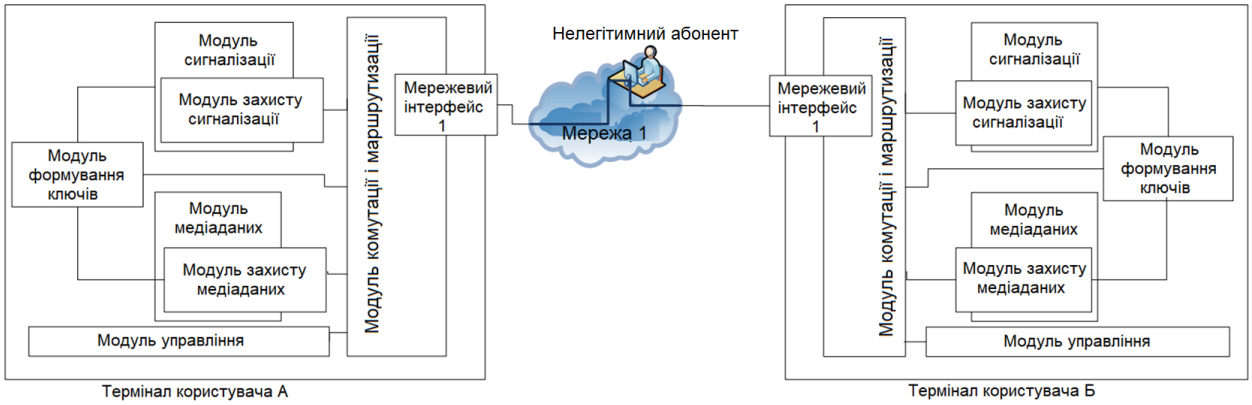


Рис. 1. Схема встановлення з'єднання в сценарії клієнт–клієнт

Під VoIP монітор абонента як правило мається на увазі, IP-телефон, шлюз безпечної IP-телефонії, стаціонарний комп'ютер, ноутбук, планшет, смартфон із встановленим для успішної взаємодії спеціалізованим програмним забезпеченням безпечної IP-телефонії. VoIP монітор надає можливість абонентам отримувати надавані послуги IP-телефонії, а також виконувати аудіо, відео виклики.

При проведені активних на VoIP монітор абонента будемо рахувати, що в одній підмережі з об'єктом захисту на який направлена атака може перебувати тільки нелегітимний оператор першого рівня.

Для отримання несанкціонованого доступу до сервісів IP телефонії нелегітимний абонент може використовувати для проведення успішної атаки наступні засоби і механізми: несанкціонований доступ на сервіси IP-телефонії, НСД може бути отриманий за рахунок атаки в лоб – перебору пароля; модифікація таблиці маршрутизації, часткове перенаправлення трафіку; виконання атаки «зустріч посередині» спеціалізований вплив на програмний розподіл загальної секретної інформації, а також на потоки даних, які передаються між абонентами IP-телефонії, мета даного типу атаки порушення конфіденційності і цілісності потоку даних; активна атака на шифр на переданий між абонентами, мета атаки – дешифрування даних і порушення конфіденційності; атака спрямована на програмне забезпечення одного або декількох абонентів, мета атаки – впровадження закладок в програмне забезпечення; активна атака з метою установка на вузлів оператора додаткового обладнання; активна атака на конфігураційні файли VoIP монітор, метою даної атаки є зміни налаштувань політики безпеки прийнятої в організації; активна атака направлена на перехоплення авторизаційних секретних даних, метою даної атаки є подальше управління обладнанням користувача, а також доступ до даних, які передаються між абонентами.

Для побудови математичної моделі нелегітимний абонента проведений аналіз можливих активних успішних атак (загроз) та проведено дослідження виявлення їх можливих джерел. Знаючи вразливості та рівень захищеності об'єкта, для якого необхідно провести захист, активний зловмисник може виконувати комбінацію атак, яка може привести до отримання несанкціонованого доступу до даних об'єкта.

Модель нелегітимного кореспондента буде враховувати рівень можливостей зловмисників, до першого рівня віднесемо нелегітимних операторів які мають відповідний рівень доступу до сервісів безпечної IP-телефонії. До другого рівня віднесемо нелегітимних абонентів які не мають відповідного рівня доступу до сервісів безпечної IP-телефонії.

Таким чином нелегітимними операторами (перший рівень) в даному випадку можуть виступати: працівники даної організації; розробники програмного забезпечення або постачальники технічних засобів, працівники які забезпечують удосконалення, супровід, ремонт засобів на об'єкті, на якому необхідний захист інформаційних ресурсів.

Визначмо цілі нелегітимних абонентів першого рівня при проведенні активної атаки з метою отримання несанкціонованого доступу до потоку даних IP-телефонії: $Ц_{ЗАХОБЛ}$ – захоплення обладнання оператора нелегітимним абонентом першого рівня; $Ц_{ЗАХМОН}$ – захоплення монітору абонента нелегітимним кореспондента першого рівня. Кінцевою метою кожної активної атаки є отримання несанкціонованого доступу до потоку даних IP-телефонії. На основі проведеного аналізу алгоритмів поведінки нелегітимних абонентів розпочнемо розробку моделі нелегітимного абонента першого рівня по кожній з перерахованих цілей.

Захоплення обладнання оператора нелегітимним абонентом першого рівня. Розглянемо модель нелегітимного абонента першого рівня, задачею якого є проведенні активної атаки з метою отримання несанкціонованого доступу до потоку даних IP-телефонії, результатом успішної активної атаки – захоплення обладнання оператора.

У порівнянні із нелегітимним абонентом другого рівня, нелегітимний абонента першого рівня має декілька переваг. На перших кроках виконання атаки він має певний рівень доступу на обладнання оператора зв'язку IP-телефонії, а також може мати можливість підключення і установки додаткового обладнання до мережі оператора IP-телефонії.

У випадку коли нелегітимний абонент не має достатнього рівня доступу на обладнання оператора, може спробувати отримати доступ, виконуючи атаку на перебір паролів для отримання більш високого рівня доступу до сервісів IP-телефонії. Алгоритм дій нелегітимного абонента першого рівня наведено на рис. 2. Імовірність $p_{18_{ЗАХОБЛ}}$ характеризує ймовірність, що у нелегітимного абонента першого рівня на початку виконання активної атаки є доступ відповідного рівня достатній для проведення подальших дій з метою отримання несанкціонованого доступу до потоку даних IP-телефонії. Імовірність $p_{18_{ЗАХОБЛ}}$ може бути визначена, наступним чином:

$$p_{18_{ЗАХОБЛ}} = \begin{cases} 1, якщо\ нелегітимний абонент\ має\ достатній\ рівень\ доступу; \\ 0, якщо\ нелегітимний абонент\ не\ має\ достатній\ рівень\ доступу. \end{cases}$$

Імовірність $p_{19_{ЗАХОБЛ}}$ відображає ймовірність події, у випадку коли нелегітимний абонент підключив своє необхідне обладнання в мережі оператора IP-телефонії на вузол, через який є доступ до даних (медіа-трафіку).

$$p_{19_{ЗАХОБЛ}} = \begin{cases} 1, якщо нелегітимний абонент змігвстановити своє обладнання \\ навузліоператора; \\ 0, якщо нелегітимний абонент незмігвстановити своє обладнання \\ навузліоператора. \end{cases}$$

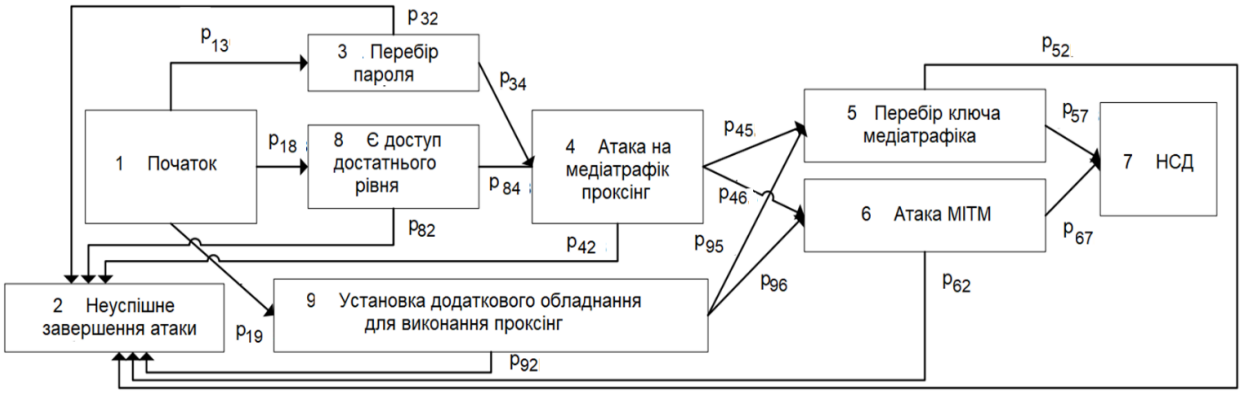


Рис. 2. Алгоритм дій при виконанні захоплення обладнання оператора нелегітимним абонентом

Обладнання, яке встановлюється нелегітимним абонентом повинно мати функціонал модифікації або віддзеркалення пакетів. Починаючи з цього моменту нелегітимний абонент для подальшого проведення активної атаки вибирає один з можливих наступних двох шляхів. Вибір продовження активної атаки залежить від встановленого обладнання та його технічних характеристик. Однак, навіть у випадку установки необхідного устаткування в нелегітимного абонента є ймовірність, що активна атака може бути проведена неуспішна. Наприклад, – це може відбутися, якщо захищаючий об'єкт почне використовувати додаткові сервіси та механізми IP-телефонії для відстеження атаки (вторгнення) нелегітимного абонента або додаткові IP-протоколи IP-телефонії, використання яких не було враховано при проведені активної атаки нелегітимним абонентом, і не враховані в обладнанні нелегітимного абонента.

На основі отриманих результатів, які отримані проведеним аналізом, можливих дій нелегітимного абонента побудований відповідний імовірнісний граф, представлений на рис. 3. У наведеному імовірнісному графі виділена гілка, яка відповідає успішному виконанню атаки, метою якої є отримання несанкціонованого доступу до потоку даних IP-телефонії і складена утворююча функція $H(x)$ цієї гілки. Для імовірнісного графа показаного на рис. 3 представлені $P_{НСД}$.

Для імовірнісного графа захоплення обладнання оператора, представлені $P_{НСД} = H(x = 1)$:

$$P_{НСДЦ_{ЗАХОБЛ}} = \left((p_{13}p_{34} + p_{18}p_{84})p_{45} + p_{19} + p_{95}\right)p_{57} + \left((p_{13}p_{34} + p_{18}p_{84})p_{46} + p_{19} + p_{96}\right)p_{67},$$

де p_{ij} – ймовірність переходу з вершини i графа у вершину j.

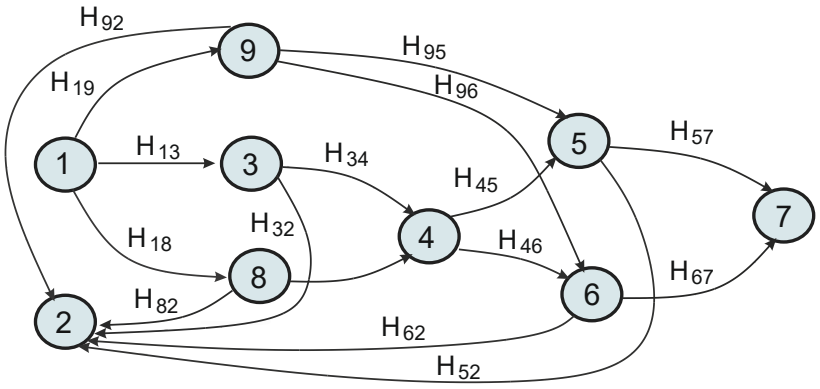


Рис. 3. Імовірнісний граф захоплення обладнання оператора нелегітимним абонентом першого рівня

Тоді ймовірність захисту від атаки несанкціонованого доступу до потоку даних IP-телефонії матиме наступний вигляд:

$$P_{ЗАХ\_НСДШ_{ЗАХОБЛ}} = 1 - P_{НСДШ_{ЗАХОБЛ}} = 1 - \Big((p_{13}p_{34} + p_{18}p_{84})p_{45} + p_{19} + p_{95}\Big)p_{57} + \\ + \Big((p_{13B}p_{34} + p_{18}p_{84})p_{46} + p_{19} + p_{96}\Big)p_{67},$$

де p_{13} – ймовірність вибору активної атаки перебір пароля для доступу нелегітимного абонента до обладнання оператора IP-телефонії; p_{18} – ймовірність наявності в нелегітимного абонента успішного доступу достатнього рівня на обладнання оператора IP-телефонії; p_{19} – ймовірність наявності в нелегітимного абонента можливості установки необхідного обладнання для успішного виконання атаки; p_{34} – ймовірність для нелегітимного абонента успішного завершення атаки по перебору пароля для доступу до обладнання оператора IP – телефонії Інтернет мереж; p_{45} – ймовірність вибору атаки нелегітимним абонентом «злом шифру» для проведення дешифрування захищеного потоку даних IP-телефонії; p_{46} – ймовірність вибору атаки нелегітимним абонентом на механізм програмного розподілу секретної інформації (ключів); p_{57} – ймовірність успішного завершення нелегітимним абонентом активної атаки «злом шифру» для проведення дешифрування захищеного потоку даних IP-телефонії; p_{67} – ймовірність успішного завершення атаки нелегітимним абонентом на механізм програмного розподілу секретної інформації (ключів); p_{95} – ймовірність вибору атаки нелегітимним абонентом «злом шифру» для проведення дешифрування захищеного потоку даних IP-телефонії; p_{96} – ймовірність вибору атаки нелегітимним абонентом на механізм програмного розподілу секретної інформації (ключів) між учасниками сесії.

Значення деяких ймовірностей, які використанні при опису імовірнісного графа захоплення обладнання оператора кореспондента нелегітимним абонентом, вимагають більш детальної оцінки експертами. Значення даних ймовірностей також залежать від нелегітимним абонентом, його рівня можливостей, рівня захисту та якості сервісів IP-телефонії.

Висновки. Проведений аналіз можливих активних успішних атак (загроз) та проведено дослідження виявлення їх можливих джерел. Знаючи вразливості та рівень захищеності об'єкта, для якого необхідно провести захист, активний нелегітимний абонент може виконувати комбінацію атак, яка може привести до отримання несанкціонованого доступу до даних об'єкта.

Запропонована модель нелегітимного кореспондента буде враховувати рівень можливостей зловмисників. Модель нелегітимного кореспондента першого рівня враховує нелегітимних операторів які мають відповідний рівень доступу до сервісів безпечної IP-телефонії: працівники даної організації; розробники програмного забезпечення або постачальники технічних засобів, працівники які забезпечують удосконалення, супровід, ремонт засобів на об'єкті, на якому необхідний захист інформаційних ресурсів.

Визначені цілі нелегітимних абонентів першого рівня при проведенні активної атаки з метою отримання несанкціонованого доступу до потоку даних IP-телефонії: $Ц_{ЗАХОБЛ}$ – захоплення обладнання оператора нелегітимним абонентом першого рівня; $Ц_{ЗАХМОН}$ – захоплення монітору абонента нелегітимним кореспондента першого рівня. Кінцевою метою кожної активної атаки є отримання несанкціонованого доступу до потоку даних IP-телефонії. На основі проведеного аналізу алгоритмів поведінки нелегітимних абонентів почнемо розроблено модель нелегітимного абонента першого рівня по кожній з перерахованих цілей.

Література

1. Про науково-технічну інформацію : Закон України з 25.06.1993 № 3322-XII. Дата оновлення: 19.04.2014. URL: http://zakon5.rada.gov.ua/laws/main/3322-12 (дата звернення: 02.09.2020).

2. Про захист інформації в інформаційно-телекомунікаційних системах : з Закону України від 05.07.1994 № 80/94-ВР. Дата оновлення: 04.07.2020. URL: http://zakon5.rada.gov.ua/laws/show/80/94-вр (дата звернення: 02.09.2020).

3. Бабаш, А.В. Криптографические методы защиты информации : учебник для студетнов вузов / А. В. Бабаш, Є. К. Баранова. - М. : КНОРУС, 2016. - 190 с.

4. Борисов, М.А. Основы для программно-аппаратной защиты информации : учеб. пособие для вузов / М. А. Борисов, И. В. Заводцев, И. В. Чижов. - 4-е изд., переработаное и доп. - М. : ЛЕНАНД, 2016. - 416 с.

5. Васильева, И. И. Криптографические методы защиты информации : практикум и учебник для академ. бакалавриата / И. И. Васильева. - Санкт-Петерб. гос. эконом. университет . - М. : Юрайт, 2017. - 349 с.

6. Нестеров, С.А. Основы информационной безопасности : учебник / С. А. Нестеров. - СПб. : Лань, 2017. – 423 с.

7. Олифер, В.Г. Безопасность компьютерных сетей / В. Г. Олифер, Н. А. Олифер. - М. : Горячая линия-Телеком, 2017. - 644 с.

8. Kim Peter. The Hacker Playbook 3: Practical Guide To Penetration Testing / Securety planet LLC 2018 359 p.

9. Шаньгин, В. Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. - М. : ДМК Пресс, 2017. - 702 с.

References

1. Pro naukovo-tekhnichnu informatsiyu : Zakon Ukrayiny vid [About scientific and technical information : Law of Ukraine from] 25.06.1993 № 3322-XII. Data onovlennya: 19.04.2014. URL: http://zakon5.rada.gov.ua/laws/main/3322-12 (data zvernennya: 02.09.2020).

2. Pro zakhyst informatsiyi v informatsiyno-telekomunikatsiynykh systemakh : Zakon Ukrayiny vid [On information protection in information and telecommunication systems : Law of Ukraine from] 05.07.1994 № 80/94-VR. Data onovlennya: 04.07.2020. URL: http://zakon5.rada.gov.ua/laws/show/80/94-вр (data zvernennya: 02.09.2020).

3. Babash, A.V. Kryptohrafycheskye metodы zashchytы ynformatsyy : uchebnyk dlia studetnov vuzov / A. V. Babash, Ye. K. Baranova. - M. : KNORUS, 2016. - 190 s.

4. Borysov, M.A. Osnovы dlia prohrammno-apparatnoi zashchytы ynformatsyy : ucheb. posobye dlia vuzov / M. A. Borysov, Y. V. Zavodtsev, Y. V. Chyzhov. - 4-e yzd., pererabotanoe y dop. - M. : LENAND, 2016. - 416 s.

5. Vasyleva, Y. Y. Kryptohrafycheskye metodы zashchytы ynformatsyy : praktykum y uchebnyk dlia akadem. bakalavryata / Y. Y. Vasyleva. - Sankt-Peterb. hos. эkonom. unyversytet . - M. : Yurait, 2017. - 349 s.

6. Nesterov, S.A. Osnovы ynformatsyonnoi bezopasnosty : uchebnyk / S. A. Nesterov. - SPb. : Lan, 2017. – 423 s.

7. Olyfer, V.H. Bezopasnost kompiuternыkh setei / V. H. Olyfer, N. A. Olyfer. - M. : Horiachaia lynyia-Telekom, 2017. - 644 s.

8. Kim Peter. The Hacker Playbook 3: Practical Guide To Penetration Testing / Securety planet LLC 2018 359 p.

9. Shanhyn, V. F. Ynformatsyonnaia bezopasnost y zashchyta ynformatsyy / V.F. Shanhyn. - M. : DMK Press, 2017. - 702 s.

Надійшла / Paper received: 07.07.2020 Надрукована / Paper Printed : 02.12.2020

УДК 004.057.4
DOI: 10.31891/2219-9365-2020-66-2-8

БЕЛЬФЕРР. Е., МЕДЗАТИЙ Д. М., ОМЕЛЬЧУК Р. В.
Хмельницький національний університет

ДОСЛІДЖЕННЯ ТА ЕКСПЕРИМЕНТАЛЬНІ ВСТАНОВЛЕННЯ ЕФЕКТИВНОСТІ ПРОТОКОЛУ КОНСЕНСУСУ PROOF-OF-ACTIVITY

У роботі проведено детальний аналіз відомих протоколів для реалізації в системах блокчейн. Виділено основні проблеми, які виникають в реальному використанні таких систем. Зокрема, це проблема енерговитрат та безпеки для користувачів. Пропонується новий соціально-орієнтований протокол, який дозволяє уникнути псевдодецентралізації та монополізації мережі, підвищити доступність системи, забезпечити безпеку учасників. Запропонований протокол передбачає створення та додавання нових блоків до блокчейну.

Розроблений алгоритм представлено узагальненими кроками і на основі нього можна створювати протокол. Враховуються принципи побудови розподілених систем та вимоги до архітектури таких систем. У процесі розробки запропонованого протоколу були опрацьовані основні аспекти безпеки, пов'язані із захистом від різних типів шкідливого програмного забезпечення, включаючи бот-мережі та комп'ютерні віруси.

Для застосування PoA мережа розроблена на архітектурі, особливістю якої є те, що вузли взаємодіють на різних рівнях відповідно до їх типізації або параметризації, що буде використано для виконання розробленого алгоритму та пошуку консенсусу.

Проведено оцінку системи, базованої на розробленому новому соціально-орієнтованому протоколі.

Ключові слова: розподілена система, протокол, мережа, блокчейн, архітектура системи.

BELFER R., MEDZATYI D., OMELCHUK R.
Khmelnytsky National University

RESEARCH AND EXPERIENTIAL ESTABLISHMENT OF PROOF-OF-ACTIVITY CONSENSUS PROTOCOL EFFICIENCY

The paper analyzes the analysis of known protocols for implementation in blockchain systems. The main problems that arise in the actual use of such systems are highlighted. In particular, this is a problem of energy consumption and safety for users.

The article proposes a new socially-oriented protocol that avoids pseudo-decentralization and monopolization of the network, increase the availability of the system, ensure the safety of participants. The proposed protocol involves creating and adding new blocks to the blockchain.

The developed algorithm is represented by generalized steps and on the basis of it it is possible to create the protocol. The principles of construction of distributed systems and requirements for the architecture of such systems are taken into account. In the process of developing the proposed protocol, the main aspects of security related to protection against various types of malware, including botnets and computer viruses, were addressed.

For PoA application, the network is developed on an architecture, the feature of which is that the nodes interact at different levels according to their typing or parameterization, which will be used to perform the developed algorithm and find consensus.

An evaluation of the system based on the developed new socially-oriented protocol was carried out.

Keywords: distributed system, protocol, network, blockchain, system architecture.

Вступ. Постановка задачі. Мережний протокол для створення децентралізованих систем для користувачів може бути одним з етапів впровадження нових принципів податкової локальної політики, де податки будуть прив’язані до активностей окремих членів громадськості, а також, оновлення виборчого права, що базуватиметься на соціальній активності учасників мережі та стане якісно новим принципом проведення нових, експериментальних але якісних виборів.

Розроблено багато таких протоколів. Частина з них активно використовується в системах блокчейн. Наявні протоколи постійно потребують вдосконалення, особливо в частині безпеки та використання енергоресурсів.

Пов’язані роботи. Технологія розподіленої книги стала надзвичайно популярною в 2018 році через надзвичайно високий курс криптовалюти. Блокчейн є однією з найважливіших галузей інформатики поряд з AI, IoT та хмарними компіляціями, які активно використовуються і розвиваються в останні роки. Відомі і поширені методи організації мереж блокчейнів є консенсусні протоколи – Proof-of-Work (PoW) та Proof-of-Stake (PoS). Але вони мають недоліки, які впливають на безпеку, швидкість роботи. доступність, масштабування та ефективне використання енергії. PoW має енергоефективність [2, 3]. Розробники протоколу PoS створювали його як альтернативу протоколу PoW [4] з певними перевагами перед протоколом PoW. Ці переваги: електроенергія не потрібна для вирішення головоломки, вузли зацікавлені в безпеці мережі, оскільки вони володіють монетами в ній, і швидші транзакції. Але він має проблему псевдодецентралізації [5], як і протокол PoW. Для розробки нового соціально орієнтованого протоколу, який дозволяє уникнути псевдодецентралізації та монополізації мережі, є захист від шкідливого програмного забезпечення,

включаючи бот-мережі та різні типи комп'ютерних вірусів [6–10]. Ці проблеми спонукають дослідників шукати нові протоколи, в яких таких проблем не буде.

Метою дослідження є розробка нового протоколу, який дозволяє уникнути псевдодецентралізації та монополізації мережі, а також проведення оцінки результатів.

Основна частина. Компанії NEM [11] та Mithril [12] працюють над блокчейнами на основі соціально-орієнтованих платформ, а не звичайних принципів Proof-of-Work і Proof-of-Stake. Вони розробили першу криптовалюту на основі консенсусного протоколу Proof-of-Importance (PoI) [13]. На створення транзакції потрібно 5 секунд, а на її обробку – 20 с. Мережа готова обробляти 3000 транзакцій в секунду [14].

Децентралізована платформа соціальних медіа Mithril [15] винагороджує кожного, хто створює медіа-контент. Використовуючи технологію блокчейну, Mithril може забезпечувати безпеку транзакцій, щоб захистити всіх залучених. Крім того, технологія розподілених даних зберігає надійні та недоторкані транзакції. Соціальний майнінг [16] спочатку використовувався Mithril для запуску процесу базової системної функціональності.

Консенсус-протокол Proof-of-Brain [16] розробила компанія Steem, який базується на діяльності користувачів і винагороджує виробництво високоякісного вмісту на конкретних платформах. Майнінг базується на «колективному інтелекті», що робить алгоритм «розумним» [17].

Basic Atttion Token [18] є соціально-орієнтованою технологією блокчейну. Браузерний браузер відстежує активність користувачів та їх взаємодію з опублікованою рекламою.

Проведений аналіз робіт [19–34] приводить до результату, що частина проблем пов’язаних з безпекою вирішена в певних протоколах, але це досягнуто за рахунок складності аутентифікації користувачів. Від такого результату частина користувачів не хочуть користуватись таким протоколом. При послабленні вимог безпеки відбувається втрата довіри зі сторони користувачів до такого ресурсу. Подальші використання таких протоколів не можуть бути основою для соціально-орієнтованих платформ. Тому, це питання потребує подальшого дослідження.

В роботі [35] пропонується варіант соціально-орієнтованого протоколу, який усуває частину важливих недоліків відомих протоколів. Консенсусний протокол Poof-of-Activity (PoA) дозволяє створювати нові блоки та додавати їх до блокчейну. Протокол PoA також вибирає вузли валідатора на основі значення активності вузла в мережі та будь-яких критеріїв, визначених конкретною системою блокчейнів. Для використання протоколу PoA мережа повинна бути спроектована відповідно до архітектури Layer Peer to Peer (LP2P). Алгоритм консенсусу PoA може бути впроваджений для будь-якої соціально орієнтованої структури: соціальних мереж, платформи краудфандингу, цивільних або муніципальних сайтів. Протокол PoA може бути використаний для створення муніципальних чи урядових платформ, які могли б об'єднати громадські ініціативи та допомогти реалізувати успішні.

Алгоритм роботи протоколу при створення нового блоку

Передумовою початку роботи алгоритму є наявність у множині вхідних транзакцій готових до запису у блок. Аналогічно до стандарту Bitcoin, розмір блоку транзакцій дорівнює 1 mb інформації. Отже, на вхід алгоритму подається така кількість транзакцій, що $\sum_{i=1}^{n} \text{size}_i = const_{size}$, де size – розмір транзакції, *N* – кількість транзакцій готових до запису в блок, $const_{size}$ – сталий розмір блоку транзакцій = 1 mb.

Узагальнені кроки алгоритму знаходження консенсусу між вузлами та виділення єдиного вузла валідатора, що матиме право здійснити створення блоку, його підпис та додавання до блокчейну.

Крок 1. Для множини з *N* рівнів [*A, B, C … N*], розміщених згідно мережевої архітектури LP2P, та множини вузлів кожного рівня, де вузол $a_i \in A, \text{де } i \leq k$, вузол $b_i \in B, \text{де } i \leq l$, вузол $c_i \in C, \text{де } i \leq k$,…, вузол $n_i \in N, \text{де } i \leq p$, для кожного з рівнів виконуються визначена функція відбору потенційного валідатора *f*. Отже, для множини рівнів [*A, B, C … N*] та множинам вузлів що належать кожному з рівнів, отримуємо множину функцій: $f_a(a_1, a_2, a_3 \dots a_k)$, $f_b(b_1, b_2, b_3 \dots b_l)$, $f_c(c_1, c_2, c_3 \dots c_m) \dots f_n(n_1, n_2, n_3 \dots n_p)$. Результатом виконання функції *f* для кожного з рівня з множини *[A, B, C … N]* та множини вузлів, що належать кожному з рівнів, є потенційний валідатор. Відповідно отримано результуючу множину потенційних валідаторів $[a', b', c' \dots n']$.

Крок 2. Множина потенційних валідаторів $[a', b', c' \dots n']$ використовується як параметр для функції випадкового визначення результуючого вузла валідатора – $random([a', b', c' \dots n'])$. Результатом виконання функції є кінцевий вузол *v* - визначений випадковим чином серед вузлів множини $[a', b', c' \dots n']$.

Крок 3. Кінцевий вузол *v* використовується як параметр для додавання блоку транзакцій до блокчейну та підпису цього блоку хеш значенням, отриманого в результаті попереднього виконання хеш функції, $block(v, T, hash)$, де *v* – вузол валідатор, *T* – множина валідних транзакцій готових до запису в блок, *hash* – хеш-ключ, яким буде підписано блок.

Кожний об'єкт розподіленої системи повинен мати певний набір атрибутів доступу, який включає унікальний ідентифікатор та іншу інформацію, що визначає його права доступу і/або права доступу до нього. Атрибут доступу використовується для опису інформації, яка використовується при керуванні доступом і зв'язана з користувачами, процесами або пасивними об'єктами. Відповідність атрибутів доступу і об'єкта може бути як явною, так і неявною. Атрибути доступу об'єкта є частиною його подання в архітектурі системи. Коли користувачі або процеси намагаються одержати доступ до пасивних об'єктів, механізми, що реалізують керування доступом, на підставі політики безпеки і перевірки атрибутів доступу можуть «прийняти рішення» про легальність запиту. Використовуючи набір атрибутів доступу відповідно до прийнятої політики безпеки, можна реалізувати довірче керування доступом, адміністративне, контроль за цілісністю та інші види керування доступом.

Для відображення функціональності розподіленої системи у простір, в якому не розглядаються права власності, використовується концепція матриці доступу. Матриця доступу є таблицею, уздовж кожного виміру якої відкладені ідентифікатори об'єктів, а в якості елементів матриці виступають дозволені або заборонені режими доступу. Матриця доступу може бути двомірною (наприклад, користувачі/пасивні об'єкти або процеси/пасивні об'єкти) або тримірною (користувачі/процеси/пасивні об'єкти). Матриця доступу може бути повною, тобто містити вздовж кожної з осей ідентифікатори всіх існуючих на даний час об'єктів КС даного типу, або частковою. Повна тримірна матриця доступу дозволяє точно описати, хто (ідентифікатор користувача), через що (ідентифікатор процесу), до чого (ідентифікатор пасивного об'єкта), який вид доступу може одержати.

Програмні компоненти з погляду користувачів КС можна розділити на дві категорії: компоненти без внутрішнього стану, що зберігається між віддаленими викликами своїх методів (stateless components); компоненти із внутрішнім станом, що зберігається між віддаленими викликами своїх методів (statefull components). Під станом у цьому випадку розумітимемо сукупність значень полів об'єктів, що реалізують компоненти, що зберігаються в пам'яті адміністратора. Якщо компонента в ході своєї роботи зберігає які-небудь дані в зовнішньому сховищі, наприклад у базі даних або черги повідомлень, це звичайно не розглядається як її внутрішній стан. Модель єдиного виклику не зберігає стану віддаленого об'єкта між викликами його методів, у силу чого дана модель може використовуватися тільки з розподіленими компонентами без внутрішнього стану. Модель одного екземпляра може бути використана для виклику компонентів із внутрішнім станом. Модель активації по запиту компонента може бути використана з будь-якими компонентами, але для компонент без внутрішнього стану такий підхід звичайно призводить до непродуктивного використання пам'яті при деякому виграші у витратах часу процесора в порівнянні з моделлю одного виклику. Компоненти без збереження внутрішнього стану, що використовуються разом з моделлю єдиного виклику з пулом об'єктів, мають найбільші можливості масштабування системи при оптимальному балансі між витратами пам'яті й навантаженням на процесор.

Таким чином, розроблений протокол, алгоритм та вимоги до архітектури системи на основого нового соціально-орієнтованого протоколу дозволяють вирішити ряд проблеми безпеки.

Експерименти та оцінка. Протокол консенсусу Proof-of-Activity та алгоритм додавання нових блоків до блокчейну базується на 3-рівневому наборі тексту [35].

На рис. 1 показано розрахункове споживання електроенергії, що використовується різними консенсусними протоколами. Протоколи консенсусу PoA та PoB мають нульове розрахункове споживання електроенергії. У той же час протокол PoW вимагає найбільшої кількості електроенергії. Протоколи PoS та PoI можуть вимагати певного споживання електроенергії на початкових етапах, якщо для початкового видобутку використовується алгоритм PoW.

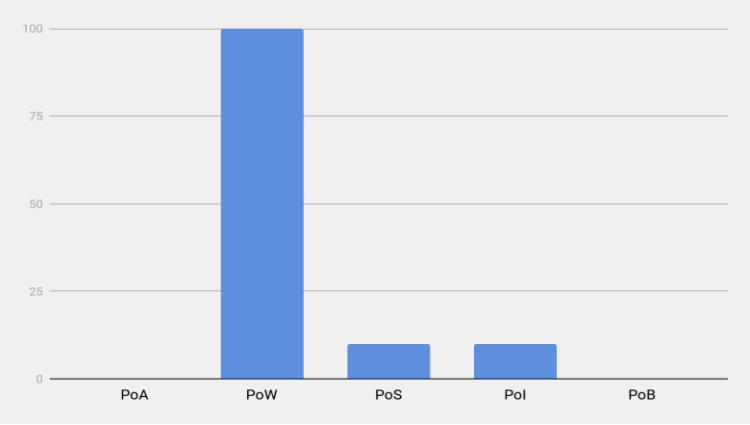


Рис. 1. Розрахункове споживання електроенергії, яке вимагається різними консенсусними протоколами

У таблиці 1 порівнюється протокол консенсусу Proof-of-Activity з деякими найпопулярнішими та найрелевантнішими протоколами. Для порівняння були розглянуті такі критерії, як споживання електроенергії, децентралізація, моніторинг діяльності, соціальна орієнтація, масштабованість, труднощі в приєднанні до мережі тощо.

Таблиця 1

Порівняння протоколів консенсусу

Критерій	PoA	PoW	PoS	PoI	PoB
Споживання електроенергії	–	+	+/–	+/-	–
Питання псевдодецентралізації	–	+/–	+	–	–
Монополізація ресурсів	–	+	+	+/–	–
Легко приєднатися	+	+/–	–	+/–	+
Моніторинг діяльності	+	–	–	+/–	+
Соціальна спрямованість	+	–	–	–	+
Масштабованість	+	+	+	+	+
Широке застосування	+	+	+	+	–
Потрібне початкове володіння монетами	–	–	+	+	–

Протокол PoB найбільш подібний до протоколу Proof-of-Activity: він соціально орієнтований, уникає псевдодецентралізації, не вимагає первинного володіння монетами та не вимагає багато електроенергії. Основна відмінність між протоколами PoA та PoB полягає в тому, що PoB може використовуватися лише для медіа-мереж – він вимагає оцінки та голосування вмісту. З іншої сторони, протокол PoA може використовуватися для немедіа-мереж, таких як платформи для краудфандингу, муніципальні сайти та ресурси для управління проектами.

Висновки. Розроблено новий соціально орієнтований протокол, основними задачами якого є уникнення псевдо-децентралізації та монополізації мережі, збільшення доступності участі у підтримці роботи системи для всіх активних вузлів мережі. Він покращує безпеку. Також, розроблено вимоги до розподіленої системи та алгоритм за яким функціонуватиме система.

Напрямком подальших досліджень є розробка складових архітектури мережної системи та методів взаємодії компонентів системи.

Література

1. Nakamoto, S.: Bitcoin: “A Peer-to-Peer Electronic Cash System”. Available: https://bitcoin.org/bitcoin.pdf.
2. Ethereum Energy Consumption Index. Available: https://digiconomist.net/ethereum-energy-consumption.
3. Bitcoin Energy Consumption Index. Available: https://digiconomist.net/bitcoin-energy-consumption.
4. “A Next-Generation Smart Contract and Decentralized Application Platform.” Available: https://github.com/ethereum/wiki/wiki/White-Paper.
5. “Redefining Internet Protocols Through Effective Decentralization”, Available: https://hackernoon.com/redefining-internet-protocols-through-effective-decentralization-b2afbcb874d9.
6. Savenko, O., Nicheporuk, A., Hurman I., Lysenko, S.: Dynamic Signature-based Malware Detection Technique Based on API Call Tracing. CEUR Workshop, Vol. 2393, pp. 633–643 (2019).
7. Lysenko, S., Savenko, O., Kryshchuk, A., Kljots, Y. Botnet detection technique for corporate area network. In: Proc. of the 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems, pp. 363-368 (2013).
8. Savenko, O., Lysenko, S., Kryschuk, A.: Multi-agent based approach of botnet detection in computer systems. Communications in Computer and Information Science, Vol. 291, pp.171-180 (2012).
9. Pomorova, O., Savenko, O., Lysenko, S., Kryshchuk, A. and Nicheporuk, A.: A technique for detection of bots which are using polymorphic code. In: 21st International Conference, CN, Springer, Brunów, Poland, pp. 265-276 (2014)
10. Kehret, O., Walz, A., Sikora, A.: Integration of Hardware Security Modules into a Deeply Embedded TLS Stack. International Journal of Computing, Vol. 15, Issue 1, pp. 24-32 (2016).
11. NEM, New Economy Movement. Available: https://nem.io/.
12. Mithril, The Future of Social Networks. Available: https://mith.io/.
13. “What is PoI?” Available: https://docs.nem.io/ja/gen-info/what-is-poi.
14. Introduction to NEM (XEM): The Proof-of-Importance Coin. Available: https://cryptoslate.com/nem/.
15. Proof of Importance Explained. Available: https://www.mycryptopedia.com/proof-of-importance/.
16. Beginner’s Guide to Mithril: Social Platform Which Rewards Content Creators. Available: https://blockonomi.com/mithril-guide/.
17. Huang, J.: The Future of Social Networks. Mithril (MITH) Whitepaper, pp. 1-30.
18. Blockchain White Paper, China Academy of Information and Communication Technology, Trusted Blockchain Initiatives, pp. 1-49 (2018).
19. BlockChain Technology Beyond Bitcoin. Available: https://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf.
20. Blockchain disruption and smart contracts. Available: https://www.nber.org/papers/w24399.pdf.
21. Blockchain in Trade Facilitation. Available: http://www.unece.org/fileadmin/DAM/cefact /GuidanceMaterials/WhitePaper/Blockchain.pdf.
22. Blockchain Consensus Protocols in the Wild. arXiv:1707.01873, pp. 1-24 (2017)
23. Wahab, A., Memood, W.: Survey of Consensus Protocols. arXiv:1810.03357, pp. 1-12 (2018).
24. Schwartz, D., Youngs, N., Britto, A.: The Ripple Protocol Consensus Algorithm. Ripple Labs, Inc. White Paper; Ripple Labs, Inc.: San Francisco, CA, USA, Vol. 5, pp. 1-8. (2014).
25. Daian, P., Pass, R., Shi, E.: Snow White: Provably Secure Proofs of Stake, Cryptology ePrint Archive, Report 2016/919, pp. 1-62 (2016).
26. Buterin, V.: Slasher: A punitive proof-of-stake algorithm. Available: https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm/.

27. Chen, J., Micali, S.: Algorand: the efficient and democratic ledger, arXiv: 1607.01341 (2016).
28. Proof of Stake FAQ. Available: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ
29. Analysis of the main consensus protocols of blockchain. Available: https://www.sciencedirect.com/science/article/pii/S240595951930164X
30. Mazieres, D.: Stellar Consensus Protocol. Available: https://www.stellar.org/papers/stellar-consensus-protocol
31. Basic Attention Token (BAT) Blockchain Based Digital Advertising, Available: https://basicattentiontoken.org/wpcontent/uploads/ 2017/05/BasicAttentionTokenWhitePaper-4.pdf
32. SMT Whitepaper. A technical paper on the proposed Smart Media Tokens protocol. Available: https://steem.com/wp-content/uploads/2018/11/smt-whitepaper-nov-3-2018.pdf
33. Proof of Brain Bluepaper. Available: https://steem.com/steem-bluepaper.pdf
34. Basic Attention Token. "Introducing blockchain based digital advertising". Available: https://basicattentiontoken.org/.
35. Belfer R. Proof-of-Activity Consensus Protocol Based on a Network's Active Nodes / R. Belfer, A. Kashtalian, A. Nicheporuk, A. Sachenko, G. Markovsky – CEUR-WS. – 2020. Vol. 2623. – Pp.239-251.

References

1. Nakamoto, S.: Bitcoin: "A Peer-to-Peer Electronic Cash System". Available: https://bitcoin.org/bitcoin.pdf.
2. Ethereum Energy Consumption Index. Available: https://digiconomist.net/ethereum-energy-consumption.
3. Bitcoin Energy Consumption Index. Available: https://digiconomist.net/bitcoin-energy-consumption.
4. "A Next-Generation Smart Contract and Decentralized Application Platform." Available: https://github.com/ethereum/wiki/wiki/White-Paper.
5. "Redefining Internet Protocols Through Effective Decentralization", Available: https://hackernoon.com/redefining-internet-protocols-through-effective-decentralization-b2afbcb874d9.
6. Savenko, O., Nicheporuk, A., Hurman I., Lysenko, S.: Dynamic Signature-based Malware Detection Technique Based on API Call Tracing. CEUR Workshop, Vol. 2393, pp. 633–643 (2019).
7. Lysenko, S., Savenko, O., Kryshchuk, A., Kljots, Y. Botnet detection technique for corporate area network. In: Proc. of the 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems, pp. 363-368 (2013).
8. Savenko, O., Lysenko, S., Kryschuk, A.: Multi-agent based approach of botnet detection in computer systems. Communications in Computer and Information Science, Vol. 291, pp.171-180 (2012).
9. Pomorova, O., Savenko, O., Lysenko, S., Kryshchuk, A. and Nicheporuk, A.: A technique for detection of bots which are using polymorphic code. In: 21st International Conference, CN, Springer, Brunów, Poland, pp. 265-276 (2014)
10. Kehret, O., Walz, A., Sikora, A.: Integration of Hardware Security Modules into a Deeply Embedded TLS Stack. International Journal of Computing, Vol. 15, Issue 1, pp. 24-32 (2016).
11. NEM, New Economy Movement. Available: https://nem.io/.
12. Mithril, The Future of Social Networks. Available: https://mith.io/.
13. "What is PoI?" Available: https://docs.nem.io/ja/gen-info/what-is-poi.
14. Introduction to NEM (XEM): The Proof-of-Importance Coin. Available: https://cryptoslate.com/nem/.
15. Proof of Importance Explained. Available: https://www.mycryptopedia.com/proof-of-importance/.
16. Beginner's Guide to Mithril: Social Platform Which Rewards Content Creators. Available: https://blockonomi.com/mithril-guide/.
17. Huang, J.: The Future of Social Networks. Mithril (MITH) Whitepaper, pp. 1-30.
18. Blockchain White Paper, China Academy of Information and Communication Technology, Trusted Blockchain Initiatives, pp. 1-49 (2018).
19. BlockChain Technology Beyond Bitcoin. Available: https://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf.
20. Blockchain disruption and smart contracts. Available: https://www.nber.org/papers/w24399.pdf.
21. Blockchain in Trade Facilitation. Available: http://www.unece.org/fileadmin/DAM/cefact /GuidanceMaterials/WhitePaper/Blockchain.pdf.
22. Blockchain Consensus Protocols in the Wild. arXiv:1707.01873, pp. 1-24 (2017)
23. Wahab, A., Memood, W.: Survey of Consensus Protocols. arXiv:1810.03357, pp. 1-12 (2018).
24. Schwartz, D., Youngs, N., Britto, A.: The Ripple Protocol Consensus Algorithm. Ripple Labs, Inc. White Paper; Ripple Labs, Inc.: San Francisco, CA, USA, Vol. 5, pp. 1-8. (2014).
25. Daian, P., Pass, R., Shi, E.: Snow White: Provably Secure Proofs of Stake, Cryptology ePrint Archive, Report 2016/919, pp. 1-62 (2016).
26. Buterin, V.: Slasher: A punitive proof-of-stake algorithm. Available: https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm/.
27. Chen, J., Micali, S.: Algorand: the efficient and democratic ledger, arXiv: 1607.01341 (2016).
28. Proof of Stake FAQ. Available: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ
29. Analysis of the main consensus protocols of blockchain. Available: https://www.sciencedirect.com/science/article/pii/S240595951930164X
30. Mazieres, D.: Stellar Consensus Protocol. Available: https://www.stellar.org/papers/stellar-consensus-protocol
31. Basic Attention Token (BAT) Blockchain Based Digital Advertising, Available: https://basicattentiontoken.org/wpcontent/uploads/2017/05/BasicAttentionTokenWhitePaper-4.pdf
32. SMT Whitepaper. A technical paper on the proposed Smart Media Tokens protocol. Available: https://steem.com/wp-content/uploads/2018/11/smt-whitepaper-nov-3-2018.pdf
33. Proof of Brain Bluepaper. Available: https://steem.com/steem-bluepaper.pdf
34. Basic Attention Token. "Introducing blockchain based digital advertising". Available: https://basicattentiontoken.org/.
35. Belfer R. Proof-of-Activity Consensus Protocol Based on a Network's Active Nodes / R. Belfer, A. Kashtalian, A. Nicheporuk, A. Sachenko, G. Markovsky – CEUR-WS. – 2020. Vol. 2623. – Pp.239-251.

Надійшла / Paper received: 15.09.2020 Надрукована / Paper Printed : 01.12.2020

УДК 004.3
DOI: 10.31891/2219-9365-2020-66-2-9

БАБЧУК С. М., РОМАНІВ І. Т.
Івано-Франківський національний технічний університет нафти і газу

МАТЕМАТИЧНІ МОДЕЛІ ВАРТОСТІ ОБЧИСЛЕННЯ 1 ГФЛОПС КЛАСТЕРНОЮ СИСТЕМОЮ НА БАЗІ RASPBERRY PI 3B+

На сьогодні суперкомп'ютери забезпечують високу швидкодію за допомогою паралельних обчислень великих об'ємів даних. Проте вони дуже дорогі, складні в розробці, і потребують дуже багато електроенергії для живлення та охолодження. Розробка програм, які забезпечують розпаралелення виконання завдань, є дуже важливою в організації ефективної роботи суперкомп'ютерів. Оскільки для роботи з суперкомп'ютерами відводяться обмежені невеликі інтервали часу, то для розробника програми важливо бути впевненим, що вона буде правильно працювати в реальному багатопроцесорному середовищі, а розпаралелювання задач буде відбуватися належним чином. Для тестування та відлагоджування програм написаних для виконання на суперкомп'ютерах, навчання студентів програмування для реального багатопроцесорного середовища зараз є актуальною розробка кластерних систем з дешевих одноплатних комп'ютерів Raspberry Pi. Під час попередніх досліджень кластерних систем на базі одноплатних комп'ютерів Raspberry Pi основна увага приділялася їх продуктивності. Проте, важливо також знати вартість обчислення 1 Гфлопс кластерною системою, адже цей показник впливає на загальну ефективність роботи такої системи. Для проведення експериментів було розроблено кластерну систему з одноплатних комп'ютерів Raspberry Pi 3B+. З метою визначення вартості обчислення 1 Гфлопс кластерною системою на базі одноплатних комп'ютерів Raspberry Pi 3B+ при різних конфігураціях кластера під час експериментів проводилась зміна кількості плат в кластері від двох до чотирьох а також використовувались різні підходи до охолодження кластерної системи. Для забезпечення отримання достовірних даних про вартість обчислення 1 Гфлопс кластерною системою на базі одноплатних комп'ютерів Raspberry Pi 3B+ при різній кількості плат Raspberry Pi 3B+ в ній та при різних підходах до охолодження кластера було проведено по 49 однотипних досліди для кожної конфігурації кластеру. В результаті проведених досліджень розроблено математичні моделі залежності вартості обчислення 1 Гфлопс кластерною системою на базі одноплатних комп'ютерів Raspberry Pi 3B+ від кількості плат Raspberry Pi 3B+ в ній при різних підходах до охолодження кластера. Визначені особливості та залежності зміни вартості обчислення 1 Гфлопс кластерною системою на базі одноплатних комп'ютерів Raspberry Pi 3B+ від кількості плат Raspberry Pi 3B+ в ній, при різних підходах до охолодження кластера, що дозволить в подальшому вибирати конфігурацію кластерної системи, яка забезпечить її ефективну роботу.

Ключові слова: математична модель, кластерна система, кластер, Raspberry Pi 3B+, вартість обчислення 1 Гфлопс.

BABCHUK S., ROMANIV I.
Ivano-Frankivsk National Technical University of Oil and Gas

MATHEMATICAL MODELS COST OF CALCULATION 1 GFLOPS CLUSTER SYSTEM BASED ON RASPBERRY PI 3B+

Nowadays, supercomputers provide high performance with parallel computing of large amounts of data. However, they are very expensive, difficult to develop, and require a lot of electricity to power and cool. Developing programs that provide parallel tasks is very important in organizing the efficient operation of supercomputers. Because there are limited time intervals for working with supercomputers, it is important for the developer of the program to be sure that it will work properly in a real multiprocessor environment, and the parallelization of tasks will take place properly. To test and debug programs written for execution on supercomputers, teaching students programming for a real multiprocessor environment, it is now important to develop cluster systems from cheap Raspberry Pi single-board computers. Previous research on Raspberry Pi single-board cluster systems has focused on their performance. However, it is also important to know the cost of calculating 1 Gflops cluster system, because this indicator affects the overall efficiency of such a system. A cluster system of Raspberry Pi 3B+ single-board computers was developed for the experiments. In order to determine the cost of computing 1 Gflops cluster system based on single-board computers Raspberry Pi 3B+ in different cluster configurations during the experiments, the number of boards in the cluster was changed from two to four and different approaches to cooling the cluster system were used. To provide reliable data on the cost of computing 1 Gflops cluster system based on single-board computers Raspberry Pi 3B+ with different number of Raspberry Pi 3B+ boards in it and with different approaches to cooling the cluster, 49 similar experiments were performed for each cluster configuration. As a result of the research, mathematical models of the dependence of the cost of calculating 1 Gflops cluster system based on single-board computers Raspberry Pi 3B+ on the number of Raspberry Pi 3B+ boards in it with different approaches to cluster cooling have been developed. Features and dependences of change of cost of calculation of 1 Gflops by the cluster system on the basis of single-board computers Raspberry Pi 3B+ on quantity of boards of Raspberry Pi 3B+ in it, at various approaches to cooling of a cluster are defined that will allow to choose the best configuration that will ensure efficient operation.

Keywords: mathematical model, cluster system, cluster, Raspberry PI 3B+, cost of calculating 1 Gflops.

Постановка проблеми. На сьогодні суперкомп'ютери забезпечують високу швидкодію за допомогою паралельних обчислень великих об'ємів даних. Проте вони дуже дорогі, складні в розробці, і потребують дуже багато електроенергії для живлення та охолодження [1].

Суперкомп'ютер Fugaku встановлений в Центрі обчислювальної науки RIKEN в японському місті Кобе. Розробка даного суперкомп'ютера розпочалась ще в 2014 році. Введення в повноцінну експлуатацію на запланованій потужності має відбутись тільки в 2021 році. Проте частина комп'ютера була введена в експлуатацію в червні 2020 р. В червні 2020 р. суперкомп'ютер Fugaku випередив інший суперкомп'ютер

Summit та став першим номером в переліку ТОП500 [2]. Таким чином розробка суперкомп'ютера Fugaku має скласти 7 років.

Суперкомп'ютер Summit (OLCF-4) розроблений компанією IBM для Oak Ridge National Laboratory. З 8 червня 2018 р. він був найпотужнішим суперкомп'ютером у світі та утримував першість до червня 2020 р., коли поступився суперкомп'ютеру Fugaku. Суперкомп'ютер Summit охолоджується системою, в якій циркулює 15150 л очищеної води. Необхідно відмітити, що суперкомп'ютер Summit споживає 15 МВт енергії, якої вистачило б на постачання 8100 середньостатистичних житлових будинків [3].

Науковці, програмісти, студенти майже не мають можливості працювати на суперкомп'ютерах і запускати на них розроблені ними програми. Як правило, суперкомп'ютери неперервно задіяні для виконання програм великих корпорацій та урядів великих держав. Дуже складно одержати дозвіл на роботу з суперкомп'ютером. Зазвичай, потрібно наперед написати звернення і очікувати в черзі на допуск до роботи із суперкомп'ютером [1]. Розробка програм, які забезпечують розпаралелення виконання завдань, є дуже важливою в організації максимально ефективної роботи дуже дорогих суперкомп'ютерів. Оскільки для роботи з суперкомп'ютерами відводяться обмежені невеликі інтервали часу, то для розробника програми важливо бути впевненим, що вона буде правильно працювати в реальному багатопроцесорному середовищі, а розпаралелювання задач буде відбуватися належним чином [1].

Аналіз останніх досліджень і публікацій. Сьогодні великі компанії та науково-дослідні організації в пошуку дешевих та простих комп'ютерних систем на яких вони могли б тестувати та відлагоджувати програми написані для виконання на суперкомп'ютерах. Також провідні університети світу в пошуку дешевих та простих комп'ютерних систем на яких можна б було навчати студентів програмування для реального багатопроцесорного середовища.

Професор Simon Cox з університету Southampton (Великобританія) створив кластерну систему з 64 одноплатних комп'ютерів Raspberry Pi. Вартість даної системи склала 4000 дол. США [4]. В праці "Iridis-pi: a low-cost, compact demonstration cluster" вказано, що кластери подібні до вищевказаних є ідеальним ресурсом для освітнього використання, щоб надихнути студентів, які вивчають основи високопродуктивних та наукових обчислень. Інші вчені та компанії також займались створенням кластерних систем на базі одноплатних комп'ютерів Raspberry Pi [5–11]. Зазвичай, створювались кластерні системи на базі 4, 8, 32, 64 одноплатних комп'ютерів Raspberry Pi.

Необхідно відмітити, що розробка кластерних систем на базі дешевих одноплатних комп'ютерів Raspberry Pi зацікавила не тільки університети, як дешева база для навчання студентів програмуванню для реального багатопроцесорного середовища. До таких пошуків та розробок долучились великі всесвітньовідомі компанії як Oracle та Лос-Аламоська національна лабораторія в США. В 2019 році компанія Oracle представила розроблений нею кластер з 1060 одноплатних комп'ютерів Raspberry Pi 3B+ [5]. А в Лос-Аламоській національній лабораторії було створено кластер з 1000 одноплатних комп'ютерів Raspberry Pi 3 вартістю 150 тис. дол. США [1]. Розроблений кластер в Лос-Аламоській національній лабораторії використовується для тестування програмного забезпечення, яке в подальшому має бути запущено на суперкомп'ютері Trinity, який теж експлуатується в Лос-Аламоській національній лабораторії. Звичайно, що вартість кластеру розробленого для даної лабораторії є досить високою, але вона значно менша вартості суперкомп'ютері Trinity. Крім того, кластер з 1000 одноплатних комп'ютерів Raspberry Pi 3 споживає значно менше електроенергії чим суперкомп'ютері Trinity (25 МВт на живлення та вдвічі більше на охолодження).

При вище проаналізованих дослідженнях кластерних систем на базі одноплатних комп'ютерів Raspberry Pi основна увага приділялася їх продуктивності. Проте, важливо також знати вартість обчислення 1 Гфлопс кластерною системою, адже цей показник впливає на загальну ефективність роботи такої системи.

Мета досліджень. Мета роботи полягає у встановленні вартості обчислення 1 Гфлопс кластерною системою на базі одноплатних комп'ютерів Raspberry Pi 3B+ при різній кількості плат в кластері і при різних системах охолодження та розробка математичних моделей зміни вартості обчислення 1 Гфлопс кластерною системою на базі Raspberry Pi 3B+ залежно від різної кількості плат в ній та при різних системах охолодження.

Визначення вартості обчислення 1 Гфлопс кластерною системою на базі одноплатних комп'ютерів Raspberry Pi 3B+. Для проведення експериментів було розроблено кластерну систему з чотирьох одноплатних комп'ютерів Raspberry Pi 3B+, гігабітного некерованого комутатора D-Link DGS-1005A, блоку живлення 60 W, кулера DeepCool XFAN 120 L/W.

З метою визначення вартості обчислення 1 Гфлопс кластерною системою на базі одноплатних комп'ютерів Raspberry Pi 3B+ при різних конфігураціях кластера під час експериментів проводилась зміна кількості плат в кластері від двох до чотирьох а також використовувались різні підходи до охолодження кластерної системи:

– без охолодження;

– з пасивним охолодженням;

– з активним охолодженням за допомогою кулера DeepCool XFAN 120 L/W.

Для забезпечення отримання достовірних даних про вартість обчислення 1 Гфлопс кластерною системою на базі одноплатних комп'ютерів Raspberry Pi 3B+ при різній кількості плат Raspberry Pi 3B+ в ній та при різних підходах до охолодження кластера було проведено по 49 однотипних досліди для кожної конфігурації кластеру.

Вартість обчислення 1 Гфлопс кластерною системою на базі одноплатних комп'ютерів Raspberry Pi 3B+ досліджувалась за даними, які були отримані при проведенні тесту "High performance challenge benchmark" [12].

Під час виконання тесту "High performance challenge benchmark" кластерною системою на базі чотирьох одноплатних комп'ютерів Raspberry Pi 3B+ при використанні різних підходів до охолодження кластера було визначено вартість обчислення 1 Гфлопс (рис. 1).

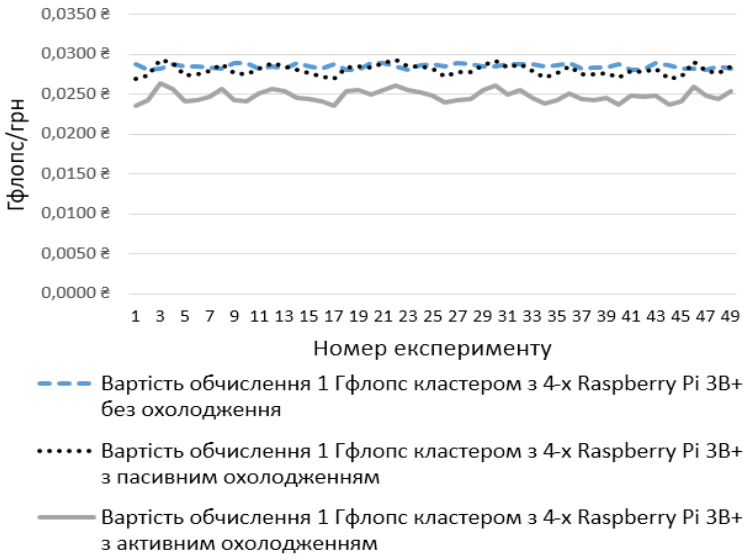


Рис. 1. Вартість обчислення 1 Гфлопс кластерною системою на базі чотирьох одноплатних комп'ютерів Raspberry Pi 3B+ під час виконання тесту "High performance challenge benchmark" та при використанні різних підходів до охолодження кластера

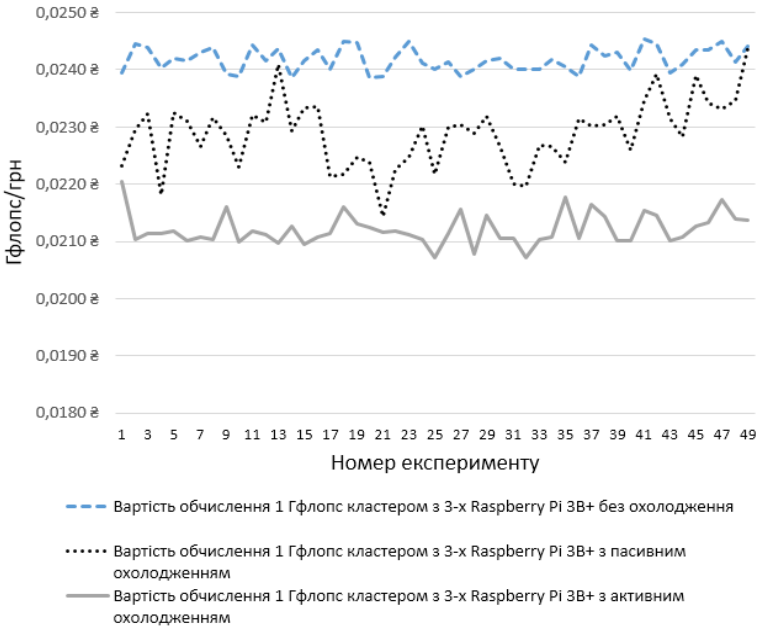


Рис. 2. Вартість обчислення 1 Гфлопс кластерною системою на базі трьох одноплатних комп'ютерів Raspberry Pi 3B+ під час виконання тесту "High performance challenge benchmark" та при використанні різних підходів до охолодження кластера

Під час виконання тесту "High performance challenge benchmark" кластерною системою на базі трьох одноплатних комп'ютерів Raspberry Pi 3B+ при використанні різних підходів до охолодження кластера було визначено вартість обчислення 1 Гфлопс (рис. 2).

Під час виконання тесту “High performance challenge benchmark” кластерною системою на базі двох одноплатних комп’ютерів Raspberry Pi 3B+ при використанні різних підходів до охолодження кластера було визначено вартість обчислення 1 Гфлопс (рис. 3).

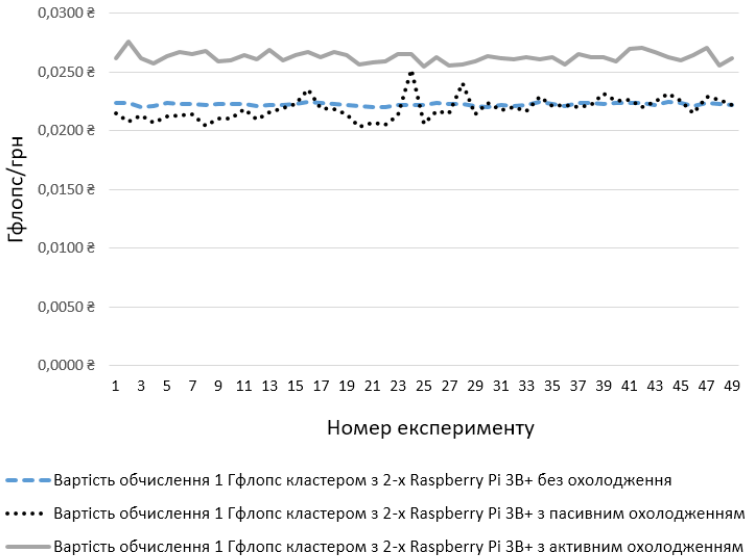


Рис. 3. Вартість обчислення 1 Гфлопс кластерною системою на базі двох одноплатних комп’ютерів Raspberry Pi 3B+ під час виконання тесту “High performance challenge benchmark” та при використанні різних підходів до охолодження кластера

Для зручності проведення аналізу результатів експериментів було розраховано середні значення вартості обчислення 1 Гфлопс кластерною системою на базі одноплатних комп’ютерів Raspberry Pi 3B+ при різній кількості плат Raspberry Pi 3B+ в ній та при різних підходах до охолодження кластера (рис. 4).

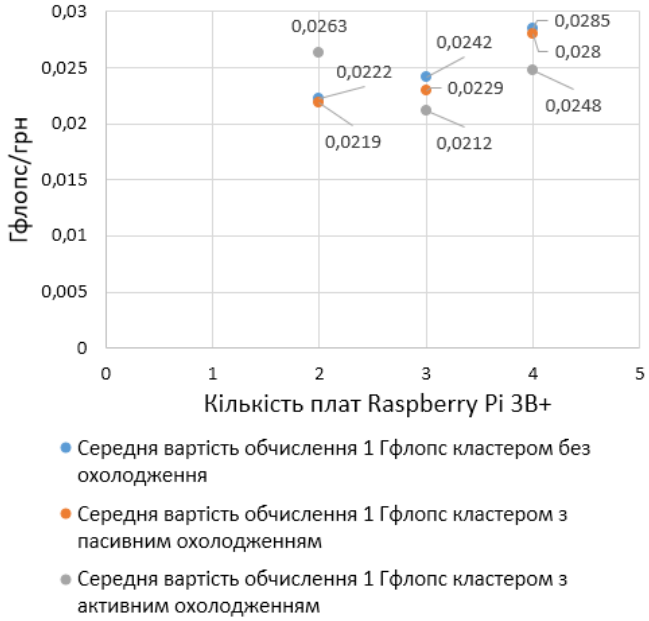


Рис. 4. Середні значення вартості обчислення 1 Гфлопс кластерною системою на базі одноплатних комп’ютерів Raspberry Pi 3B+ при різній кількості плат Raspberry Pi 3B+ в ній та при різних підходах до охолодження кластера

З рис. 4 видно, що середні значення вартості обчислення 1 Гфлопс кластерною системою на базі одноплатних комп’ютерів Raspberry Pi 3B+ при різній кількості плат Raspberry Pi 3B+ в ній при пасивній системі охолодження і без системи охолодження майже однакові: при використанні пасивної системи охолодження вартість обчислення 1 Гфлопс нижча в межах від 1,35% до 5,37 %:

– 1,35 % при 2 Raspberry Pi 3B+;
– 5,37 % при 3 Raspberry Pi 3B+;
– 1,75 % при 4 Raspberry Pi 3B+.

Таким чином, впровадження пасивної системи охолодження в кластерній системі на базі одноплатних комп'ютерів Raspberry Pi 3B+ призводить до незначного зменшення вартості обчислення 1 Гфлопс кластерною системою на базі одноплатних комп'ютерів Raspberry Pi 3B+ (від 1,35 % до 5,37 %). Крім того, з рис. 4 видно, що із збільшенням кількості одноплатних комп'ютерів Raspberry Pi 3B+ в кластері зростає вартість обчислення 1 Гфлопс кластерною системою при пасивній системі охолодження і без системи охолодження.

У випадку використання кластерної системи на базі двох одноплатних комп'ютерів Raspberry Pi 3B+ вартість обчислення 1 Гфлопс кластерною системою з активним охолодженням на 20,09 % вища ніж у такої системи з пасивним охолодженням і на 18,47 % вища ніж у такої системи без охолодження. Таким чином, для кластеру на базі двох одноплатних комп'ютерів Raspberry Pi 3B+ найбільш економічно ефективною є робота кластеру з пасивною системою охолодження.

При збільшенні кількості одноплатних комп'ютерів Raspberry Pi 3B+ в кластерній системі (від 3-х і більше) найбільш економічно ефективною стає робота кластеру з активною системою охолодження в порівнянні з аналогічними системами з пасивним охолодженням та без охолодження:

– в кластері з трьох одноплатних комп'ютерів Raspberry Pi 3B+ вартість обчислення 1 Гфлопс кластерною системою з активним охолодженням на 7,42 % нижча ніж у такої системи з пасивним охолодженням і на 12,40 % нижча ніж у такої системи без охолодження;

– в кластері з чотирьох одноплатних комп'ютерів Raspberry Pi 3B+ вартість обчислення 1 Гфлопс кластерною системою з активним охолодженням на 11,43 % нижча ніж у такої системи з пасивним охолодженням і на 12,98 % нижча ніж у такої системи без охолодження.

Отже, при збільшенні числа одноплатних комп'ютерів Raspberry Pi 3B+ в кластерній системі вище двох більш економічно ефективну роботу кластера забезпечує обладнання активною системою охолодження.

Розробка математичних моделей залежності вартості обчислення 1 Гфлопс кластерною системою на базі одноплатних комп'ютерів Raspberry Pi 3B+ від кількості плат Raspberry Pi 3B+ в ній при різних підходах до охолодження кластера. В результаті проведених досліджень встановлено математичні моделі залежності вартості обчислення 1 Гфлопс кластерною системою на базі одноплатних комп'ютерів Raspberry Pi 3B+ від кількості плат Raspberry Pi 3B+ в ній при активному охолодженні (1), при пасивному охолодженні (2) та без системи охолодження (3):

$$y = 0{,}0044x^2 - 0{,}0269x + 0{,}0626, \quad (1)$$

$$y = 0{,}0021x^2 - 0{,}0093x + 0{,}0322, \quad (2)$$

$$y = 0{,}0012x^2 - 0{,}0038x + 0{,}0251. \quad (3)$$

З встановлених математичних моделей 1–3 видно, що вони мають форму полінома другого порядку.

В порівнянні з середніми значеннями вартості обчислення 1 Гфлопс кластерною системою на базі одноплатних комп'ютерів Raspberry Pi 3B+, отриманими за результатами експериментів, похибка розрахунків вартості обчислення 1 Гфлопс кластерною системою на базі одноплатних комп'ютерів Raspberry Pi 3B+ залежно від кількості плат Raspberry Pi 3B+ в ній за допомогою моделей 1–3 не перевищує 2,5 % (0,0006 грн).

Висновки. В результаті проведених досліджень розроблено математичні моделі залежності вартості обчислення 1 Гфлопс кластерною системою на базі одноплатних комп'ютерів Raspberry Pi 3B+ від кількості плат Raspberry Pi 3B+ в ній при різних підходах до охолодження кластера (похибка розрахунків не перевищує 2,5 % – 0,0006 грн).

Встановлено, що середні значення вартості обчислення 1 Гфлопс кластерною системою на базі одноплатних комп'ютерів Raspberry Pi 3B+ при різній кількості плат Raspberry Pi 3B+ в ній при пасивній системі охолодження і без системи охолодження майже однакові: при використанні пасивної системи охолодження вартість обчислення 1 Гфлопс нижча в межах від 1,35 % до 5,37 %. Із збільшенням кількості одноплатних комп'ютерів Raspberry Pi 3B+ в кластері зростає вартість обчислення 1 Гфлопс кластерною системою при пасивній системі охолодження і без системи охолодження.

У випадку використання кластерної системи на базі двох одноплатних комп'ютерів Raspberry Pi 3B+ вартість обчислення 1 Гфлопс кластерною системою з активним охолодженням на 20,09 % вища ніж у такої системи з пасивним охолодженням і на 18,47 % вища ніж у такої системи без охолодження. При збільшенні числа одноплатних комп'ютерів Raspberry Pi 3B+ в кластерній системі вище двох більш економічно ефективну роботу кластера забезпечує його обладнання активною системою охолодження.

Визначені особливості та залежності зміни вартості обчислення 1 Гфлопс кластерною системою на базі одноплатних комп'ютерів Raspberry Pi 3B+ від кількості плат Raspberry Pi 3B+ в ній, при різних підходах до охолодження кластера, що дозволить в подальшому вибирати конфігурацію кластерної системи, яка забезпечить більш ефективну роботу.

Література

1. Мини-суперкомпьютер: 1000 Raspberry Pi объединили в кластер [Електронний ресурс]. – Режим доступу: https://habr.com/ru/post/408695/

2. Cutress I. New #1 Supercomputer: Fugaku in Japan, with A64FX, take Arm to the Top with 415 PetaFLOPs. - Anandtech. - [Electronic resource]. – Access mode: https://www.anandtech.com/show/15869/new-1-supercomputer-fujitsus-fugaku-and-a64fx-take-arm-to-the-top-with-415-petaflops

3. Lohr S. Move Over, China: U.S. Is Again Home to World's Speediest Supercomputer. - The New York Times. - [Electronic resource]. – Access mode: https://www.nytimes.com/2018/06/08/technology/supercomputer-china-us.html?hp&action=click&pgtype=Home/page&clickSource=/ story-heading&module=first-column-region&region=top-news&WT.nav=top-news

4. Simon J. Cox, James T. Cox, Richard P. Boardman, Steven J. Johnston, Mark Scott, Neil S. O'Brien Iridis-pi: a low-cost, compact demonstration cluster // Cluster Computing, June 2013, Volume 17, Issue 2, pp 349-358

5. Шиллинг А. Суперкомпьютерный кластер из 1.060 Raspberry Pi 3 B+ [Електронний ресурс]. – Режим доступу: https://www.hardwareluxx.ru/index.php/news/hardware/prozessoren/47993-superkompyuternyj-klaster-iz-1-060-raspberry-pi-3-b.html

6. Никольский И.М., Фурманов К.К. Об использовании кластеров из одноплатных компьютеров для анализа данных в Интернете вещей. Сборник CEUR Workshop Proceedings, том 1787, 2016. - с. 381-384

7. Moore J., Performance Benchmarking a Raspberry Pi Cluster, 2014

8. Babchuk, S. Classification of Specialized Computer Networks // Journal of Automation and Information Sciences. – 2016. – Vol. 48. – P. 57-64.

9. Cloutier M. F., Paradis C., Weaver V. M., Design and Analysis of a 32-bit Embedded High-Performance Cluster Optimized for Energy and Performance // Co-HPC, 2014. – P.1–8.

10. Ellen-Louise Bleeker, Magnus Reinholdsson, Creating a Raspberry Pi-Based Beowulf Cluster, 2017. – P.66.

11. Abdurrachman M., Study of Raspberry Pi 2 Quad-core Cortex-A7 CPU Cluster as a Mini Supercomputer // 8th ICITEE. – Yogyakarta, Indonesia, 2016. – P.4.

12. High performance challenge benchmark [Electronic resource]. – Access mode: https://icl.utk.edu/hpcc/

Reference

1. Mini-superkompyuter: 1000 Raspberry Pi obedinili v klaster [Electronic resource]. – Access mode: https://habr.com/ru/ post/408695/

2. Cutress I. New #1 Supercomputer: Fugaku in Japan, with A64FX, take Arm to the Top with 415 PetaFLOPs. - Anandtech. - [Electronic resource]. – Access mode: https://www.anandtech.com/show/15869/new-1-supercomputer-fujitsus-fugaku-and-a64fx-take-arm-to-the-top-with-415-petaflops

3. Lohr S. Move Over, China: U.S. Is Again Home to World's Speediest Supercomputer. - The New York Times. - [Electronic resource]. – Access mode: https://www.nytimes.com/2018/06/08/technology/supercomputer-china-us.html?hp&action=click&pgtype=/ Homepage&clickSource=/ story-heading&module=first-column-region&region=top-news&WT.nav=top-news

4. Simon J. Cox, James T. Cox, Richard P. Boardman, Steven J. Johnston, Mark Scott, Neil S. O'Brien Iridis-pi: a low-cost, compact demonstration cluster // Cluster Computing, June 2013, Volume 17, Issue 2, pp 349-358

5. Shilling A. Superkompyuternyiy klaster iz 1.060 Raspberry Pi 3 B+ [Electronic resource]. – Access mode: https://www.hardwareluxx.ru/index.php/news/hardware/prozessoren/47993-superkompyuternyj-klaster-iz-1-060-raspberry-pi-3-b.html

6. Nikolskiy I.M., Furmanov K.K. Ob ispolzovanii klasterov iz odnoplatnyih kompyuterov dlya analiza dannyih v Internete veschey. Cbornik CEUR Workshop Proceedings, tom 1787, 2016. - P. 381-384

7. Moore J., Performance Benchmarking a Raspberry Pi Cluster, 2014.

8. Babchuk, S. Classification of Specialized Computer Networks // Journal of Automation and Information Sciences. – 2016. – Vol. 48. – P. 57-64

9. Cloutier M. F., Paradis C., Weaver V. M., Design and Analysis of a 32-bit Embedded High-Performance Cluster Optimized for Energy and Performance // Co-HPC, 2014. – P.1–8.

10. Ellen-Louise Bleeker, Magnus Reinholdsson, Creating a Raspberry Pi-Based Beowulf Cluster, 2017. – P.66.

11. Abdurrachman M., Study of Raspberry Pi 2 Quad-core Cortex-A7 CPU Cluster as a Mini Supercomputer // 8th ICITEE. – Yogyakarta, Indonesia, 2016. – P.4.

12. High performance challenge benchmark [Electronic resource]. – Access mode: https://icl.utk.edu/hpcc/

Надійшла / Paper received: 02.10.2020 Надрукована / Paper Printed : 02.12.2020

УДК 004.932
DOI: 10.31891/2219-9365-2020-66-2-10

БЕДРАТЮК Г. І.
Хмельницький національний університет

АНАЛІЗ ЯКОСТІ МЕТОДІВ ПОВОРОТУ ЗОБРАЖЕННЯ ЗА ДОПОМОГОЮ МОМЕНТНИХ ІНВАРІАНТІВ

У роботі запропоновано новий метод оцінки якості повороту напівтонових зображень на основі статистичних поворотних інваріантів зображення. Поворотні моменти довільного порядку не змінюються при повороті зображень і тому можуть слугувати мірою для оцінки зміни якості зображень при поворотах. Проведені числові експерименти показали, що поворотні моменти ефективно виявляють спотворення зображення і поводять себе аналогічно, як і відомі індекси якості зображень.

Ключові слова: якість зображення, поворот, інтерполяція зображення, індекси якості, поворотні інваріанти.

BEDRATYUK A.
Khmelnytsky National University

ROTATION IMAGE QUALITY ASSESSMENT VIA GEOMETRIC MOMENT INVARIANTS

Digital image processing often results in a loss of image quality, which is expressed in the appearance of unwanted distortion on the converted image. Visual image quality measurement is important for image and video processing programs. There are about a hundred different metrics, measuring image quality, the most popular of which are root mean square error (MSE), peak signal to noise ratio (PSNR), universal image quality index (UQI), structural similarity index (SSIM), descriptor index similarity (FSIM), gradient similarity measure (GSM), noise level measure (NQM). One of the most common standard image processing methods is to rotate an image centered at any point in the plane. In fact, rotation is a resampling of an image followed by interpolation. There have been many different rotation algorithms recently, which makes it important to study methods for assessing their quality.

In this article, we propose a new method for estimating the quality of rotation based on geometric invariant moments of the image. Geometric moments and their invariants were first introduced and are intensively used in computer vision and pattern recognition. Global image descriptors are built on moments, which characterize the shape of objects in the image and are resistant to simple transformations – parallel transfer, rotation and uniform scaling. In this paper, we offer a set of invariants that are resistant only to turns. The fact that the torques do not change for the original and perfectly interpolated image allows you to use the torques as a measure of the quality of interpolation when rotating.

The paper proposes a new method for estimating the quality of rotation of grayscale images based on statistical rotational invariants of the image. The geometric moment invariants of arbitrary order do not change under rotating images and therefore can serve as a measure to assess the image quality. Numerical experiments have shown that the invariants effectively detect image distortion and behave similarly to known image quality indices.

Keywords: image quality, rotation, image interpolation, quality indices, rotation invariants.

1. Вступ. Цифрова обробка зображення часто призводить до втрати якості зображення, яка виражається у появі на перетвореному зображенні небажаних спотворень. Вимірювання якості візуального зображення має важливе значення для програм обробки зображень та відео. Існує біля сотні різноманітних метрик, див. [1]-[5] для вимірювання якості зображення, найбільш популярні з них – середня квадратична помилка (MSE), пікове співвідношення сигналу до шуму (PSNR), універсальний індекс якості зображення (UQI), індекс структурної схожості (SSIM), індекс дескрипторної схожості (FSIM), градієнтна міра подібності (GSM), міра рівня шуму (NQM). Одним із найпоширеніших стандартних методів обробки зображень є поворот зображення з центром у довільній точці площини. Фактично, поворот є передискретизацією зображення з наступною інтерполяцією. Останнім часом з'явилося багато різноманітних алгоритмів повороту [6–10], що робить актуальним вивчення методів оцінки їхньої якості.

У статті ми пропонуємо новий метод оцінки якості повороту на основі геометричних інваріантних моментів зображення. Геометричні моменти та їхні інваріанти вперше були введені в роботі [12] і інтенсивно використовуються в комп'ютерному зорі та розпізнаванні образів. На основі моментів будуються глобальні дескриптори зображення, які характеризують форму об'єктів на зображенні і є стійкими до простих перетворень – паралельного перенесення, поворотів і рівномірного масштабування. В даній роботі ми пропонуємо множину інваріантів які стійкі лише до поворотів. Той факт, що поворотні моменти не змінюються для оригінального та ідеально інтерпольованого зображення, дозволяє використати поворотні моменти як міру якості інтерполяції при повороті.

Стаття організована наступним чином. В розділі 2 поняття геометричних моментів та геометричних моментів які є інваріантами відносно повороту зображення, без зміни його розміру. Також вводиться поняття моментної метрики. В розділі 3 дана коротка характеристика методів інтерполяції які будуть аналізуватися – інтерполяція за найближчим сусідом, лінійна інтерполяція та віконна інтерполяція Ланцоша.

В розділі 4 наводяться результати числових експериментів з обчислення поворотних моментів та аналізу якості повороту при інтерполяції.

2. Ротаційні моментні інваріанти та моментна метрика. Введення моментних інваріантів на початку 60-х років було одним з перших прикладних застосувань класичної теорії інваріантів до широкого класу задач з розпізнавання образів. В важливій роботі [12] було вперше запропоновано для вирішення проблем розпізнавання розглядати добре відомі в математиці статистичні моменти. Дамо необхідні означення. Під цифровим зображенням ми будемо розуміти функцію від двох змінних $f(x,y)$, яка інтегровна на деякій множині Ω площини $\mathbb{R}^2$. ***Геометричним моментом*** порядку $p+q$ функції $f(x,y)$ називається вираз:

$$m_{pq}(f(x,y)) = m_{pq} = \iint_{\Omega} x^p y^q f(x,y)dxdy, \Omega \subset \mathbb{R}^2.$$

У роботі [13] повна система геометричних інваріантів описана в термінах власних векторів $e_d(\lambda)$ лінійного оператора

$$D_d(m_{p,q}) = qm_{p+1,q-1} - pm_{p-1,q+1}, d = p + d,$$

де $e_d(\lambda) = \sum_{j=0}^{d} i^j \mathcal{K}_j\left(\frac{1}{2}(d-\lambda), d\right) m_{d-j,j}, \lambda \in \Lambda_d = \{d, d-2, \dots, -(d-2), -d\}$, і $\mathcal{K}_n(x,N)$ є бінарними многочленами Кравчука. Можна довести, що всі поворотні інваріанти описуються трьома типами інваріантів:

$$e_{2d}(0), e_d(\lambda)e_d(-\lambda), e_d(\lambda)e_1(-1)^{\lambda}.$$

Ми будемо використовувати такі п’ять поворотних моментів малих порядків:

$$\varphi_0 = e_0(0) = m_{0,0},$$
$$\varphi_1 = e_1(1)e_1(-1) = m_{1,0}^2 + m_{0,1}^2,$$
$$\varphi_2 = e_2(0) = m_{2,0} + m_{0,2},$$
$$\varphi_3 = e_2(2)e_2(-2) = m_{2,0}m_{0,2} - {m_{1,1}}^2,$$
$$\varphi_4 = e_2(2)e_{-1}^2 = (m_{0,2} - m_{2,0})(m_{0,1}^2 - m_{1,0}^2) + 4\, m_{1,1}m_{1,0}m_{0,1},$$
$$\varphi_5 = e_2(0) = m_{4,0} + 2\, m_{2,2} + m_{0,4}.$$

При виконанні повороту зображення на деякий кут, вирази φ_i, обчислені на зображенні до і після повороту, теоретично мають залишаться однаковими. Проте це не так, оскільки реальні зображення є дискретними а не неперервними. При переході до дискретного зображення розміру $M \times N$-пікселів, інтеграли замінюються сумами, вираз для геометричних моментів приймає такий вигляд

$$m_{p,q} = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} x^p y^q f(x,y),$$

і при обчисленні виникають помилки округлення. Крім того, при поворотах має місце неспівпадіння растрової сітки, і зображення зазнає повторної дискретизації. Тому реальні обчислення призводять до відхилення від теоретичних результатів. Для оцінки таких спотворень зображення f до і після повороту $\tilde{f}$ існують різноманітні методи, найбільш поширеним є середньо квадратичне відхилення. Проте, як зазначають різні автори, див. наприклад [14], не існує сильної кореляції між зоровою деградацією якості зображення та середньо квадратичним відхиленням. У більшій мірі структуру зображення відображають універсальний індекс якості UQI і індекс структурної схожості SSIM. Також, якісна метрика повинна задовольняти природну умову – якщо при масштабуванні відбулися спотворення зображення, то чим більші ці спотворення тим більшою повинна бути відстань між оригіналом і інтерпольованим зображенням. В розділі 3 ми експериментально підтвердимо що поворотні інваріанти задовольняють цій умові неперервності, вивчаючи їхню поведінку при поворотах зображень. Крім того ми вводимо такі дві метрики як міру оцінки якості повороту зображень:

$$DistAbs(f,f') = \sqrt{\sum_{y=0}^{s} (\varphi_1(f) - \varphi(f'))^2},$$
$$DistSqrt(f,f') = \sum_{y=0}^{s} |\varphi_1(f) - \varphi(f')|,$$

тут $\varphi_i, i = 0,1, \dots, s$ – деяка система незалежних поворотних інваріантів.

Ми оцінимо якість методів повороту та порівняємо як різні метрики реагують на спотворення при різних поворотах.

3. Алгоритми інтерполяції для повороту. Поворот навколо центру координат на кут θ переводить старі координати пікселя (x, y) у нові (x', y') за формулами:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Формули для перерахунку координат пікселя для повороту виконаного навколо довільної точки площини з координатами (x_c, y_c) на кут θ, мають вигляд:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x - x_c \\ y - y_c \end{pmatrix} + \begin{pmatrix} x_c \\ y_c \end{pmatrix}.$$

Головна проблема при довільному геометричному перетворенні зображення полягає у тому, що пікселі є елементами дискретної растрової сітки, а не неперервної площини, тому може статися так, що нові координати пікселя (x', y'), обчислені за формулами перетвореннями не є цілими числами. На рис. 1 показано ситуація яка виникає при повороті одного пікселя, який в новому положенні не потрапляє повністю в клітинку растрової сітки:

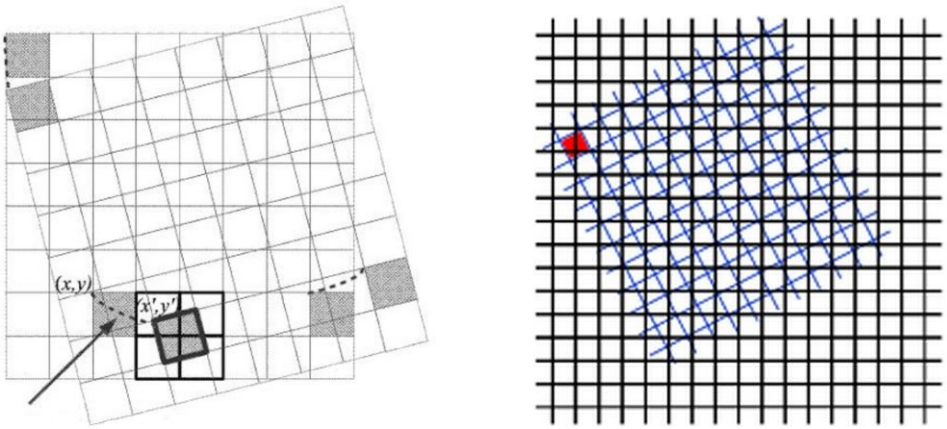


Рис. 1. Поворот растрової сітки

Проблема вирішується екстраполяцією місцеположення відсутніх пікселів в новому зображенні та інтеполяцією їхніх значень, а такий процес в цілому називається ***інтерполяцією*** зображення. Всі відомі алгоритми інтерполяції зводяться до методів присвоєння пікселям таких значень, щоб інтерпольоване зображення було візуально схожим на оригінал, і не містило нової небажаної інформації. Існує велика кількість алгоритмів інтерполяції, їх кількість постійно збільшується. Розглянемо три стандартні алгоритми повороту зображення, які ми будемо використовувати для оцінки критеріїв ефективності інтерполяції.

3.1. Інтерполяція за найближчим сусідом. При інтерполяції методом найближчого сусіда, нові координати пікселя округлюються до найближчого цілого числа:

$$x' = [x\cos\theta - y\sin\theta], \quad y' = [x\sin\theta + y\cos\theta]$$

Цей простий, легкий у реалізації, алгоритм, але він часто приводить до появи на зображенні небажаних артефактів, зокрема значного спотворення прямолінійних контурів.

3.2. Білінійна інтерполяція. Білінійна інтерполяція є узагальненням звичайної лінійної інтерполяції на випадок функції двох змінних. При білінійній інтерполяції, невідоме значення яскравості $f(x, y)$ пікселя з координатами (x, y) визначається відомою яскравістю 4-х найближчих пікселів $(x_1, y_1), (x_1, y_2), (x_1, y_1), (x_2, y_2)$ за наступною формулою:

$$f(x, y) = a_0 + a_1 x + a_2 y + a_3 xy$$

де невідомі a_0, a_1, a_2, a_3 визначаються з системи рівнянь:

$$\begin{bmatrix} 1 & x_1 & y_1 & x_1 y_1 \\ 1 & x_1 & y_2 & x_1 y_2 \\ 1 & x_2 & y_1 & x_2 y_1 \\ 1 & x_2 & y_2 & x_2 y_2 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} = \begin{bmatrix} f((x_1, y_1)) \\ f((x_1, y_2)) \\ f((x_2, y_1)) \\ f((x_2, y_2)) \end{bmatrix}.$$

Як правило, якість лінійної інтерполяції краща ніж інтерполяції методом найближчого сусіда.

3.3. Інтерполяція Ланцоша. Цей метод визначається згорткою зображення $\boldsymbol{f(x,y)}$ з таким ядром:

$$W_{Ln}(x,y) = w_{Ln}(x)w_{Ln}(y),$$

де

$$w_{Ln}(x) = \begin{cases} 1, \text{для} |x| - 0, \\ \frac{n}{\pi^2 x^2} \sin\left(\pi \frac{x}{n}\right) \sin(\pi x), \text{для} 0 < |x| < n, \\ 0, \text{для} |x| \geq n. \end{cases}$$

Нове значення пікселя у збільшеного зображення $\tilde{f}(x,y)$ в результаті такої згортки має вигляд:

$$\tilde{f}(x,y) = \sum_{v=y-n+1}^{y+n} \left[\sum_{u=x-n+1}^{x+n} f(u_i, v) W_{Ln}(x-u, y-v)\right].$$

для цілих x, y.

Інтерполяція Ланцоша вважається одним з найкращих методів інтерполяції, особливо тоді, коли розміри інтерпольованого зображення змінюються. Поворот зображення визначається матрицею повороту, та вектором зміщення, при необхідності. Після виконання повороту, відбувається інтерполяція тих пікселів які не потрапили, або потрапили неповністю у нове положення растрової сітки.

4. Чисельні експерименти. Розглянуті три алгоритми повороту реалізовані в бібліотеці OpenCV (Open Source Computer Vision Library). В OpenCV матриця повороту визначається функцією getRotationMatrix2D параметрами якої є центр повороту, кут повороту і коефіцієнт розтягу. Сам поворот зображення здійснюється функцією warpAffine параметрами якої є зображення, матриця повороту, коефіцієнт збільшення і метод інтерполяції. Для повороту зображень ми будемо використовувати три різні алгоритми – метод найближчого сусіда, лінійну інтерполяції та інтерполяцію Лакоша. В OpenCV ці алгоритми викликаються такими параметрами інтерполяції: cv2.INTER_NEAREST, cv2.cv2.INTER_LINEAR і cv2.INTER_LANCZOS4. Для інтерполяції Лакоша використовувалося 8×8-ядро. Зауважимо, що коефіцієнт стиснення має бути рівний 1, оскільки інваріанти $\boldsymbol{\phi_i}$ є стійкими лише до повороту і не стійкі до масштабування**.**

Всі числові експерименти проводилися з зображенням Cameraman, див. рис. 2, яке є стандартним зображенням в теорії цифрової обробки зображень.

Рис. 2. Тестове зображення Cameraman

Ми розглянули зображення Cameraman, розміру 68×100, а потім обертали це зображення, з використанням інтерполяції за найближчим сусідом, від 0 до 360 градусів, з кроком 36 градусів. Всі 10 тестових зображень розміщені на рис. 3:

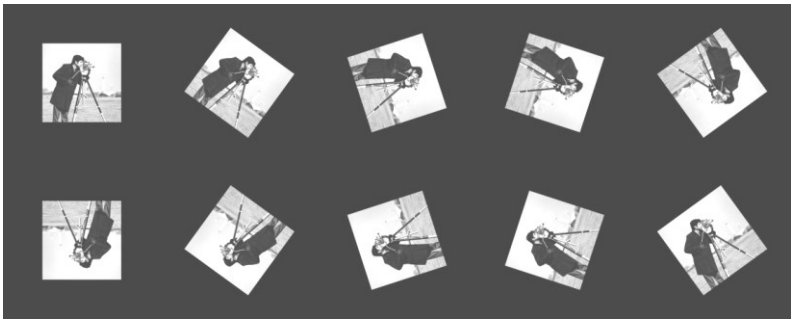


Рис. 3. Зображення, повернуті на 36°

Нам потрібно перевірити, чи обертальні моменти, як пропонований інструмент виявлення спотворень, правильно відреагують на спотворення, які відбулися при інтерполяції. Результати обчислення обертальних інваріантів малого порядку на кожному з тестових зображень показані в таблиці 1. У першому рядоку таблиці розміщені кути повороту зображення Cameraman, а кожен наступний рядок рядок таблиці є значенням відповідного модифікованого обертового моменту на одному із 10 зображень. Як видно з таблиці, значення обертових моментів коливаються навколо значення моментів на початковому, неповернутому зображенні. Причина такої поведінки зрозуміла – при повороті дискретної растрової решітки, нові місцеположення пікселів не співпадають з старим растром і тому відбувається інтерполяція при якій значення пікселів відрізняються від значень пікселів початкового зображення, на що зразу реагує обертовий момент. Максимальне співпадіння растрових решіток відбувається у випадках коли кут повороту кратний 180°. Тепер дослідимо лінійну інтерполяцію та інтерполяцію Ланцоша. Візуальний аналіз показує, що якість лінійної інтерполяції не відрізняється за інтерполяцію методом найближчого сусіда. Також таблиці результати обчислень поворотних моментів ідентичні до таблиці 1, тому ми їх не наводимо.

Таблиця 1.

Обертальні моменти зображення повернутого за алгоритмом найближчого сусіда

Кут	0°	36°	72°	108°	144°	180°	216°	252°	288°	324°
$\tilde{\varphi}_0$	7,0723	7,0723	7,0723	7,0723	7,0723	7,0723	7,0723	7,0723	7,0723	7,0723
$\tilde{\varphi}_1$	19,394	19,416	19,431	19,434	19,424	19,405	19,382	19,365	19,362	19,373
$\tilde{\varphi}_2$	12,359	12,38	12,393	12,396	12,387	12,369	12,349	12,333	12,33	12,34
$\tilde{\varphi}_3$	23,295	23,338	23,38	23,382	23,344	23,305	23,302	23,316	23,312	23,292
$\tilde{\varphi}_4$	105,36	105,5	105,59	105,62	105,56	105,44	105,28	105,16	105,13	105,22
$\tilde{\varphi}_5$	40,783	40,858	40,908	40,922	40,896	40,831	40,743	40,671	40,655	40,703

На рис. 4 графічно представлена поведінка модифікованих поворотних інварінатів. Для кращого розуміння поведінки інваріантів ми обчислили оборотні інваріанти на 360 зображеннях отриманих з оригінального зображення послідовними поворотами на 1°. Для уніфікації значення всіх інваріантів кожного повернутого зображення було нормалізоване діленням на значення.

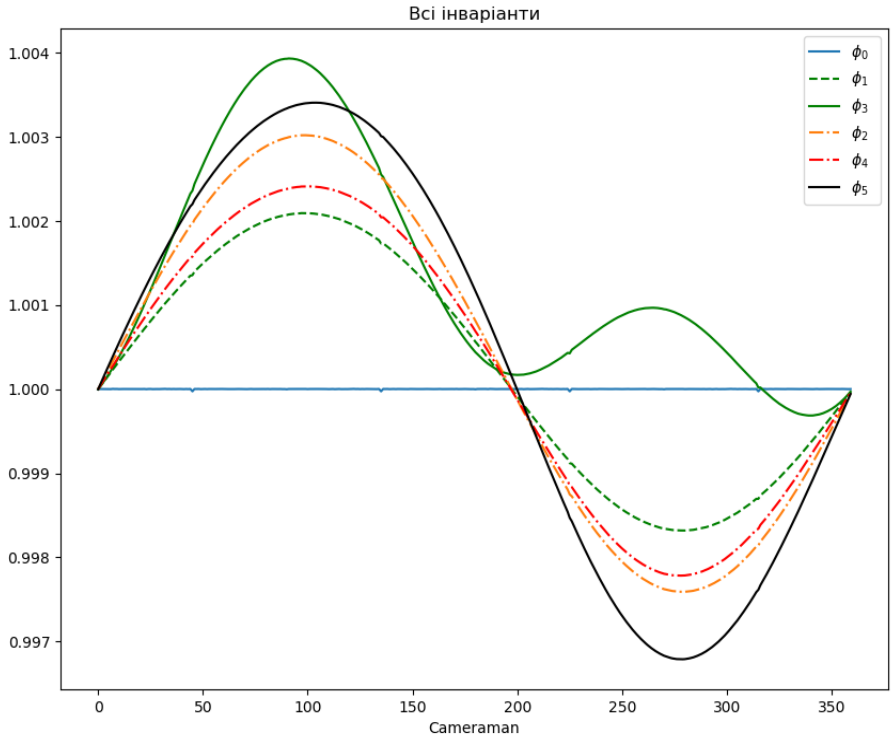


Рис. 4. Спільний графік всіх інваріантів

Отже, можна зробити такі висновки:

1) візуальна якість повороту зображення при трьох різним методах інтерполяції однакова;

2) всі обертові моменти приймають однакові значення на зображеннях інтерпольованих різними методами;

3) всі обертові моменти чутливі до зменшення якості повороту при різних кутах;

4) як і випливає з алгоритмів інтерполяції, всі поворотні інваріанти фіксують ідентичсність зображення і повернутого зображеня на кути кратні 180°;

5) деякі методи фіксують схожість зображень при повороті на на кути кратні 90°.

Для кращого розуміння поведінки інваріантів ми обчислили поворотні інваріанти на 360 зображеннях отриманих з оригінального зображення послідовними поворотами на 1°. Для уніфікації значення всіх інваріантів кожного повернутого зображення було нормалізоване діленням на фіксоване значення.

4.1. Порівняння з іншими метриками. Використаємо інші популярні метрики, які базуються на співставленні з еталоном (reference metrics), для порівняння якості зображень, зокрема MSE – середньо квадратичне відхилення, PSNR – пікове співвідношення сигналу до шуму, SSIM – індекс структурної схожості, MSSIM – модифікований індекс структурної схожості, індекс варіації інформації VIPF. Всі індекси обчислювалися для 360 зображень утворених поворотом з кроком 1°. Інтерполяція відбувалася методом найближчого сусіда.

Як видно з рис. 5, індекси PSNR та MSE прогнозовано однаково реагують на спотворення зображення при різних кутах повороту. З графіків видно, що індекси MSE та PSNR ніяк не реагують на спотворення зображення, тому вони не можуть застосовуватися для оцінки якості інтерполяції зображень.

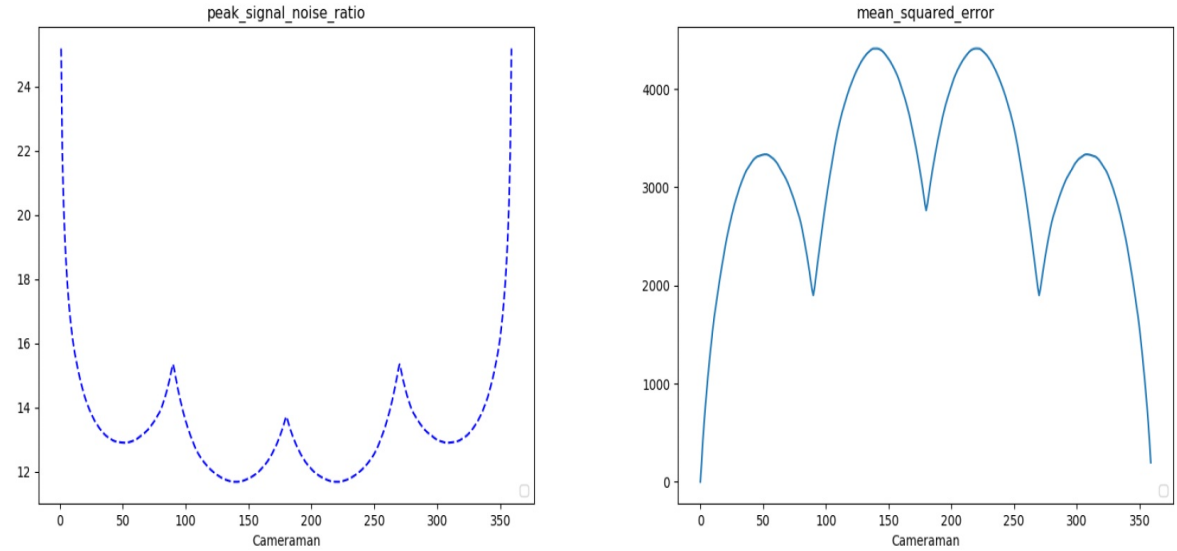


Рис. 5. Графік індексів PSNR та MSE

Як видно з рис. 6, індекси SSIM та MSSIM прогнозовано однаково реагують на спотворення зображення при різних кутах повороту.

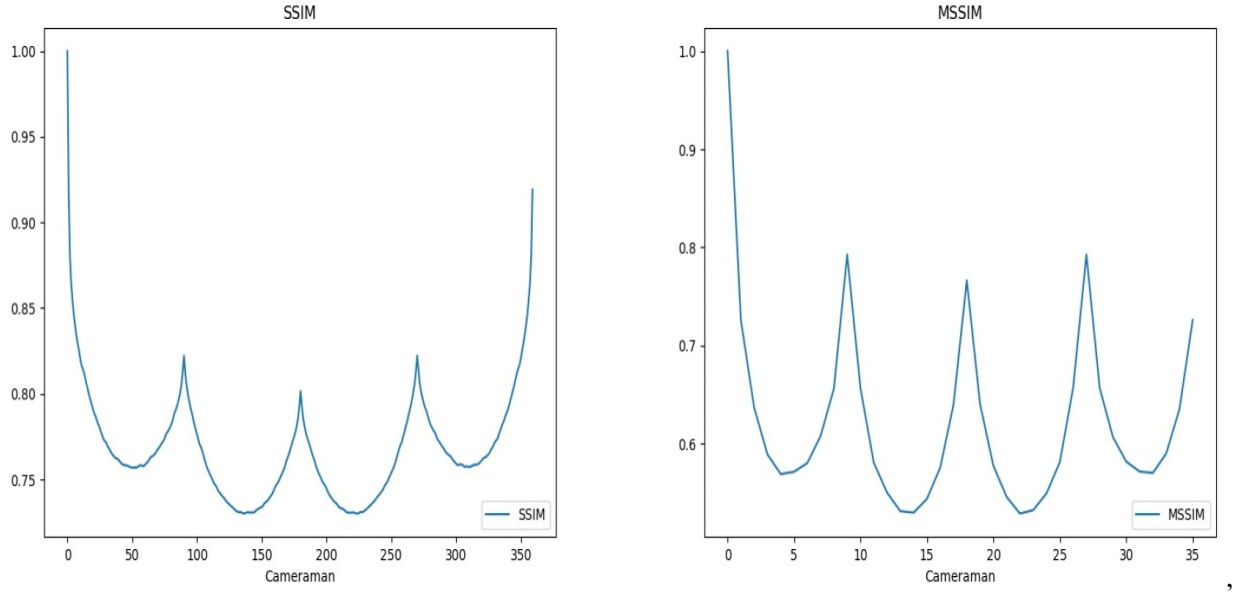


Рис. 6. Графіки індексів SSIM та MSSIM

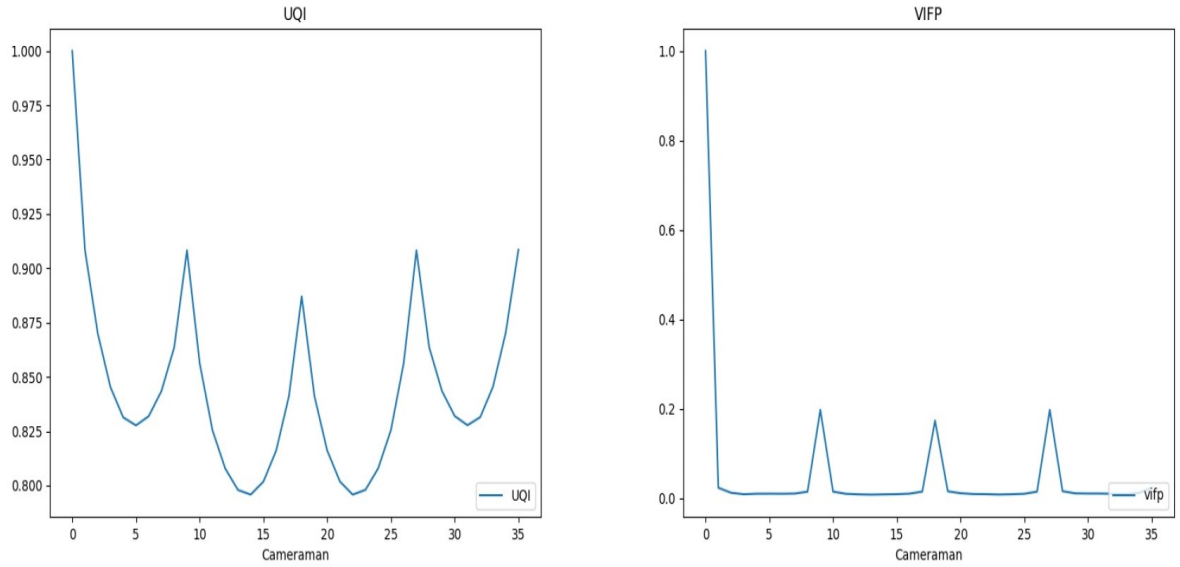


Рис. 7. Графіки індексів UQI та VIFP

Як видно з рис. 7, індекси індексі UQI добре реагує на спотворення а індекс VIFP погано реагує на спотворення зображення при різних кутах повороту. Також розглянемо дві метрики які базуються на ротаційних інваріантах:

$$DistAbs(f, f') = \sum_{i=0}^{s} |\varphi_i(f) - \varphi_i(f')|,$$

$$DistSQRT(f, f') = \sqrt{\sum_{i=0}^{s} (\varphi_i(f) - \varphi_i(f')^2}.$$

На рис. 18 показано відстані між оригінальним зображенням Cameraman та його поворотами від 0° до 360°, виконаними з кроком 1°.

Як видно, обидві метрики ведуть себе однпково і чітко реагують на спотворення якості оберненого зображення.

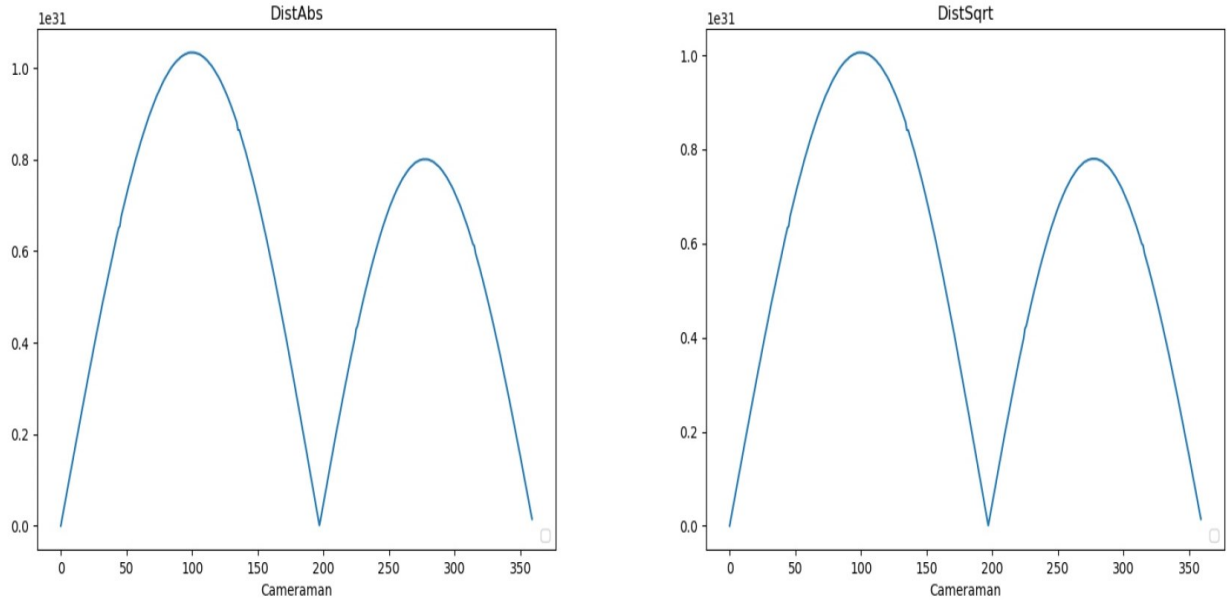


Рис. 8. Графік метрик DistAbs та DistDqrt для $s = 6$.

Висновки. Вимірювання якості візуального зображення має принципове значення для обробки зображень та відео. Метою дослідження якості (QA) є розробка алгоритмів, які можуть автоматично оцінювати якість зображень чи відеозаписів перцептивно. Алгоритми QA зображення інтерпретують якість зображення як вірність або схожість із «еталонним» або «ідеальним» зображенням у певному перцептивному просторі. У статті розглядаються поворотні моменти зображення, доводяться що вони інваріантні відносно повороту і пропонуються для оцінки якості повернутих зображень. Результати експериментальних

обчислень на конкретному зображенні показали що нормалізовані моментні інваріанти монотонно реагують на деградацію зображення і можуть застосовуватися поряд з відомими індексами якості зображень такими як SSIM. MSSIM, QUI та ін.

Література

1. Pedersen M., Hardeberg J., Full-Reference Image Quality Metrics:Classification and Evaluation, Computer Graphics and Vision, Vol. 7, No. 1,2011, 1–80.

2. Samajdar, T., Quraishi, M. I. Analysis and Evaluation of Image Quality Metrics. Information Systems Design and Intelligent Applications, 2015, 369–378.

3. Danielsson, P.-E., Hammerin, M. High-accuracy rotation of images. CVGIP: Graphical Models and Image Processing, 54(4), 1992). 340–344.

4. Lehmann T, , Gonner C., Spitzer K, Survey: Interpolation Methods in Medical Image Processing, IEEE Transactions On Medical Imaging, Vol. 18, No. 11, November 1999, 1049-1075.

5. Kipli, K, Zamhari, N., Muhammad, M. S., Sh.Masniah Wan Masra, Lee C., Lias, K. Full reference image quality metrics and their performance. 2011 IEEE 7th International Colloquium on Signal Processing and Its Applications.

6. Di Bella, E. V. R., Barclay, A. B., Eisner, R. L., Schafer, R. W. A comparison of rotation-based methods for iterative reconstruction algorithms. IEEE Transactions on Nuclear Science, 43(6), 1996, 3370–3376.

7. Asano T., Bitou S., Motoki M., Usui N. In-Place Algorithm for Image Rotation. In: Tokuyama T. (eds) Algorithms and Computation. ISAAC 2007. Lecture Notes in Computer Science, vol 4835. Springer, Berlin, Heidelberg

8. Reich, M., Yang, M. Y., Heipke, C. Global robust image rotation from combined weighted averaging. ISPRS Journal of Photogrammetry and Remote Sensing, 127, 2017, 89–101

9. Yan, F., Chen, K., Venegas-Andraca, S. E., Zhao, J. Quantum image rotation by an arbitrary angle. Quantum Information Processing, 2017, 16(11).

10. Elisa Dicke, Andreas Wachter and Werner Nahm, Estimation of the interpolation error of a three-step rotation algorithm using recorded images with rotated test pattern as ground truth. Current Directions in Biomedical Engineering 2017; 3(2): 555–558

11. Mohebbian, M. R., Rasti, J. Head and camera rotation invariant eye tracking algorithm based on segmented group method of data handling. Machine Vision and Applications, 2020,31(7-8).

12. Hu M. K.: Visual pattern recognition by moment invariants. IRE Trans. Inform. Theory. 8(2), 1962, 179–187

13. Bedratyuk, L. 2D Geometric Moment Invariants from the Point of View of the Classical Invariant Theory. J Math Imaging Vis 62, 2020,1062–1075

14. Amanatiadis A., Ioannis I., A survey on evaluation methods for image interpolation, Meas. Sci. Technol. 20, 2009,104015

Надійшла / Paper received: 19.09.2020 Надрукована / Paper Printed : 02.12.2020

УДК 621.317.73
DOI: 10.31891/2219-9365-2020-66-2-11

РАДЕЛЬЧУК Г. І., МАКАРИШКІН Д. А.,
ГРЕБІНЧУК А. Д., БОНДАР А. Ю.
Хмельницький національний університет

АДАПТИВНА МІКРОПРОЦЕСОРНА СИСТЕМА АВТОМАТИЧНОГО КЕРУВАННЯ БЕЗПІЛОТНИМ ЛІТАЛЬНИМ АПАРАТОМ

У статті наведено структуру адаптивної мікропроцесорної системи автоматичного керування безпілотним літальним апаратом із використанням нелінійної моделі безпілотного літального апарату, що дозволяє підвищити ефективність керування та вимірювання координат безпілотних літальних апаратів. Представлені результати аналізу існуючих адаптивних мікропроцесорних систем автоматичного керування безпілотним літальним апаратом. Встановлено їх переваги та недоліки. Для реалізації на практиці реальної програми керування польотом безпілотного літального апарату є необхідним застосування систематичного процесу проєктування та моделювання адаптивної мікропроцесорної системи керування використовуючи алгоритми адаптивного керування зі зворотнім зв'язком L1.

Ключові слова: адаптивна мікропроцесорна система автоматичного керування, безпілотний літальний апарат, адаптивне керування, лінійна модель, нелінійна модель.

RADELCHUK G., MAKARYSHKIN D.,
HREBINCHUK A., BONDAR A.
Khmelnitsky national university

ADAPTIVE MICROPROCESSOR SYSTEM FOR AUTOMATIC CONTROL OF UNMANNED AIRCRAFT

The modern development of unmanned aerial vehicles is extremely important for the defense capability, sovereignty and economy of Ukraine. The range of practical applications of unmanned aerial vehicles is very wide. The most important tasks of unmanned aerial vehicles are related to their use in the military, civilian (public, private, commercial) and anti-terrorist industries. Unmanned aerial vehicles have a number of advantages: high maneuverability, widely used in all areas of human activity, reliability and economy. Unmanned aerial vehicles are used in a wide range of applications, such as research, civil engineering, military use, aerial photography, search and rescue operations, and risk zone surveys. One of the most important classes of unmanned aerial vehicles are quadrocopters, which have significant advantages in many parameters, such as simplicity of design, rapid manufacture and low cost. In recent years, the subject of many scientific studies in the field of quadcopters has been the control of their position, in part the height of the quadcopter. During these scientific studies, many algorithms have been proposed to solve the problem of quadcopter control.

The paper presents the structure of an adaptive microprocessor system for automatic control of unmanned aerial vehicles using a nonlinear model of unmanned aerial vehicles, which allows to increase the efficiency of control and measurement of coordinates of unmanned aerial vehicles. The results of the analysis of the existing adaptive microprocessor systems of automatic control of the unmanned aerial vehicle are presented. Their advantages and disadvantages are established. To implement a real flight control program for an unmanned aerial vehicle, it is necessary to use a systematic process of designing and modeling an adaptive microprocessor control system using adaptive control algorithms with L1 feedback.

Key words: adaptive microprocessor automatic control system, unmanned aerial vehicle, adaptive control, linear model, nonlinear model.

Вступ. Сучасний розвиток безпілотних літальних апаратів є надзвичайно важливим для обороноздатності, суверенітету та економіки України. Спектр практичного застосування безпілотних літальних апаратів є дуже широким. Найбільш важливі задачі безпілотних літальних апаратів пов'язані із їх застосуванням у військовій, цивільній (державні, приватні, комерційні) та антитерористичній галузі [1]. Безпілотні літальні апарати мають ряд переваг: висока маневреність, широко використовуються в усіх сферах людської діяльності, надійність та економічність. Безпілотні літальні апарати застосовуються у широкому спектрі додатків, таких як наукові дослідження, громадянське будівництво, воєнне використання, аерофотозйомка, пошуково-рятувальні операції, та огляди зони ризиків [2–5]. Одним з важливіших класів безпілотних літальних апаратів є квадрокоптери, які мають значні переваги по багатьох параметрах, таких як, простота конструкції, швидке їх виготовлення та мала ціна [6, 7]. В останні роки предметом багатьох наукових досліджень в області квадрокоптерів було керування їх положенням, у частковому випадку висоти квадрокоптера [6]. Під час проведення цих наукових досліджень було запропоновано багато алгоритмів для вирішення проблеми керування квадрокоптером.

Останнім часом, однією з переваг безпілотних літальних апаратів є їх застосування в різних аерокосмічних програмах. Однак, є необхідність використовувати такі транспортні засоби в потенційно несприятливих умовах, тому дуже важливо розробляти їх з високою ефективністю та надійністю, що в свою чергу викликає науковий інтерес до використання адаптивного керування у таких випадках. Еталонні

моделі сучасних адаптивних регуляторів на основі мікропроцесорних систем на сьогодні набули широкого застосування, однак вони характеризуються одним суттєвим недоліком, які полягає у тому, що сучасні адаптивні регулятори можуть бути дуже чутливими до затримок часу. Для подолання цього недоліку та проєктування реалістичної адаптивної системи автоматичного керування, були створені відфільтровані версії сучасних адаптивних регуляторів на основі мікропроцесорних систем, які називається отримали назву адаптивне керування L1.

Аналіз останніх досліджень та публікацій. Основна перевага адаптивного керування L1 перед іншими алгоритмами адаптивного керування полягає у чіткому розділені продуктивності та надійності, де включення фільтра низьких частот гарантує необмежену пропускну здатність сигналу керування та високу швидкість адаптації, яка у свою чергу обмежується тільки доступними обчислювальними ресурсами. Звідси випливає, що проблему адаптивного керування можна поділити на два обмеження: пропускну здатність каналу та доступні ресурсні обчислення.

Найпростіша та ефективніша версія реалізації адаптивного керування L1 – це реалізація такого керування із зворотнім зв'язком, основною перевагою якого є один вхід на один вихід, тому стани такої внутрішньої системи не потребують їх моделювання та вимірювання. Модель один вхід на один вихід охоплює усю систему замкнутого циклу та формується за допомогою простих методів ідентифікації системи. Таким чином, сучасні адаптивні регулятори на основі мікропроцесорних систем зі зворотнім зв'язком, які реалізують адаптивне керування L1 представляє собою стабільну систему із замкнутим циклом, з ефективною продуктивністю та надійністю. У таких системах легко передбачити та спрогнозувати час затримки використовуючи стандартний лінійний системний аналіз. Також необхідно врахувати, що зворотний зв'язок L1 є простим в практичній реалізації.

Виклад основного матеріалу дослідження. На основі сучасного аналізу відомих адаптивних мікропроцесорних систем керування безпілотними літальними апаратами, можна зробити висновок, що найбільш застосовуються наступні адаптивні мікропроцесорні системи регулювання безпілотних літальних апаратів: адаптивні мікропроцесорні системи керування безпілотних літальних апаратів на основі пропорційно-інтегрально-диференційного регулятора; адаптивні мікропроцесорні системи керування безпілотних літальних апаратів на основі лінійно-квадратичного регулятора; адаптивні мікропроцесорні системи керування безпілотних літальних апаратів на основі методу H на нескінченості; адаптивні мікропроцесорні системи керування безпілотних літальних апаратів на основі нелінійного регулювання.

Адаптивна мікропроцесорна система керування безпілотними літальними апаратами на основі пропорційно-інтегрально-диференційного регулятора створюється на базі лінійної моделі безпілотного літального апарату в точці стабілізації, яка здатна стабілізувати систему на протязі 3-х секунд. Однак, суттєвими недоліками такої адаптивної системи автоматичного регулювання є обмежене використання, тільки у точці рівноваги та нездатність здійснювати складних маневрів, якщо така система автоматичного керування застосовується для регулювання положення та висоти безпілотного літального апарату.

Адаптивна мікропроцесорна система керування безпілотними літальними апаратами на основі лінійно-квадратичного регулятора також створюється на базі лінійної моделі безпілотного літального апарату застосовуючи декілька точок для стабілізації. Суттєвими недоліками такої адаптивної системи автоматичного регулювання є нездатність привести систему до стабілізації на фізичні моделі та неврахування динаміки двигуна у цій моделі, тобто менша продуктивність у порівнянні з адаптивною мікропроцесорною системою керування безпілотними літальними апаратами на основі пропорційно-інтегрально-диференційного регулятора.

Адаптивна мікропроцесорна система керування безпілотними літальними апаратами на основі методу H на нескінченості здатна забезпечувати ефективне та надійне відстеження заданих сигналів і відмови від порушень застосовуючи нелінійну математичну модель. При цьому нелінійна математична модель базується на змішаній чутливості методу H на нескінченості та μ-синтезу з ітераційними алгоритмами DK, завдяки цьому розробляється адаптивна мікропроцесорна система керування безпілотними літальними апаратами з високоефективною надійністю його роботи.

Адаптивну мікропроцесорну систему керування безпілотними літальними апаратами на основі нелінійного керування, краще всього застосовувати у випадках, коли відхилення є досить великими.

Як показано у науковій роботі [8], загальна структурна схема керування безпілотним літальним апаратом може бути представлена та описана через керування чотирма вхідними силами: крену, тангажу, рискання і загальної тяги (див. рис. 1).

Адаптивний алгоритм керування L1, який використовується для керування польотом безпілотного літального апарату і представляє собою систему з замкненим циклом, зображено на рис. 2. До такої адаптивної системи керування входять: низькочастотний фільтр C(s) та еталоні моделі. Застосування фільтра нижніх частот C(s) надає дві переваги: обмеження пропускної здатності керуючого сигналу u; в еталоні моделі надходить сигнал високої частоти.

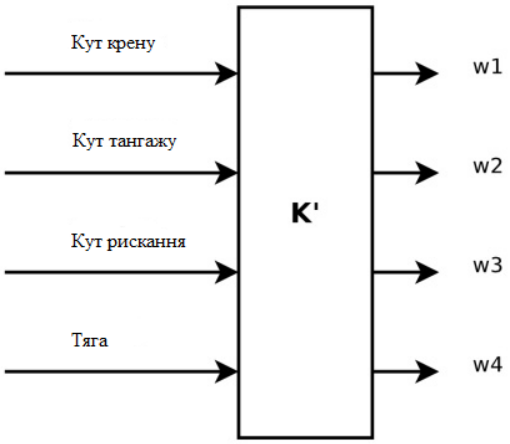


Рис. 1. Загальна структурна схема керування крену, тангажу, рискання і загальної тяги

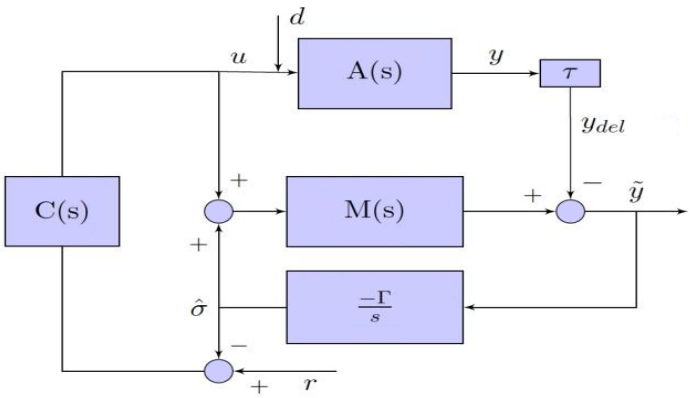


Рис. 2. Структурна схема адаптивного керування зі зворотнім зв'язком L1

Загальна структурна схема адаптивної мікропроцесорної системи автоматичного керування безпілотним літальним апаратом, яка реалізує алгоритм адаптивного керування зі зворотнім зв'язком L1 може бути представлена як показано на рис. 3.

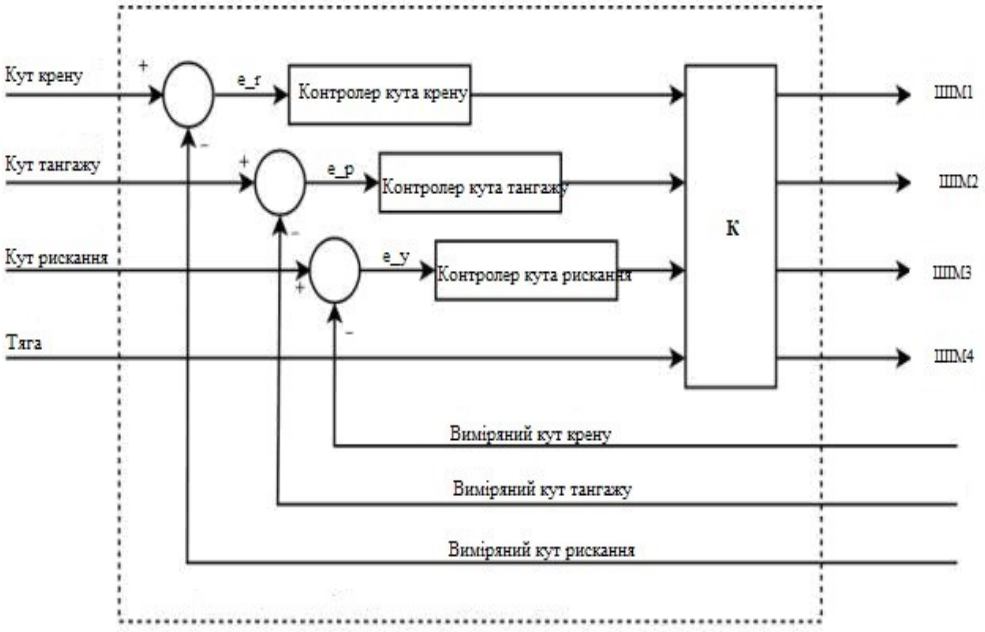


Рис. 3. Структурна схема адаптивної мікропроцесорної системи автоматичного керування безпілотним літальним апаратом

Для тестування адаптивних мікропроцесорних систем керування безпілотними літальними апаратами на основі пропорційно-інтегрально-диференційного регулятора та уникненню пошкоджень реального безпілотного літального апарату є необхідним побудова наступної нелінійної моделі безпілотного літального апарату за допомогою Simulink, яка представлена на рис. 4. Така нелінійна модель безпілотного літального апарату дозволяє імітувати рівняння руху і додати насичення до швидкості електродвигунів, що у свою чергу призводить до обмеження їх обертів в секунду у діапазоні від 0 до 150. З проведеного аналізу рис. 1, можна зробити висновок, що нелінійна математична модель складається з таких частин, як динаміка твердих тіл 6DOF, підсистема гравітаційна і двигунів, а також підсистема візуалізації. Блок динаміки твердих тіл 6DOF враховує рівняння руху твердого тіла, такі параметри як початкові умови, тензор інерції тіла, маса. Вхідними даними тут виступають вхідні сили та моменти сил. Гравітаційний блок враховує перетворення вагової сили. Призначення підсистеми двигунів полягає у вироблені зовнішніх моментів сил та сили тяги. Підсистема візуалізації для надсилання даних про положення, при цьому відбувається перетворення декартових координат у сферичні.

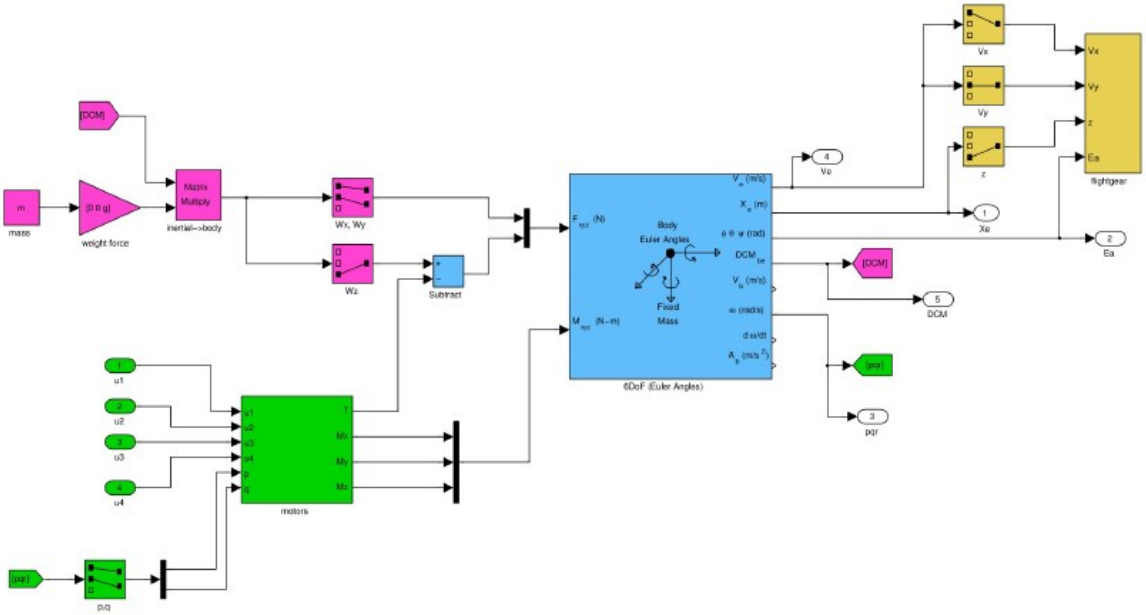


Рис. 4. Нелінійна модель безпілотного літального апарату

Висновки. Встановлено, що найбільшого використання набули адаптивні мікропроцесорні системи регулювання безпілотних літальних апаратів на основі пропорційно-інтегрально-диференційного регулятора, основі лінійно-квадратичного регулятора, методу Н на нескінченості та нелінійного керування. Проведено аналіз існуючих адаптивних мікропроцесорних систем регулювання безпілотних літальних апаратів. Встановлено їх переваги та недоліки, при використанні лінійної і нелінійної моделі безпілотного літального апарату. Встановлено, що для реалізації на практиці реальної програми керування польотом безпілотного літального апарату є необхідним застосування систематичного процесу проєктування та моделювання адаптивної мікропроцесорної системи керування використовуючи алгоритми адаптивного керування зі зворотнім зв'язком L1. Наведено структурну схему адаптивної мікропроцесорної системи автоматичного керування безпілотним літальним апаратом, яка реалізує нелінійну модель та складається з динаміка твердих тіл 6DOF, підсистеми гравітаційна, двигунів та візуалізації.

Література

1. Луцький М.Г. Розвиток міжнародного регулювання та нормативної бази використання безпілотних літальних апаратів / М.Г. Луцький, В.П. Харченко, Д.О. Бугайко // Вісник НАУ. – 2015. – № 4. – С. 5-14. Дьяконов В.П. Генерация и генераторы сигналов / Дьяконов В.П.– Издательство: Л.: Энергия, 2009. – 384 с.

2. Xuan-Mung N. A Multicopter ground testbed for the evaluation of attitude and position controller / Xuan-Mung N., Hong S.K. // Int. J. Eng. Technol. - 2018,. - №7. - p. 65–73.

3. Yu Y. A Quadrotor test bench for six degree of freedom flight / Yu, Y., Ding, X. // J. Intell. Robot. Syst. – 2012. - № 68. – p. 323–338.

4. Lee K.U. Inverse optimal design for position control of a quadrotor / Lee K.U., Choi Y.H., Park J.B.// Appl. Sci. – 2017. – p. 907.

5. Nguyen N.P. Sliding mode thau observer for actuator fault diagnosis of quadcopter UAVs / Nguyen N.P., Hong S.K. // Appl. Sci. - 2018 – p. 1893.

6. Xuan-Mung N. Improved Altitude Control Algorithm for Quadcopter Unmanned Aerial Vehicles / Xuan-Mung N., Hong S.K. // Applied sciences - 2019,. - №9., 2122. - p.1–15.

7. Santos M.C.P. An adaptive dynamic controller for quadrotor to perform trajectory tracking tasks / Santos M.C.P., Rosales C.D., Sarapura J.A., Sarcinelli-Filho M., Carelli R. // J. Intell. Robot. Syst. – 2019. – p.5–16.

8. Jayakrishnan H.J. Position and attitude control of a quadrotor UAV using super twisting sliding mode / Jayakrishnan H.J. // IFAC Pap. Online – 2016. - p. 284–289.

References

1. Luckij M.G. Rozvitok mizhnarodnogo regulyuvannya ta normativnoyi bazi vikoristannya bezpilotnih litalnih aparativ / M.G. Luckij, V.P. Harchenko, D.O. Bugajko // Visnik NAU. – 2015. – № 4. – S. 5-14. Dyakonov V.P. Generaciya i generatory signalov / Dyakonov V.P.– Izdatelstvo: L.: Energiya, 2009. – 384

2. Xuan-Mung N. A Multicopter ground testbed for the evaluation of attitude and position controller / Xuan-Mung N., Hong S.K. // Int. J. Eng. Technol. - 2018,. - №7. - p. 65–73.

3. Yu Y. A Quadrotor test bench for six degree of freedom flight / Yu, Y., Ding, X. // J. Intell. Robot. Syst. – 2012. - № 68. – p. 323–338.

4. Lee K.U. Inverse optimal design for position control of a quadrotor / Lee K.U., Choi Y.H., Park J.B.// Appl. Sci. – 2017. – p. 907.

5. Nguyen N.P. Sliding mode thau observer for actuator fault diagnosis of quadcopter UAVs / Nguyen N.P., Hong S.K. // Appl. Sci. - 2018 – p. 1893.

6. Xuan-Mung N. Improved Altitude Control Algorithm for Quadcopter Unmanned Aerial Vehicles / Xuan-Mung N., Hong S.K. // Applied sciences - 2019,. - №9., 2122 - p.1–15.

7. Santos M.C.P. An adaptive dynamic controller for quadrotor to perform trajectory tracking tasks / Santos M.C.P., Rosales C.D., Sarapura J.A., Sarcinelli-Filho M., Carelli R. // J. Intell. Robot. Syst. – 2019. – p.5–16.

8. Jayakrishnan H.J. Position and attitude control of a quadrotor UAV using super twisting sliding mode / Jayakrishnan H.J. // IFAC Pap. Online – 2016. - p. 284–289.

Надійшла / Paper received: 14.06.2020 Надрукована / Paper Printed : 01.12.2020

УДК 004.415.2
DOI: 10.31891/2219-9365-2020-66-2-12

СТЕЦЮК М. В., КАШТАЛЬЯН А. С., ГРИБИНЧУК В. І.
Хмельницький національний університет

АРХІТЕКТУРА СПЕЦІАЛІЗОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ З ВРАХУВАННЯМ ВИМОГ ЖИВУЧОСТІ ТА ВІДМОВОСТІЙКОСТІ В УМОВАХ ВПЛИВІВ ЗЛОВМИСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

У статті запропоновано архітектурні рішення для створення спеціалізованих інформаційних систем (ІС) з врахуванням вимог живучості та відмовостійкості в умовах впливів зловмисного програмного забезпечення, а також вимоги до апаратного забезпечення, на якому реалізуються такі архітектури ІС.

Розроблена архітектура та вимоги до її реалізації та апаратної підтримки, які враховують відмовостійкість та живучість, та можуть бути розширені для врахування інших характеристичних величин. Для забезпечення відмовостійкості та живучості ІС розроблено систему заходів в результаті виконання яких отримано ІС вузькоспеціалізованого використання для різних сфер застосування. Живучість ІС забезпечується: резервуванням серверної частини з територіальним рознесенням основного і резервного сервера, особливістю резервування є те, що функцію сервера, в критичний момент, переймає на себе дзеркальний SQL-сервер, який в штатному режимі забезпечує роботу FTP-сервера; резервуванням програмного забезпечення клієнтської частини, особливістю резервування є те, що в якості резерву слугує не спеціально виділений комп'ютерів, а резерв продуктивності окремих клієнтських комп'ютерів, на які, згідно плану резервування, встановлюється програмного забезпечення клієнтської частини, що резервуються, яке в критичний момент буде використовуватись як штатне, не допускаючи втрати функціональності ІС.

Проведені експериментальні дослідження підтверджують можливість застосування запропонованих рішень стосовно архітектури ІС.

У результаті використання розроблених заходів було отримано архітектуру ІС вузькоспеціалізованого використання для різних сферах застосування, де супроводжуванні процеси відносяться до ірреального або нереального часу із досить високими параметрами відмовостійкості, живучості та загалом резилентності.

Ключові слова: інформаційні системи, архітектура, відмовостійкість, живучість, комп'ютерні мережі.

STETSYUK M., KASHTALIAN A., GRIBINCHOOK V.
Khmelnytsky National University

ARCHITECTURE OF SPECIALIZED INFORMATION SYSTEMS, TAKING INTO ACCOUNT THE REQUIREMENTS OF RESISTANCE AND RESISTANCE FROM FAILURE IN THE CONDITIONS OF THE EFFECTS OF MALWARE SOFTWARE

The article proposes architectural solutions for the creation of specialized information systems (IS) taking into account the requirements of survivability and fault tolerance in the conditions of malicious software, as well as the requirements for the hardware on which such IP architectures are implemented.

Developed architecture and requirements for its implementation and hardware support, which take into account fault tolerance and survivability, and can be extended to take into account other characteristics. To ensure fault tolerance and survivability of IP, a system of measures has been developed, as a result of which IPs of narrowly specialized use for different areas of application have been obtained. The survivability of the IS is provided by: redundancy of the server part with the territorial separation of the main and backup server, the feature of redundancy is that the server function, at a critical moment, takes over the mirror SQL-server, which in normal mode provides FTP-server; reservation of the software of the client part, the peculiarity of the reservation is that the reserve is not a dedicated computer, and the performance reserve of individual client computers, which, according to the backup plan, is installed software of the client part of the reserved, which in the critical moment will be used as a regular, preventing the loss of IP functionality.

The conducted experimental researches confirm the possibility of application of the offered decisions concerning IP architecture.

As a result of using the developed measures, the architecture of IP of specialized use for different areas of application was obtained, where the accompanying processes belong to unreal or unreal time with rather high parameters of fault tolerance, survivability and overall resistance.

Keywords: information systems, architecture, fault tolerance, survivability, computer networks.

Вступ. Постановка задачі дослідження. Відмовостійкість та живучість [1] забезпечують ефективність ІС, яка досягається різними шляхами. Одним із її параметрів є час недоступності, тобто час, коли система не в змозі виконувати свої функції в рамках вимог до неї. Для різних систем цей час різний і знаходиться в діапазоні від нуля до певної порогової прийнятної величини. Для спеціалізованих ІС, які функціонують в корпоративних комп'ютерних мережах та виконують функцію інформаційного забезпечення в такій вузькоспеціалізованій предметній області, як фінансово-господарська діяльність в різних сферах застосування, цей параметр значно вище нуля, але вимоги до таких ІС теж достатньо високі, особливо при постійному зростанні їх кількісних параметрів функціонування (збільшення числа користувачів, складності інформаційних потоків та об'ємів оброблюваних даних) та роботи в умовах впливів зловмисного ПЗ.

Живучість розробленої ІС забезпечується: резервуванням серверної частини ІС з територіальним рознесенням основного і резервного сервера, особливістю резервування є те, що функцію сервера, в критичний момент, переймає на себе дзеркальний SQL-сервер, який в штатному режимі забезпечує роботу FTP-сервера; резервуванням програмного забезпечення клієнтської частини, особливістю якого є те, що в якості резерву слугує не спеціально виділений комп'ютер, а резерв продуктивності окремих клієнтських комп'ютерів, на які, згідно плану резервування, встановлюється ПЗ клієнтської частини, що резервуються, яке в критичний момент буде використовуватись як штатне, не допускаючи втрати функціональності ІС.

Відмовостійкість її клієнтської частини ІС забезпечено шляхом виконання комплексу заходів, що включає окрім традиційно апаратної надмірності ще і функціональну надмірність: організація автоматичного оновлення системного та прикладного ПЗ клієнтських ПК шляхом моніторингу його актуальності із заданою періодичністю; алгоритми процедур, які реалізують критичні функції клієнтської частини ІС, із включенням в них нетривіального (інтелектуального) блоку обробки помилок, що виконується паралельно із самою процедурою; використання нетривіальних редакторів даних, які включають до свого алгоритму роботи інтерактивну процедуру, що виключає неконрольоване маніпулювання даними бази даних, оператором; реалізацією критичних по використанню ресурсів, розрахункових процедур із можливістю оперативного вибору місця їх виконання, що не допускає перевантаження засобів апаратної платформи для ІС. В цих умовах актуальності набирає питання розробки таких архітектур спеціалізованих ІС, які б могли підтримувати свою живучість та відмовостійкість в умовах впливу зловмисного програмного забезпечення. Це було б одним із елементів з покращення рівня безпеки в корпоративних комп'ютерних мережах. І його розвиток дозволив би створювати функціонально живучіші та відмовостійкіші спеціалізовані ІС. Відомі архітектури недостатньо забезпечують рівні живучості та відмовостійкості, тому метою роботи є подальший розвиток відомих архітектур і створення нових для покращення безпеки в корпоративних комп'ютерних мережах за рахунок підвищення рівнів живучості та стійкості безпосередньо спеціалізованих ІС.

1. Відомі методи створення спеціалізованих ІС на основі врахування критеріїв живучості та відмовостійкості в умовах впливу зловмисного програмного забезпечення

Відмовостійкістю ІС вважатимемо властивість системи зберігати повну або часткову працездатність у випадках відмов окремих елементів, що непов'язані із зовнішніми нерегламентованими діями. Під живучістю інформаційної системи розумітимемо її властивість залишатися працездатною з допустимим зменшенням продуктивності в умовах негативних зовнішніх впливів [1]. Ці поняття визначають таку мету як забезпечення доступності ІТ, що досягається різними шляхами. Від забезпечення цих параметрів в прямій залежності знаходиться ефективність функціонування всієї спеціалізованої ІС.

Інформаційну технологію оцінки надійності технічних об'єктів, структура якої відповідає одному з відомих типів нейронних мереж запропоновано в роботі [2]. В роботах [3, 4] розглянуто хмарні програми як складові з декількох компонентів хмарних служб, що спілкуються між собою через інтерфейси веб-служб. В роботах [5, 6] розроблено забезпечення надійності інформаційних систем. Для підвищення надійності інформаційних систем використано метод, базований на оцінці та нейтралізації ризиків. В роботі [7] показано як налагоджувані програмні системи складаються з великої кількості різних, критичних, некритичних та взаємозалежних конфігурацій. В [8] розглянуто як хмари стають важливою платформою для наукової роботи за рахунок програм. В роботі [9] представлено метод та технологія для уникнення функціональних збоїв під час виконання в прикладних системах. В [10] запропонована проактивна схема відновлення, заснована на міграції служб. В роботі [11] толерантність відмов є головним питанням гарантування доступності та надійності критичних послуг. В роботі [12] показано як хмарні обчислення пропонують нову потужність та гнучкість для високоефективних обчислювальних програм із забезпеченням великої кількості віртуальних машин для обчислювальних програм. В роботах [13–16] кібер-стійкість та кібер-життєздатність представлено як тісно пов'язані між собою поняття. В роботах [17–24] показано вплив на відмовостійкість та живучість ІС комп'ютерних атак та різних типів зловмисного програмного забезпечення.

Відомі архітектури базовані на критеріях забезпечення відмовостійкості та живучості спеціалізованих ІС недостатньо систематизовані та не завжди можуть бути реалізовані через специфіку використання. Тому, необхідним є подальше дослідження та розробка нових архітектур ІС, які б дозволили покращити їх відмовостійкість та живучість, зокрема і від кібер-атак та зловмисного програмного забезпечення.

2. Забезпечення живучості та відмовостійкості спеціалізованих ІС в умовах руйнуючого впливу зловмисного програмного забезпечення за рахунок удосконалення архітектур систем

Основними напрямами для підвищення живучості та відмовостійкості ІС є внесення надмірності в конфігурацію апаратних і програмних засобів, підтримуючої інфраструктури, резервування інформаційних ресурсів (програм та даних). При цьому ІС повинна відповідати наступним основним вимогам: система повинна будуватись так, щоб в ній був відсутній компонент (ресурс), відмова якого призведе до повної відмови всієї системи. Для систем реального часу, додатково, накладаються часові обмеження досягнення результату. Розглядатимемо спеціалізовану ІС, яка відноситься до систем ірреального часу. Тому часові обмеження для неї набагато менш жорсткі, порівняно з системами реального часу. В зв'язку з вибраною для

розгляду архітектурою реалізації ІС, яка складається із серверної та клієнтської частин, то відповідно розглядатимемо питання відмовостійкості та живучості в співвіднесенні до функцій покладених на них.

Головною властивістю відмовостійкості є прозорість відмов її окремих компонентів для кінцевого користувача. Це означає, що відмовостійка система автоматично змінює свою конфігурацію у випадку відмови. Її програмне забезпечення в процесі виконання шукає обхідні шляхи, намагаючись в умовах відмови, привести виконувану функцію до успішного завершення. Для ІС, призначених для інформаційного забезпечення у вузькій спеціалізованій предметній області, наприклад фінансово-господарська діяльність закладу вищої освіти, буде доцільним відмовитись від автоматичної системи керування відмовостійкістю на користь автоматизованої. При такому підході частина дорогих функцій управління надмірностями, присутніми в ІС, буде покладена на людину, якщо це не загрожує можливими значними втратами. Але вирішенням задачі побудови ІС, є не забезпечення максимально можливої відмовостійкості системи, а знаходження прийнятного балансу параметрів системи, в рамках певного технологічного базису. А, також, в тому числі враховуючи вимоги критерію «відмовостійкість \ вартість». Дослідимо вирішення питань забезпечення відмовостійкості ІС при використанні такої стратегії. Проаналізуємо фактори, що негативно впливають на відмовостійкість ІС зі сторони клієнта. Це потрібно для того, щоб оцінити і виробити адекватні заходи протидії. Схему впливу негативних факторів на відмостійкість клієнтської частини спеціалізованої ІС зображено на рис. 1.

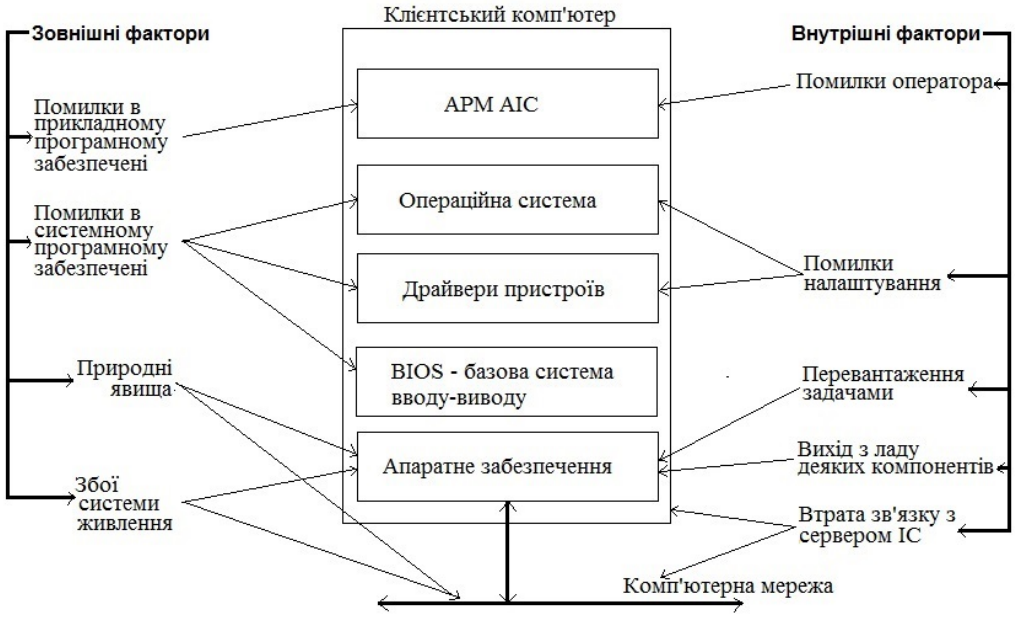
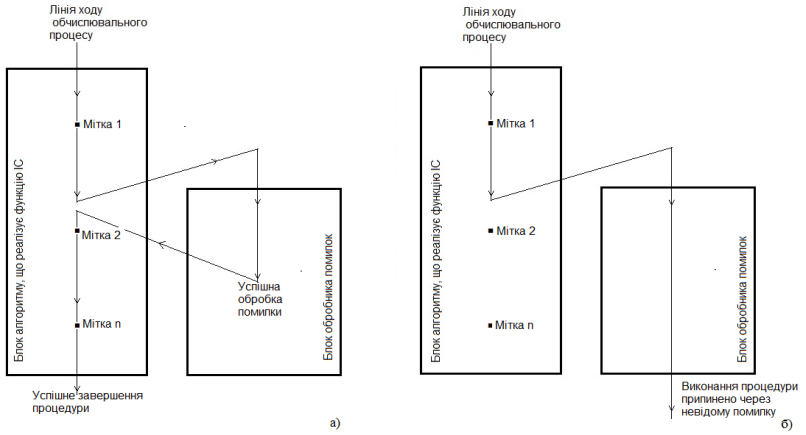


Рис. 1. Схема дії негативних факторів, що впливають на відмовостійкість клієнтської частини спеціалізованої ІС

Негативні фактори, що впливають на відмовостійкість клієнтської частини ІС поділено на зовнішні та внутрішні. Серед зовнішніх факторів найбільшу загрозу представляють собою збої в роботі енергосистем живлення та природні явища, які можуть призвести до відмов компонентів комп’ютерів та комп’ютерних мереж. Іншим важливим фактором є помилки в коді системного програмного забезпечення. Зменшити його прояви можна шляхом використання програмного забезпечення з автоматичним налаштуванням, що не завжди прийнятно, та залученням більш кваліфікованого персоналу.

Для прикладного програмного забезпечення, до якого відносяться клієнтські частини спеціалізованої ІС, то критичні помилки, які проявились в ході експлуатації робочих місць, фіксуються разом із своїми параметрами в реєстрі системи в автоматичний спосіб і, в подальшому використовується для аналізу з метою усунення причин, що їх викликали. Це досягається завдяки підходу, який базований на привнесенні деякої надмірності в програмне забезпечення клієнтської частини ІС. З цією метою всі розрахункові процедури, які можуть містити критичні для функціонування помилки, розроблені з дотриманням певного однотипного шаблону побудови алгоритму її виконання. Суть алгоритму відображена на рис. 2.

В цій структурі алгоритм виконання будь-якої нетривіальної процедури розділяється на два взаємодіючих блоки. В першому блоці реалізується функція процедури ІС, а в другому обробник помилок. В процесі виконання деякої процедури, яка реалізує одну із функцій компоненти ІС, обидва блоки взаємодіють між собою, передаючи управління обчислювальним процесом один одному, поки виконувана функція не завершиться. Його суть полягає в тому, що алгоритм, який реалізує функцію ІС, розділяється маркерами (мітка 1,..., мітка *n* на рис. 2) на фрагменти за принципом функціональної завершеності.



Мал. 2. Модель роботи алгоритма відмовостійкої процедури. а) для випадку успішного завершення процедури після виникнення помилки; б) для випадку, коли помилка., невідома для обробника помилок.

Рис. 2. Модель роботи алгоритму відвостійкої процедури:
***а*) для випадку успішного завершення процедури; *б*) для випадку, коли помилка, невідома для обробника помилок**

Перед початком виконання поточного фрагменту алгоритму в реєстр фатальних помилок заноситься інформація про гіпотетично можливу помилку (код екземпляра робочого місця клієнта, код функції, номер мітки, час тощо). У подальшому можливі наступні варіанти розвитку подій:

1. Фрагмент алгоритму функції успішно виконався. В цьому випадку інформація в реєстрі про помилку, що не сталась, знищується, а обчислювальний процес переходить до виконання наступного фрагмента.

2. У процесі виконання фрагменту сталась помилка, але вона успішно локалізована обробником помилок (рис. 2, *а*). В цьому випадку інформація про помилку також може бути видалена з реєстру.

3. У процесі виконання фрагмента сталась помилка, яка не була локалізована обробником помилок (рис. 2, *б*). В цьому випадку інформація про можливу помилку залишиться в реєстрі.

Більш детальніше алгоритм виконання нетривіальної процедури із застосуванням вище згаданого шаблону зображено на рис. 3. Такий підхід до побудови алгоритму виконання функції ІС дозволяє фіксувати в реєстрі помилок, також, і інформацію про помилки, викликані збоями або критичними відмовами в апаратному забезпечені клієнтського комп'ютера, його системного програмного забезпечення.

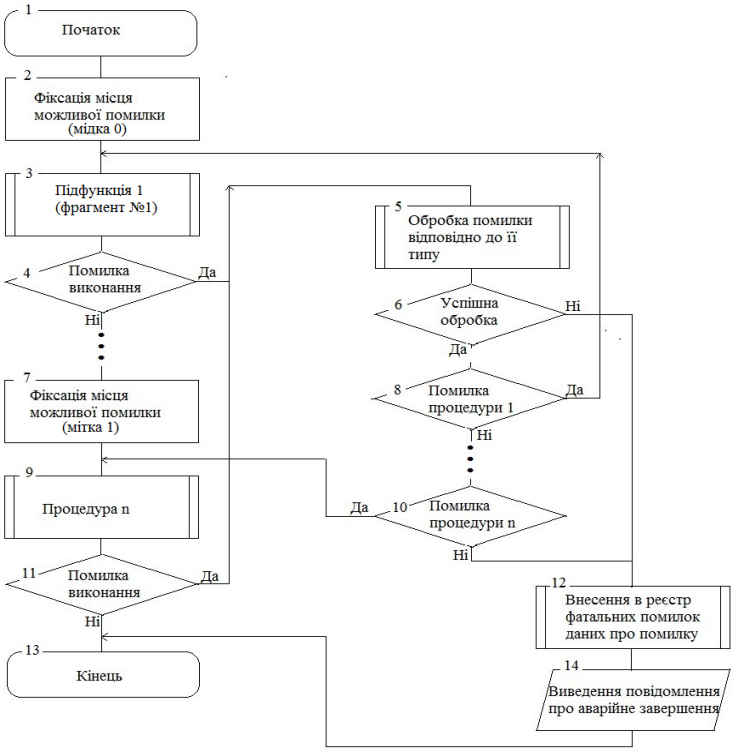


Рис. 3. Алгоритм обробки помилок в підсистемі забезпечення відмовостійкості

Зібрана в такий спосіб інформація про фатальні помилки, що стались в процесі функціонування ІС, дозволяє їх класифікувати та, в процесі подальшого аналізу виявити слабкі ланки з метою їх усунення, шляхом удосконалення програмного забезпечення клієнтської частини.

Розглянемо внутрішні фактори, що впливають на відмовостійкість клієнтської частини ІТ (рис. 1) та методи, які були застосовані з метою його зменшення. Перший з них, за частотою виникнення, відбувається через помилки оператора. Ця проблема вирішена шляхом використання типового редактора даних, в якому всі процедури внесення змін в базу даних реалізовані з використанням шаблона (рис. 4), структура якого включає надмірності у вигляді блоків алгоритму, які передбачають перевірку дій оператора.

Рис. 4. Алгоритм шаблону реалізації функцій редагування баз даних

Як видно з блок-схеми шаблона типового редактора (рис. 4), оператор не має змоги прямого редагування даних. Всі його дії по маніпулюванню даними знаходяться під контролем процедур попередньої перевірки, які включають в себе набір правил (допустима повнота внесення даних, знаходження значень в заданих діапазонах, відсутність протиріч з раніше внесеними даними і т.д.), контекстно зв’язаних із виконуваною функцією. Таким чином, фактор помилок оператора знімається, шляхом ускладнення алгоритму роботи редактора даних.

Наступним із значимих внутрішніх факторів, що негативно впливають на відмостійкість є перевантаження апаратної платформи клієнтського комп’ютера задачами, що може різко погіршити часові параметри виконуваних завдань клієнтською частиною ІС, або навіть зробити неможливою його роботу, через вичерпання технічних ресурсів. Щоб нейтралізувати дію цього фактора, при розробці програмного забезпечення, а саме тієї його частини, яка відповідальна за реалізацію «бізнес-логіки» застосоване функціональне резервування (рис. 5).

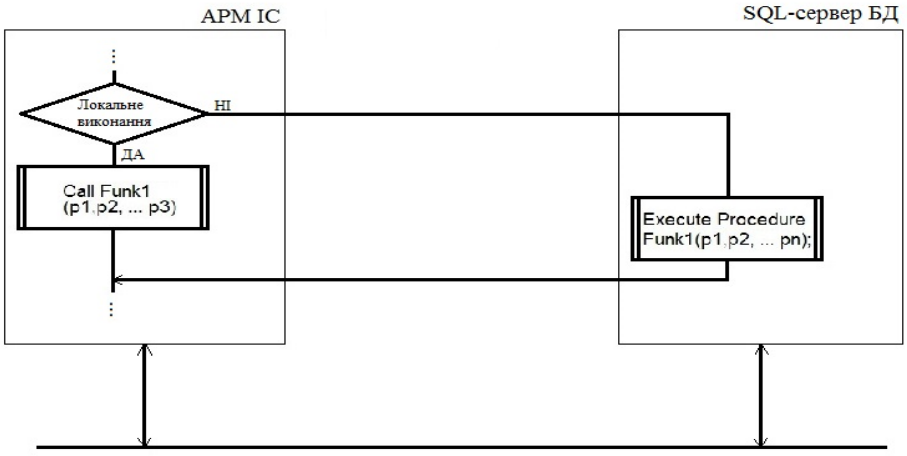


Рис. 5. Застосування функціонального резервування функцій ІС

Наявність функціонального резерву «важких» розрахункових функцій дозволяє здійснювати маневр обчислювальними потужностями апаратної платформи, в разі перевантаження окремих її ланок, підвищуючи таким чином відмовостійкість.

Таким чином, відмовостійкість клієнтської частини забезпечено шляхом виконання комплексу заходів, що включає апаратну та функціональну надмірності: живлення клієнтських ПК від окремої лінії з пристроями захисту; використання пристроїв грозозахисту в лініях комп'ютерної мережі; організація автоматичного оновлення системного програмного забезпечення клієнтських ПК; розробка алгоритмів процедур, які реалізують критичні функції клієнтської частини ІС, із включенням в них нетривіального (інтелектуального) блоку обробки помилок, що виконується паралельно із самою процедурою; використання нетривіальних редакторів даних, які включають до свого алгоритму роботи інтерактивну процедуру, що виключає неконтрольоване маніпулювання даними бази даних, оператором; реалізацією критичних по використанню ресурсів, розрахункових процедур із можливістю оперативного вибору місця їх виконання, що не допускає перевантаження апаратних засобів. Отже, процес забезпечення відмовостійкості є неперервним протягом всього життєвого циклу ІС. Він розпочинається з планування заходів забезпечення відмовостійкості, що проектується і триває до часу завершення її функціонування взагалі.

Показники живучості в складній системі: багатофункціональність окремих компонент; наявність єдиної (головної) мети функціонування всієї системи; можливість не тільки інформаційного обміну між окремими компонентами, але й інформаційної взаємодії з користувачами; наявність засобів захисту, контролю, діагностики й самоорганізації. Задача аналізу структурної живучості потребує визначення: системної архітектури, необхідної для виконання цілі функці-онування ІС у деякий момент або проміжок часу, коли виникають небажані впливи на систему; вимог щодо окремих видів ресурсів системи та їх взаємозв'язку; вимог щодо функціональних можливостей ресурсів системи; особливостей характеру небажаних впливів чи їх наслідків. З рис. 6 видно, як в рамках розробленої системи реалізована задача підвищення живучості ІС, шляхом структурного резервування основних її компонентів, а саме серверної її частини. У випадку виходу з ладу основного сервера ІС, його функції може взяти на себе резервний, який має абсолютно однакові налаштування з основним. При цьому основний та резервний сервери рознесені територіально і живляться з різних ліній. Оскільки вихід з ладу зразу двох серверів є подія малоймовірна, то цим забезпечується висока живучість серверної частини ІС. Реконфігурація реальної системи займає не більше 10 хв. Копія бази даних підтримується в актуальному стані службою реплікацій, тому заміна основної бази даних на базу даних – копію виконується без втрат інформації. Але незначна втрата інформації при такій схемі все ж можлива. Це може трапитись при відмові деяких чутливих компонентів апаратної платформи сервера. Як правило, це останні запущені транзакції, виконання яких буде припинене через відмову обладнання. І якщо це транзакції на зміну інформації в базі даних, то в цьому випадку інформація буде втрачена. Але оскільки така подія в життєвому циклі інформаційної системи сама по собі рідкісна, то такою можливою кількістю втрати інформації можна знехтувати. Після відновлення роботи серверної частини, операторам, чиї транзакції були втрачені, потрібно повторно виконати останні операції, для відновлення втраченої інформації. При регулярному діагностуванні критичного обладнання сервера можна в більшості випадків виявити назріваючу відмову і вчасно замінити відповідний компонент. Так організація роботи дозволяє зменшити вірогідність виходу з ладу серверної частини ІС і тим самим звести нанівець втрату інформації.

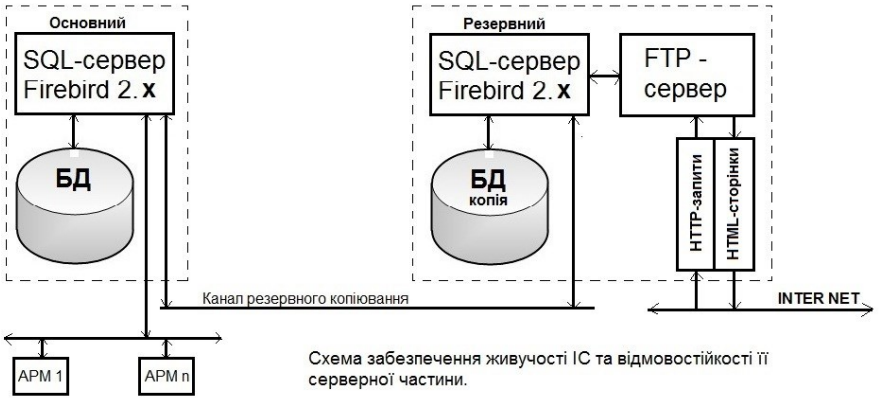


Рис. 6. Схема резервування серверної частини ІС

Таким чином, живучість ІС забезпечується: резервуванням серверної частини ІС з територіальним рознесенням основного і резервного сервера, особливістю резервування є те, що функцію сервера, в критичний момент, переймає на себе дзеркальний SQL-сервер, який в штатному режимі забезпечує роботу

FTP-сервера; резервуванням програмного забезпечення клієнтської частини, особливістю резервування є те, що в якості резерву слугує не спеціально виділений комп'ютерів, а резерв продуктивності окремих клієнтських комп'ютерів, на які, згідно плану резервування, встановлюється програмного забезпечення клієнтської частини, що резервуються, яке в критичний момент буде використовуватись як штатне, не допускаючи втрати функціональності ІС. В результаті використання перелічених заходів було отримано архітектуру ІС вузькоспеціалізованого використання для різних сферах застосування, де супроводжуванні процеси відносяться до ірреального або нереального часу із досить високими параметрами відмовостійкості, живучості та загалом резилентності.

3. Експерименти

Для визначення на скільки ефективними є запропоновані рішення із забезпечення відмовостійкості та живучості проведемо порівняння критерію ефективності для ІТ без забезпечення відмовостійкості та живучості і з включенням цих характеристик на основі формули (1):

$$K_e(S_{IT}) = \alpha_{1,j,p,q} \cdot \frac{T_{f_1(s_i),1} - (T_{f_1(s_i),2} + T_{f_1(s_i),3})}{T_{f_1(s_i),1}} + \alpha_{2,j,p,q} \cdot \frac{T_{f_2(s_i),1} + T_{f_2(s_i),2}}{T_{f_2(s_i),1}}, \quad (1)$$

де $\alpha_{1,j,p,q}$ – коефіцієнт для значення, яке визначає відмовостійкість в кількісних одиницях; $\alpha_{2,j,p,q}$ – коефіцієнт для значення, яке визначає живучість в кількісних одиницях; $\alpha_{1,j,p,q} + \alpha_{2,j,p,q} = 1$.

Значення величини критерія ефективності ІТ, в якій не забезпечуються вимоги відмовостійкості і живучості отримуємо з формули (1) так: 1) вирішення проблем, пов'язаних із відсутністю забезпечення в ІТ реалізованих відмовостійкості та живучості, покладено на оператора чи адміністратора, який постійно моніторить функціонування ІТ; вирішення проблемних ситуацій здійснюється тільки при їх виявленні. Ефективним значенням є значення мінімально відхилене від одиниці. Результати забезпечення відмовостійкості та живучості спеціалізованої ІТ зображені в реалізованій ІТ на рис. 7.

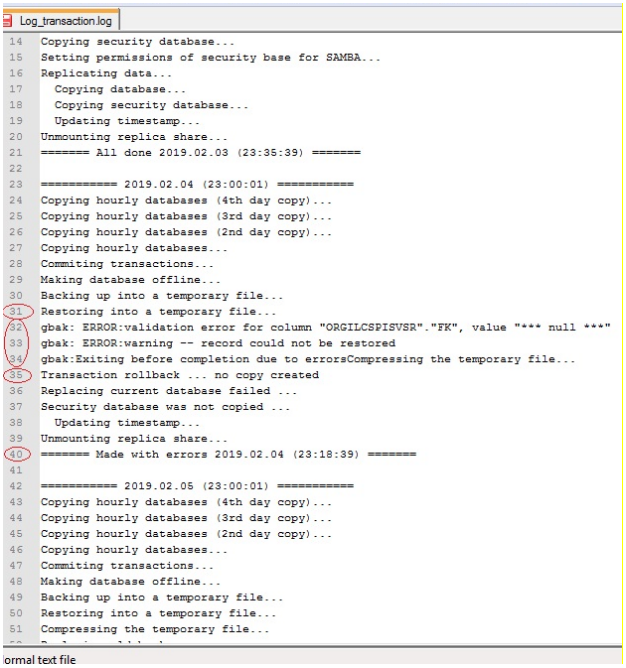


Рис. 7. Фрагмент лог-файла підсистеми резервного копіювання бази даних

Цей фрагмент відображає роботу підсистеми транзакцій бази даних під час її резервного копіювання. При виконані процедури створення резервної копії бази даних утилітою GBAK 4 лютого 2019 року сталась помилка в даних, що призвела до відкату транзакції. Критичні позиції виділені.

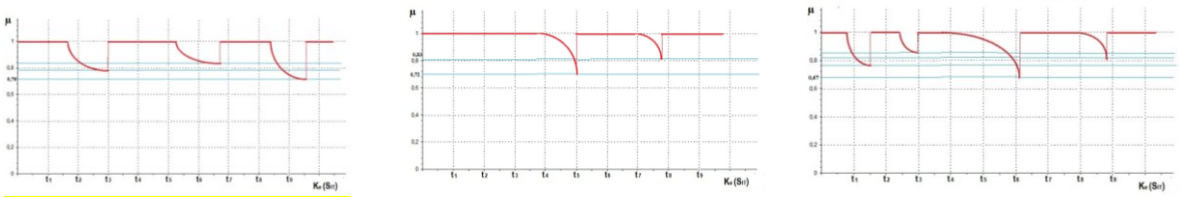
Позиція 31. Створення тимчасового файла бази даних.

Позиція 32–34. Повідомлення утиліти GBAK про помилку при спробі запису в поле [FK] таблиці ORGILCSPISVSR значення по умовчанню визначника NULL.

Позиція 35. Відкат поточної транзакції через помилку.

Позиція 40. Сповіщення, що процедура створення резервної копії завершилась із помилками.

Результати відмовостійкості, графік проявів живучості та графік відображення одночасних проявів та відмовостійкості та живучості зображені на рис. 8.



а *б* *в*

Рис. 8. Графік відмовостійкості (*а*); графік проявів живучості (*б*);
графік відображення одночасних проявів та відмовостійкості та живучості (*в*)

Результати дослідження підтверджують високий рівень стійкості та виживання в корпоративних комп'ютерних мережах, який становить понад 75%.

Напрями подальших досліджень. Важливим напрямом подальших досліджень для покращення ефективності ІС є розробка методу забезпечення ефективного захисту інформації в архітектурі ІС. Їх врахування в загальному критерії визначенні ефективності ІС дозволить збалансувати такі величини як живучість, відмовостійкість та захист інформації, виражені в кількісному вигляді, та стане основою розробки спеціалізованої ІС з покращеними характеристиками.

Висновки. Таким чином, розроблена архітектура та вимоги до її реалізації та апаратної підтримки, які враховують відмовостійкість та живучість, та можуть бути розширені для врахування інших характеристичних величин. Для забезпечення відмовостійкості та живучості ІС розроблено систему заходів в результаті виконання яких отримано ІС вузькоспеціалізованого використання для різних сфер застосування, де супроводжуванні процеси відносяться до ірреального або нереального часу із досить високими параметрами відмовостійкості, живучості та загалом резилентності і, в той же час, прийнятним рівним фінансових витрат на її експлуатацію. Проведені експериментальні дослідження підтверджують можливість застосування запропонованих рішень стосовно архітектури ІС.

Література

1. ДСТУ 3396.2-97 Protection of information. Technical protection of information. Terms and definitions. State Committee of Ukraine, Kyiv (1997) [in Ukrainian]

2. Savelyeva, O. S., Krasnozhon, O. M., Lebedeva, O. U. (2014). Using the structural fault-tolerance index in project designing. Odes'kyi Politechnichnyi Universytet. Pratsi, 2, 130–135. doi: 10.15276/opu.2.44.2014.24.

3. Liu J, Zhou J, Buyya R (2015) Software rejuvenation based fault tolerance scheme for cloud applications In: 2015 IEEE 8th International Conference on Cloud Computing, 1115–1118, New York. https://doi.org/10.1109/CLOUD.2015.164.

4. Liu J, Wang S, Zhou A, Kumar SAP, Yang F, Buyya R (2016) Using Proactive Fault-Tolerance Approach to Enhance Cloud Service Reliability. IEEE Trans Cloud Comput PP(99):1–1. http://dx.doi.org/10.1109/TCC.2016.2567392.

5. S. Boranbayev, S. Altayev, A. Boranbayev. Applying the method of diverse redundancy in cloud based systems for increasing reliability, in Proceedings of the 12th International Conference on Information Technology: New Generations (ITNG 2015) (Las Vegas, Nevada, 2015), pp. 796–799.

6. Boranbayev A., Boranbayev S., Yersakhanov K., Nurusheva A., Taberkhan R. (2018) Methods of Ensuring the Reliability and Fault Tolerance of Information Systems. In: Latifi S. (eds) Information Technology - New Generations. Advances in Intelligent Systems and Computing, vol 738. Springer, Cham.

7. Chinnaiah, M., Niranjan, N. Fault tolerant software systems using software configurations for cloud computing. J Cloud Comp 7, 3 (2018). https://doi.org/10.1186/s13677-018-0104-9.

8. Zhu X, Wang J, Guo H, Zhu D, Yang LT, Liu L (2016) Fault-tolerant scheduling for real-time scientific workflows with elastic resource provisioning in virtualized clouds. IEEE Trans Parallel Distrib Syst 27(12):3501–3517. https://doi.org/10.1109/TPDS.2016.2543731.

9. Nicolo P (2013) A frame work for self-healing software systems In: IEEE 35th International Conference on Software Engineering (ICSE), 1397–1400. https://doi.org/10.1109/ICSE.2013.6606726.

10. Zhao W, Wenbing Z, Melliar-Smith PM, Moser LE (2010) Fault Tolerance Middleware for Cloud Computing In: 2010 IEEE 3rd International Conference on Cloud Computing, 67–74, Miami. https://doi.org/10.1109/CLOUD.2010.26.

11. Bala A, Chana I (2012) Fault tolerance- challenges, techniques and implementation in cloud computing, ISSN (Online): 16940814. IJCSI Int J Comput Sci 9(1). www.IJCSI.org.

12. Egwutuoha IP, Chen S, Levy D, Selic B (2012) A fault tolerance framework for high performance computing in cloud, Cluster, Cloud and Grid Computing (CCGrid) In: Proceedings of the 12th IEEE/ACM international symposium. 13-16 May, 709–710. https://doi.org/10.1109/CCGrid.2012.80.

13. S. Pitcher, "New DoD Approaches on the Cyber Survivability of Weapon Systems (25 March 2019)," 25 March 2019. [Online]. Available: https://www.itea.org/wp-content/uploads/2019/03/Pitcher-Steve.pdf.

14. D. J. Bodeau, R. D. Graubart, R. M. McQuaid and J. Woodill, "Cyber Resiliency Metrics and Scoring in Practice: Use Case Methodology and Examples (MTR 180449)," The MITRE Corporation, Bedford, MA, 2018.

15. D. Fitzpatrick, D. Bodeau, R. Graubart, R. McQuaid, C. Olin and J. Woodill, "(DRAFT) Cyber Resiliency Evaluation Framework for Weapon Systems: Foundational Principles and Their Potential Effects on Adversaries," The MITRE Corporation, Bedford, MA, 2019.

16. NIST, "Initial Public Draft of NIST SSP 800-160 Volume 2, Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems," 21 March 2018. [Online]. Available: https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft.pdf.

17. Lysenko, S., Savenko, O., Kryshchuk, A., Kljots, Y. Botnet detection technique for corporate area network. In: Proc. of the 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems, pp. 363-368 (2013).

18. Savenko, O., Lysenko, S., Nicheporuk, A., Savenko, B.: Metamorphic Viruses' Detection Technique Based on the Equivalent Functional Block Search. CEUR Workshop, Vol. 1844, pp. 555–569 (2017).

19. Savenko, O., Lysenko, S., Nicheporuk, A., Savenko, B.: Approach for the Unknown Metamorphic Virus Detection. In: 9-th IEEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems. Technology and Applications, pp. 453–458 (2017).

20. Pomorova, O., Savenko, O., Lysenko, S., Kryshchuk, A. and Nicheporuk, A.: A technique for detection of bots which are using polymorphic code. In: 21st International Conference, CN, Springer, Brunów, Poland, pp. 265-276 (2014)

21. Kondratenko, Y., Kondratenko, N.: Soft Computing Analytic Models for Increasing Efficiency of Fuzzy Information Processing in Decision Support Systems. Chapter in book: Decision Making: Processes, Behavioral Influences and Role in Business Management, R. Hudson (Ed.), Nova Science Publishers, New York, 41-78 (2015)

22. Savenko O.S Research of methods of antiviral diagnostics of computer networks / O.S Savenko, S.M Lysenko // Visnyk of Khmelnytsky National University. Technical sciences. - 2007. - № 2, v. 2. - P. 120–126.(in Ukrainian)

23. Savenko O.S., Payuk V.P., Savenko B.O, Kashtalyan A.S. Models of undocumented software bookmarks in local computer networks / Measuring and computing equipment in technological processes / 2019. - №2. - P.84-90.(in Ukranian)

24. Савенко О.С. Модель процесу пошуку троянських програм в персональному комп'ютері / О.С. Савенко, С.М. Лисенко //Радіоелектронні і комп'ютерні системи. – 2008. – №7. – С.87-92.

References

1. DSTU 3396.2-97 Protection of information. Technical protection of information. Terms and definitions. State Committee of Ukraine, Kyiv (1997) [in Ukrainian]

2. Savelyeva, O. S., Krasnozhon, O. M., Lebedeva, O. U. (2014). Using the structural fault-tolerance index in project designing. Odes'kyi Politechnichnyi Universytet. Pratsi, 2, 130–135. doi: 10.15276/opu.2.44.2014.24.

3. Liu J, Zhou J, Buyya R (2015) Software rejuvenation based fault tolerance scheme for cloud applications In: 2015 IEEE 8th International Conference on Cloud Computing, 1115–1118, New York. https://doi.org/10.1109/CLOUD.2015.164.

4. Liu J, Wang S, Zhou A, Kumar SAP, Yang F, Buyya R (2016) Using Proactive Fault-Tolerance Approach to Enhance Cloud Service Reliability. IEEE Trans Cloud Comput PP(99):1–1. http://dx.doi.org/10.1109/TCC.2016.2567392.

5. S. Boranbayev, S. Altayev, A. Boranbayev. Applying the method of diverse redundancy in cloud based systems for increasing reliability, in Proceedings of the 12th International Conference on Information Technology: New Generations (ITNG 2015) (Las Vegas, Nevada, 2015), pp. 796–799.

6. Boranbayev A., Boranbayev S., Yersakhanov K., Nurusheva A., Taberkhan R. (2018) Methods of Ensuring the Reliability and Fault Tolerance of Information Systems. In: Latifi S. (eds) Information Technology - New Generations. Advances in Intelligent Systems and Computing, vol 738. Springer, Cham.

7. Chinnaiah, M., Niranjan, N. Fault tolerant software systems using software configurations for cloud computing. J Cloud Comp 7, 3 (2018). https://doi.org/10.1186/s13677-018-0104-9.

8. Zhu X, Wang J, Guo H, Zhu D, Yang LT, Liu L (2016) Fault-tolerant scheduling for real-time scientific workflows with elastic resource provisioning in virtualized clouds. IEEE Trans Parallel Distrib Syst 27(12):3501–3517. https://doi.org/10.1109/TPDS.2016.2543731.

9. Nicolo P (2013) A frame work for self-healing software systems In: IEEE 35th International Conference on Software Engineering (ICSE), 1397–1400. https://doi.org/10.1109/ICSE.2013.6606726.

10. Zhao W, Wenbing Z, Melliar-Smith PM, Moser LE (2010) Fault Tolerance Middleware for Cloud Computing In: 2010 IEEE 3rd International Conference on Cloud Computing, 67–74, Miami. https://doi.org/10.1109/CLOUD.2010.26.

11. Bala A, Chana I (2012) Fault tolerance- challenges, techniques and implementation in cloud computing, ISSN (Online): 16940814. IJCSI Int J Comput Sci 9(1). www.IJCSI.org.

12. Egwutuoha IP, Chen S, Levy D, Selic B (2012) A fault tolerance framework for high performance computing in cloud, Cluster, Cloud and Grid Computing (CCGrid) In: Proceedings of the 12th IEEE/ACM international symposium. 13-16 May, 709–710. https://doi.org/10.1109/CCGrid.2012.80.

13. S. Pitcher, "New DoD Approaches on the Cyber Survivability of Weapon Systems (25 March 2019)," 25 March 2019. [Online]. Available: https://www.itea.org/wp-content/uploads/2019/03/Pitcher-Steve.pdf.

14. D. J. Bodeau, R. D. Graubart, R. M. McQuaid and J. Woodill, "Cyber Resiliency Metrics and Scoring in Practice: Use Case Methodology and Examples (MTR 180449)," The MITRE Corporation, Bedford, MA, 2018.

15. D. Fitzpatrick, D. Bodeau, R. Graubart, R. McQuaid, C. Olin and J. Woodill, "(DRAFT) Cyber Resiliency Evaluation Framework for Weapon Systems: Foundational Principles and Their Potential Effects on Adversaries," The MITRE Corporation, Bedford, MA, 2019.

16. NIST, "Initial Public Draft of NIST SSP 800-160 Volume 2, Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems," 21 March 2018. [Online]. Available: https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft.pdf.

17. Lysenko, S., Savenko, O., Kryshchuk, A., Kljots, Y. Botnet detection technique for corporate area network. In: Proc. of the 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems, pp. 363-368 (2013).

18. Savenko, O., Lysenko, S., Nicheporuk, A., Savenko, B.: Metamorphic Viruses' Detection Technique Based on the Equivalent Functional Block Search. CEUR Workshop, Vol. 1844, pp. 555–569 (2017).

19. Savenko, O., Lysenko, S., Nicheporuk, A., Savenko, B.: Approach for the Unknown Metamorphic Virus Detection. In: 9-th IEEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems. Technology and Applications, pp. 453–458 (2017).

20. Pomorova, O., Savenko, O., Lysenko, S., Kryshchuk, A. and Nicheporuk, A.: A technique for detection of bots which are using polymorphic code. In: 21st International Conference, CN, Springer, Brunów, Poland, pp. 265-276 (2014)

21. Kondratenko, Y., Kondratenko, N.: Soft Computing Analytic Models for Increasing Efficiency of Fuzzy Information Processing in Decision Support Systems. Chapter in book: Decision Making: Processes, Behavioral Influences and Role in Business Management, R. Hudson (Ed.), Nova Science Publishers, New York, 41-78 (2015)

22. Savenko O.S Research of methods of antiviral diagnostics of computer networks / O.S Savenko, S.M Lysenko // Visnyk of Khmelnytsky National University. Technical sciences. - 2007. - № 2, v. 2. - P. 120–126.(in Ukrainian)

23. Savenko O.S., Payuk V.P., Savenko B.O, Kashtalyan A.S. Models of undocumented software bookmarks in local computer networks / Measuring and computing equipment in technological processes / 2019. - №2. - P.84-90.(in Ukranian)

24. Savenko O.S. Model of the process of searching for Trojan programs in a personal computer / O.S. Savenko, S.M. Lysenko // Radio electronic and computer systems. - 2008. - №7. - P.87-92. (in Ukrainian)

Надійшла / Paper received: 02.09.2020 Надрукована / Paper Printed : 01.12.2020

УДК 621.317.73
DOI: 10.31891/2219-9365-2020-66-2-13

ФОРКУН Ю. В., ФОРКУН І. В.,
МАКАРИШКІН Д. А., ФЕНЕНКО В. О.
Хмельницький національний університет

СУЧАСНИЙ СТАН ПРОБЛЕМ ПРОМИСЛОВИХ БАГАТОРІВНЕВИХ СИСТЕМ КЕРУВАННЯ НА ОСНОВІ КОНЦЕПЦІЇ SCADA-СИСТЕМ

В статті наведено сучасний стан проблеми промислових багаторівневих систем керування на основі програмно-технічних комплексів SCADA-систем. Проведено аналіз концепції SCADA-систем. Наведені їх переваги та недоліки, а також досліджено архітектури та компоненти SCADA-систем. Встановлено, що з урахуванням концепції Індустрії 4.0 та розвитком кіберфізичного виробництва, сучасні SCADA-системи представляють собою відкриті системи промислового Інтернету речей, а тому для забезпечення ефективного проєктування промислових багаторівневих систем керування необхідно використовувати новий підхід до кібербезпеки SCADA-систем, який пов'язаний з взаємозв'язком різних областей безпеки, враховуючи різні її аспекти. Набули подальшого розвитку промислові багаторівневі системи керування з використанням хмарних SCADA-систем.

Ключові слова: промислові багаторівневі системи керування, SCADA-системи, Інтернет речей, безпека SCADA-системи, архітектура та компоненти SCADA-систем.

FORKUN Y., FORKUN I.,
MAKARYSHKIN D., FENENKO V.
Khmelnitsky national university

CURRENT STATE OF PROBLEMS OF INDUSTRIAL MULTILEVEL CONTROL SYSTEMS BASED ON THE CONCEPT OF SCADA-SYSTEMS

Modern development of multilevel control systems is extremely important for the field of industrial automation. Industrial multilevel control systems include components such as control and data acquisition systems (SCADA), distributed control systems, and other control system configurations, such as programmable logic controllers in the industrial sector and critical infrastructure. At the same time, these components of multilevel control systems must meet the unique requirements of a complete integrated automation system, such as performance, reliability and safety. When designing multilevel control systems, it is necessary to take into account their types for a specific task of industrial automation and typical system topologies, identify typical threats and vulnerabilities of such systems and propose solutions and safety measures to reduce associated risks.

The industrial multilevel control system consists of a combination of the following controls, such as electrical, mechanical, hydraulic, pneumatic and other elements. The controls of industrial multi-level control systems work together to achieve industrial goals (eg, fabrication, transportation of materials or energy). A typical industrial multilevel control system may include multiple control cycles, human-machine interfaces (HMIs), and remote diagnostics and maintenance tools built using a number of network protocols. Industrial control processes apply to electricity, water and wastewater, oil and gas, chemicals, transportation, pharmaceuticals, pulp and paper, food and beverages, and discrete manufacturing (such as automobiles, aerospace, and durable goods). The actual implementation of industrial multi-level control systems can be a hybrid that blurs the boundaries between distributed systems and SCADA systems.

The article presents the current state of the problem of industrial multilevel control systems based on software and hardware SCADA-systems. The analysis of the concept of SCADA-systems is carried out. Their advantages and disadvantages are given, as well as the architectures and components of SCADA-systems are studied. It is established that taking into account the concept of Industry 4.0 and the development of cyberphysical production, modern SCADA-systems are open systems of industrial Internet of Things, and therefore to ensure effective design of industrial multilevel control systems it is necessary to use a new approach to cybersecurity SCADA-systems. the relationship of different areas of security, taking into account its various aspects. Industrial multilevel control systems using cloud SCADA systems have been further developed.

Key words: industrial multilevel control systems, SCADA-systems, Internet of Things, security of SCADA-systems, architecture and components of SCADA-systems.

Вступ. Сучасний розвитку багаторівневих систем керування є надзвичайно важливим для галузі промислової автоматизації. До складу промислових багаторівневих систем керування входять такі компоненти як системи керування та збору даних (SCADA), розподілені системи керування та інші конфігурації систем керування, такі як програмовані логічні контролери у промисловому секторі та критичній інфраструктурі. При цьому ці компоненти багаторівневих систем керування мають задовольняти унікальним вимогам цілої комплексної системи автоматизації, таким як, продуктивність, надійність та безпека. Під час проєктування багаторівневих систем керування необхідно враховувати їх типи для конкретної задачі промислової автоматизації та типових топологій системи, визначати типові загрози та вразливості таких систем та пропонувати рішення і рекомендаційні заходи безпеки для зменшення пов'язаних із ними ризиків [1, 2].

Промислова багаторівнева система керування складається з комбінації наступних елементів керування, таких як електричні, механічні, гідравлічні, пневматичні та інші елементи. Елементи керування промислових багаторівневих систем керування працюють разом для досягнення промислових цілей (наприклад, виготовлення, транспортування матеріалів або енергії). Типова промислова багаторівнева

система керування може включати безліч циклів керування, людино-машинні інтерфейси (HMI) та засоби віддаленої діагностики та обслуговування, побудовані з використанням ряду мережевих протоколів. Промислові процеси керування застосовуються для електроенергії, води та стічних водах, нафті та газі, хімічних речовинах, транспорті, фармацевтиці, целюлозі та папері, продуктах харчування та напоях та дискретному виробництві (таких як автомобілі, аерокосмічна промисловість та товари тривалого користування). Фактична реалізація промислових багаторівневих систем керування може бути гібридом, який стирає межі між системами розподіленим та SCADA-системами.

На основі інтеграції IT-можливостей в існуючі фізичні системи, що в свою чергу доповнює або замінює фізичне керування було розроблено багато сучасних промислових багаторівневих систем керування. Наприклад, вбудовані цифрові елементи керування замінили аналогові механічні елементи керування в обертових машинах та двигунах. Зростання вартості та продуктивності зумовило цей розвиток і призвело до багатьох сучасних «розумних» технологій, таких як розумні мережі, розумне транспортування, розумні будівлі та розумне виробництво. Однак незважаючи на те, що це збільшує зв'язок та важливість таких систем, це також ставить більш високі вимоги до їхньої пристосованості, стійкості та безпеки. Інженерна технологія промислових багаторівневих систем керування продовжує розвиватися, надаючи нові функції, зберігаючи типовий тривалий життєвий цикл цих систем. Впровадження IT-функцій у фізичні системи представляє нову поведінку, яка впливає на безпеку. У теперішній час розробляються інженерні моделі та аналіз для вирішення цих нових особливостей, включаючи взаємозалежність безпеки, конфіденційності та впливу на навколишнє середовище.

Аналіз останніх досліджень та публікацій. Основні операції та компоненти, які виконуються промисловими багаторівневими системами керування представлені на рисунку 1 [1]. Типова промислова багаторівнева система керування включає безліч циклів керування, людино-машині інтерфейси, засоби віддаленої діагностики та обслуговування, які побудовані з використанням масиву мережевих протоколів на багатошаровій архітектурі мережі. Шлейф керування використовує датчики, виконавчі механізми та контролери (наприклад програмований логічний контролер) для маніпулювання певними керуючими процесами. Датчик - це пристрій, який вимірює певні фізичні властивості, а потім надсилає цю інформацію контролеру як керовану змінну. Контролер інтерпретує сигнал відповідно до алгоритму керування і заданого значення цілі, генерує відповідну маніпульовану змінну і передає його на привід. Пускачі, такі як, регулюючі клапани, вимикачі, автоматичні вимикачі та двигуни використовуються для безпосереднього керування керованим процесом на основі команд контролера.

Рис. 1. Операції та компоненти промислових багаторівневих систем керування

Оператори та інженери використовують людино-машині інтерфейси для моніторингу та регулювання заданих значень, алгоритмів керування та налаштування параметрів в контролері. Людино-

машині інтерфейси також відображають інформацію про стан процесу та історичну інформацію. Службові програми діагностики та обслуговування використовуються для запобігання, виявлення та відновлення після ненормальних операцій або збоїв. Іноді ці цикли керування вкладені та/або каскадно – задана точка в одному циклі базується на змінній процесу, яка визначена іншим циклом. Цикл рівня керування та цикл низького рівня працюють безперервно протягом усього процесу, а час циклу становить мілісекунди до хвилин.

Під час проєктування промислової багаторівневої системи керування, є необхідним, визначення ключових факторів, що пов'язані з атрибутами керування, зв'язку, надійності та надмірності промислової багаторівневої системи керування. Оскільки ці фактори значною мірою впливають на розробку промислову багаторівневу систему керування, вони також допоможуть визначити вимоги до безпеки системи. Тому при проектуванні промислової багаторівневої системи керування враховуються наступні вимоги до: контролю часу, географічного розподілу, ієрархії, складності керування, доступності та надійності системи, впливу нестабільності і безпеки [1, 2].

На сьогодні критична інфраструктура зазвичай описується як інфраструктура, яка забезпечує та обслуговує основні послуги системи безпеки, економіки та охорони здоров’я будь-якої країни. Кіберфізична система та Інтернет речей доповнюють традиційну критичну інфраструктуру операціями з великими даними. Список галузей, що належать до критичної інфраструктури зазвичай включають у себе сільське господарство, охорону здоров’я, ядерні реактори, транспорт, енергетичний сектор, цивільна та хімічна інженерія, структура води, дослідження тощо, як представлено на рис. 2. Системи диспетчерського керування та обробка даних (SCADA-системи) при проєктуванні промислових багаторівневих систем керування відіграють ключову роль в управлінні та контролю критичної інфраструктури.

Система SCADA здійснює керування та моніторинг географічно розподілених активів. Історично склалося, що SCADA-системи були обмежені такими системами, як системами передачі енергії, транспортуванням природного газу та керування водою. Сучасний розвиток технологій привів до того, що SCADA-системи використовуються у таких промислових секторах, як металургія, хімічна обробка (переробка), телекомунікації, експериментальне та виробниче обладнання [2]. З розвитком концепції Індустрії 4.0 та промислового Інтернету Речей, сучасні SCADA-системи включають у себе такі компоненти, як CPS / IoT, хмарні технології, аналіз великих даних, штучний інтелект та машинне навчання. Інтеграція цих технологій значно покращує сумісність та спрощує обслуговування і зниження витрат на інфраструктуру.

Рис. 2. Сфера застосувань SCADA-систем

SCADA-системи можуть підвищити ефективність ключових промислових систем і забезпечити більш високу ефективність захисту обладнання. Дайте структуру SCADA. SCADA- системи розроблені для роботи в автономному режимі, а сама SCADA-система була захищена через мережу повітряного зазору та власний протокол. Ось чому оригінальний проєкт SCADA-система, ніколи не включала до свого складу функції безпеки [3, 4]. Однак в останні роки через розширення бізнесу та центральний попит на розподілений програмний моніторинг, система SCADA-система перетворилася на складну відкриту систему, яка є з’єднаною з Інтернетом за допомогою передових технологій. Однак це призвело до того, що система SCADA стала більш вразливою для цілей зловмисників з будь-якої точки світу [5].

Виклад основного матеріалу дослідження. Зазвичай SCADA – це комп’ютерна система, яка широко застосовується для дистанційного керування та моніторингу об’єкту керування. SCADA-система збирає інформація та дані про технологічні процеси, які аналізуються в режимі реального часу. SCADA-

система складається з таких елементів: головний термінал master terminal unit (MTU), комунікація, віддалений термінал remote terminal unit (RTU) та людино-машиний інтерфейс Human-machine-interface (HMI).

Апаратна архітектура SCADA використовує програмовані логічні контролери (PLC) та віддалені термінальні блоки (RTU). Архітектура програмного забезпечення SCADA включає людино-машиний інтерфейс (HMI), центральна база даних та інші користувачі програмне забезпечення [6]. ПЛК і RTU є мікрокомп'ютерами, які взаємодіють з масивом об'єктів, таких як промислові машини, HMI, датчики та кінцеві пристрої, а потім передають інформація від цих об’єктів до комп’ютерів із програмним забезпеченням SCADA. Програмне забезпечення SCADA обробляє, розповсюджує та відображає дані, допомагаючи операторам та іншим працівникам аналізувати дані та приймати важливі рішення. SCADA-системи здатні повідомляти оператора про проблему допомагає йому для її усунення та запобігання подальшій втраті продукту. Найбільший контроль дії виконуються RTU або PLC.

Апаратна система SCADA класифікується на дві основні частини: шари клієнта та сервер даних. Шар клієнта – це шар, який обслуговує людину і машинну взаємодію. Рівень сервера даних – це той, який обробляє більшу частину процесів даних. Програмовані логічні контролери є підключеними до серверів даних безпосередньо або через мережі або шини. SCADA-система використовує, як глобальну мережу (WAN) так, і локальну мережу (LAN), яка складається з Інтернет-протоколів, що використовуються для зв'язку між головною станцією та пристроями, фізичним обладнанням, датчиками, які є підключеними до ПЛК або RTU. RTU перетворює сигнали датчика в цифрові дані і передає цифрові дані MTU. Більшість операцій з моніторингу та контролю виконуються RTU або PLC.

Більшість серверів використовуються для багатозадачності та бази даних у режимі реального часу. Сервери здійснюють збір та обробку даних. SCADA-система складається з програмного забезпечення для забезпечення тенденцій, діагностики даних та керування такою інформацією, як запланований порядок технічного обслуговування, логістичної інформації, детальні схеми для конкретного датчика або машини та за усунення несправностей системи. Взаємозв'язок компонентів зв'язку системи MTU, RTU, HMI, Historian та SCADA є представлені на рис. 3.

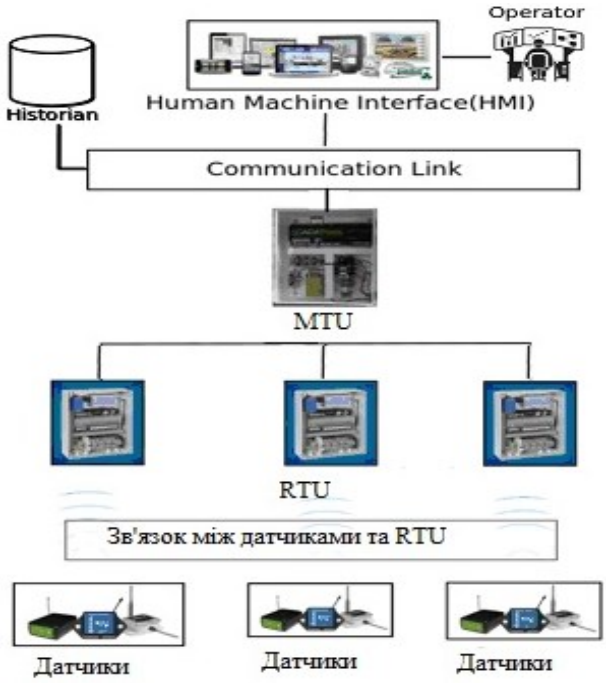


Рис. 3. Взаємозв’язок компонентів зв’язку SCADA-системи

Існують різні типи SCADA-систем, які розглядаються як архітектури SCADA чотирьох різних поколінь: монолітні або ранні системи SCADA (перше покоління); розподілені SCADA-системи (друге покоління); мережеві SCADA-системи (третє покоління); Інтернет речей.

Монолітні або ранні SCADA-системи були незалежними системами без зв'язку з іншими системами. Усі використані протоколи зв'язку були на той час власністю. Функції монолітні системи SCADA на початку першого покоління обмежується лише датчиками моніторингу в системі та позначенням будь-яких операцій у разі перевищення запрограмованих рівнів тривоги. У таких SCADA-системах резервування було досягнуто за допомогою резервної системи мейнфреймів, підключеної до всіх сайтів RTU, і використовувалася лише у випадку виходу з ладу первинної системи мейнфреймів, у цій архітектурі RTU зв’язується з MTU з використанням глобальних мереж (WAN), як показано на рис. 4 [7].

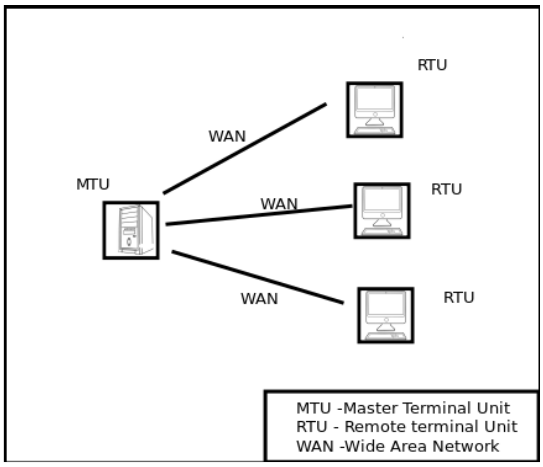


Рис. 4. Мережева архітектура монолітної SCADA-систем

Розподілені SCADA-системи (керування), архітектура, якої представлена на рис. 5, мають спільний доступ до функцій керування розподілений між декількома системами, які підключені один з одним за допомогою локальної мережі LAN [8]. При цьому кожна станція використовувалася для обміну інформацією в режимі реального часу між системами та її обробки для виконання контрольних завдань для спрацювання сигналізації, пр. певних рівнях можливих проблем, тим самим зменшуючи витрати у порівняні з попереднім поколінням SCADA-систем. Мережеві протоколи все ще не стандартизовані в розподілених SCADA-системах, а безпека установки SCADA-систем ігнорується.

У третьому поколінні SCADA-система може бути зведена до найпростішої компоненти, яка утворюються шляхом з'єднання його за допомогою протоколів зв'язку. У SCADA-системах цього типу, мережа може бути географічно розподілена та зв’язуватися за допомогою глобальної мережі WAN через лінії передачі даних або мобільний зв’язок. Такий тип SCADA-систем використовує Ethernet або оптично волоконний з’єднувач для постійної передачі даних між вузлами. Архітектура мережевих SCADA-систем представлена на рис. 6.

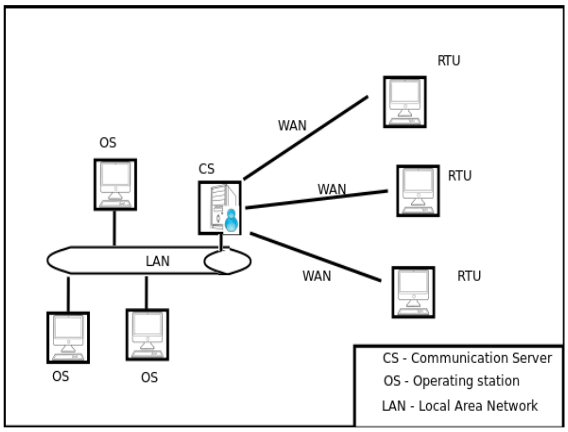


Рис. 5. Мережева архітектура розподіленої SCADA-системи

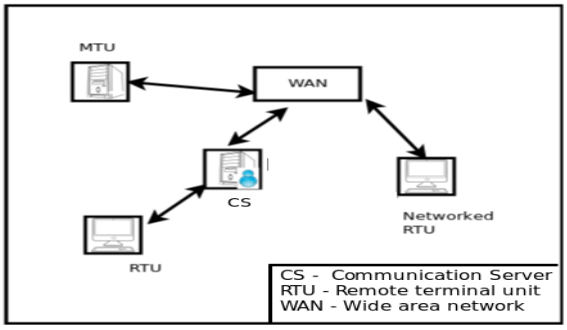


Рис. 6. Мережева SCADA-система

У четвертому поколінні SCADA-систем, за рахунок впровадження Інтернет-технологій (веб-технологій) з'являється можливість користувачам переглядати дані, обмінюватися інформацією та керувати процесами з будь-якої точки світу. Вартість інфраструктури та розгортання SCADA-систем зменшуються шляхом інтеграції технологій Інтернету речей з комерційно доступними хмарними обчисленнями. Технічне обслуговування та інтеграція з попередніми SCADA-системи є більш простим. Це мережа пристроїв зі значним зосередженням на передачі, контролі критичної інформації, отриманні статистичних даних з big data, тому для створення промислового Інтернету речей є необхідними інтегрувати зовнішні системи з існуючими на той момент SCADA-системами, серверними пристроями, протоколами і т.д. [7]. Архітектура четвертого покоління представлена на рис. 7.

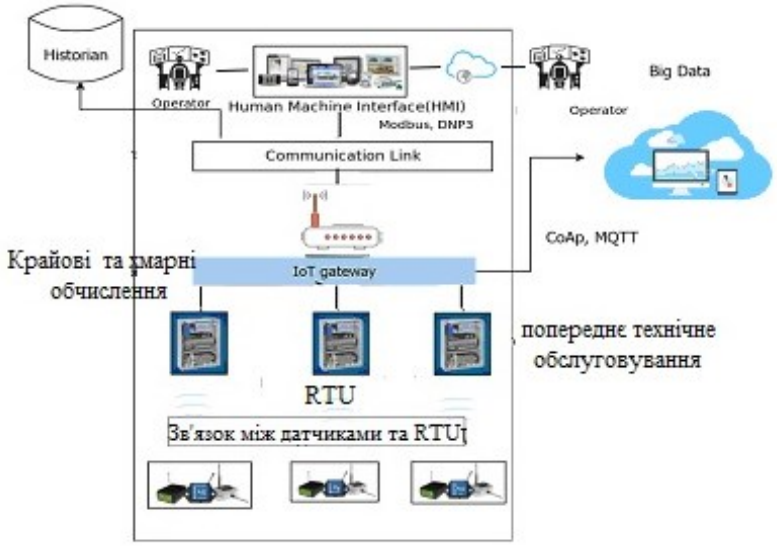


Рис. 7. Мережева архітектура Інтернету речей-четверте покоління SCADA-систем

SCADA-системи четвертого покоління здатні звітувати про стан об'єкту керування у реальному масштабі часу, при цьому використовуючи горизонтальну шкалу з хмарних обчислень. За рахунок цього можуть бути реалізовані більш складні алгоритми керування, для реалізації яких є достатніми традиційні програмовані логічні контролери. Концепція Індустрія 4.0 – це приклад четвертого покоління SCADA-системи, в яких є розподіленими когнітивні обчислення, CPS, Інтерент-речей та хмарні обчислення, які використовуються для керування дії [9].

При проектуванні промислових багаторівневих систем керування різної складності використовується концепція SCADA-систем. Ці системи можуть варіюватися від десятків до тисяч контурів керування в залежності від програми. SCADA-системи використовуються для моніторингу різноманітних даних, таких як потоки, струми, напруги, тиск, температури, рівні води та тощо, в різних галузях промисловості. У виробничих галузях SCADA-системи [8] використовуються для керування виробництвом системи для досягнення цілей продуктивності, перевіряючи кількість вироблених одиниць та підрахунок завершених етапів операцій з температурами на різних стадіях виробничого процесу.

SCADA-системи використовуються для очищення промислових стічних вод. Очисні споруди для обробки поверхневих вод бувають різного типу. Однак, це в основному системи очищення води, в яких багаторівнева система керування, процеси автоматизації та розподілені системи беруть участь в обробці води. Вирішуючи такі задачі, SCADA-системи використовуються для керування автоматичними роботами, обладнанням користувача та зворотнім промиванням фільтрів на основі годин роботи або кількості потоку води, яка проходить через фільтри. Рівні резервуару для води, тиск системи, температуру рослин, седиментація, фільтрація, хімічна обробка та інші параметри або процеси контролюються за допомогою програмно-технічних комплексів SCADA-систем, програмованих логічних контролерів, робочих станцій на базі комп'ютерної техніки, які зв'язані між собою за допомогою локальної мережі LAN, використовуючи наприклад технологію Ethernet. SCADA-системи застосовуються в телекомунікаційних та IT-системах для керування різними радіочастотними системами, засобами та системами зв'язку [10]. Наприклад, реєстрацію даних через антені системи, можна легко здійснити за допомогою SCADA-систем.

SCADA-система може використовуватися разом із програмним забезпеченням MATLAB для керування об'єктами. SCADAMATLAB представляє собою платформу, яка з'єднує звичайну SCADA-систему з програмним забезпеченням MATLAB для досягнення надійності та ефективності керування, при необхідності обробки складних алгоритмів керування.

Віддалені місця розташування та власні промислові мережі використовуються для того, щоб надати SCADA-системам значний ступінь захисту через ізоляцію. Зараз більшість промислових підприємств використовують мережеві сервери історичних процесів для зберігання даних про процеси та інші можливі інтерфейси бізнесу та процесів. Прийняття Ethernet та протоколу керування передачею/Інтернет-протоколу TCP/IP для мереж керування процесами та бездротових технологій, таких як IEEE 802.x та Bluetooth, ще більше зменшило ізоляцію мереж SCADA-систем. Зв'язок та деізоляція SCADA-системи представлено на рис. 8.

Рис. 8. Типові компоненти SCADA-систем

Кіберфізична безпека неперервних систем у режимі реального часу вимагає всебічного уявлення та цілісного розуміння мережевої безпеки, теорії управління та фізичної системи. Зрештою, будь-які життєздатні технічні рішення та напрямки досліджень щодо забезпечення систем SCADA-систем повинні бути у поєднанні з комп'ютерною безпекою, мережею зв'язку та керування. Ідея розглянути проблему в контексті ефективності керуванні має міцні напрямки. Однак дуже велика встановлена база таких систем означає, що в багатьох випадках ми повинні довгий час покладатися на реконструйовані механізми безпеки, а не мати можливість проектувати їх з нуля. Це призводить до нагальної потреби надійних SCADA-систем у виявленні вторгнень (IDS) та еластичному керуванні.

Такі міжнародні інститути, як IEEE, CPNI, AGA, ISA, NERC, NIST публікують рекомендації щодо безпечного використання SCADA-систем [11]. На рис. 9 представлено взаємозв'язок між різними областями безпеки SCADA-системи, такими як архітектура самої системи, вразливості, атаки, виявлення вторгнень та випробувальних стендів. На сьогодні, наукові праці у цьому напрямку, досліджують лише один аспект безпеки SCADA-системи, а отже недоліком є, те що, вони не розглядають взаємозв'язок між різними областями безпеки SCADA-систем, що є дуже значним при створені механізмів безпеки для складних систем промислового Інтернет речей. Таким чином, актуальною задачею, є огляд який враховує різні аспекти безпеки SCADA-систем.

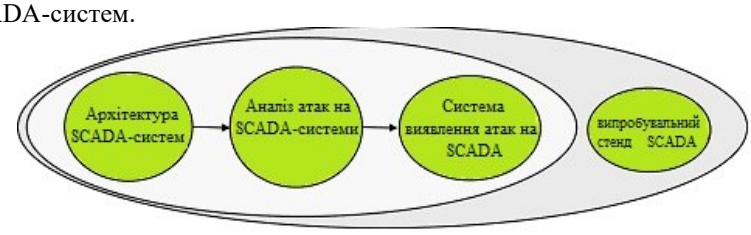


Рис. 9. Взаємозв'язок між різними областями безпеки SCADA-системи

Пропонується використовувати запропоновану у роботі [12] таксономію для вивчення аспекту архітектури та безпеки SCADA-систем, що є необхідним враховувати при проектуванні промислових багаторівневих систем керування. Така таксономія представлена на рис. 10.

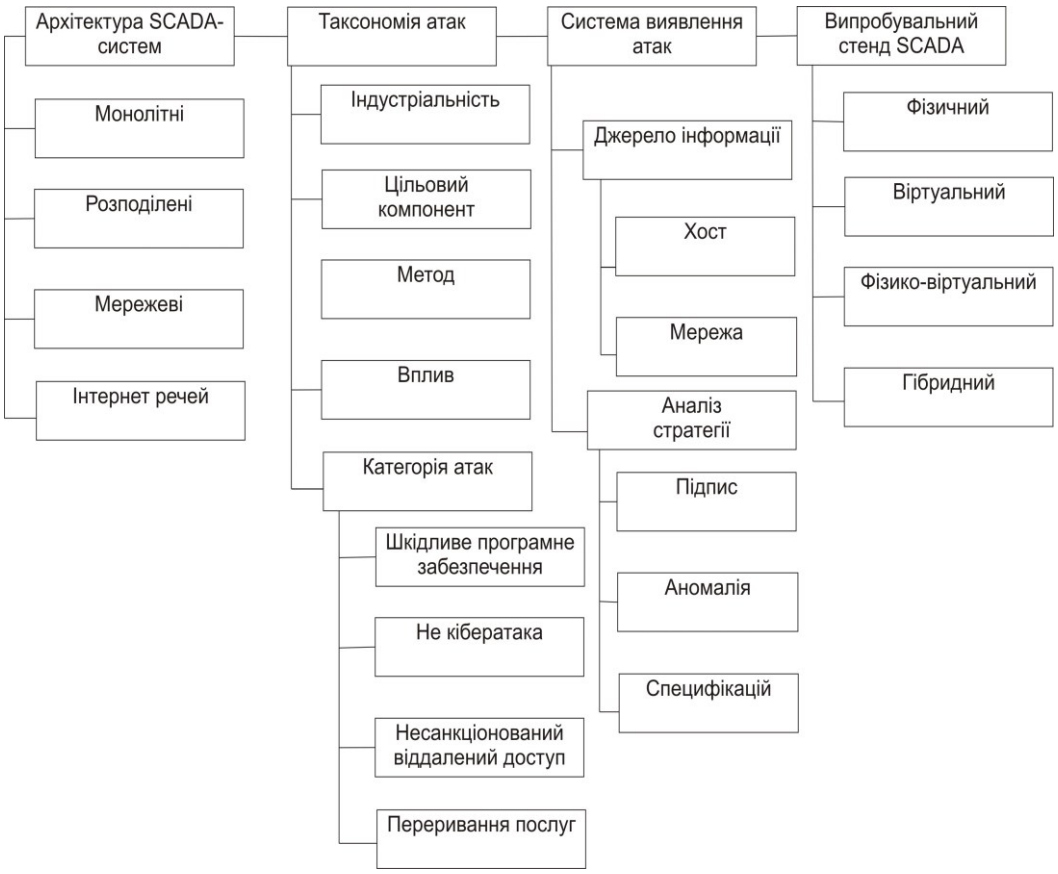


Рис. 10. Взаємозв'язок між різними областями безпеки SCADA-системи

Сучасний стан наукових досліджень, показує, що навіть із вдосконаленим алгоритмом безпеки було виявлено багато атак на SCADA-системи, а це підкреслює майбутній обсяг досліджень, що має зменшити розрив між сучасним станом SCADA-систем та передовими і надійними SCADA-системи для проектування промислових багаторівневих систем керування. Тому при проектуванні промислових багаторівневих систем керування є необхідним враховувати:

1. Бази даних атак: база даних інцидентів безпеки необхідна для аналізу різних вимірів атак для розробки стратегій запобігання подібним атакам у майбутньому. Набори даних KDD99, NSS-KDD, DARPA застарілі і не синхронізовані з сучасною архітектурою SCADA-системи. Набір даних NVD містить загальні вразливості у всіх доменах, які не фокусуються на специфічних вразливостях SCADA-систем. З 2015 року немає оновлення до бази даних RISI. Тому немає належної бази даних, яка охоплювала б всю безпеку інцидентів. Слід створити одне глобальне сховище для всіх цих інцидентів. Це сховище має бути загальнодоступним, доступні дослідникам для аналізу цих атак. Тоді можна обробляти лише атаки нульового дня.

2. Масштабовані тестові стенди та методи перевірки: на основі аналізу огляду існуючих джерел тестових стендів, можна зробити висновок, що як для фізичних, так і віртуальних тестових стендів, було досліджено програмне забезпечення та гібридний тест. Розробка випробувального стенду – це дорогий процес, який потребує величезного обсягу фінансування. Не існує такого випробувального стенду, який був би економічно вигідним, масштабованим і мав високі показники ефективності. Дослідник повинен зосередитись на масштабованості, вищому ступені ефективності, економічності та інтерполяції. Необхідними є нові протоколи зв'язку, нові методи оцінки ризику, а також перевіряти IDS. Існує нагальна вимога щодо достовірної перевірки, підходи до оцінки надійності нових методів безпеки та безпеки SCADA-систем [13].

3. IDS для SCADA-систем: у роботі [14] запропоновані дослідження для визначення показників продуктивності перевірки IDS. У більшості аналізів враховуються лише показники виявлення атак, такі, як хибнопозитивні та хибнонегативні. Час, необхідний для виявлення нападу, є важливим стандартом для вимірювання продуктивності. Отже, навіть якщо гарантовано, що IDS виявлять атаку, а затримка велика, зловмисник матиме достатньо часу, щоб пошкодити систему. Дослідницька робота зосереджена на розробці

системи виявлення для конкретних типів атак, тобто маршрутизації та атаки DOS. Різні атаки схеми виявлення, які працюють за подібних робочих параметрів, мають бути оцінені в подальших дослідженнях і при проектуванні промислових багаторівневих систем керування. Проведено значну роботу в галузі знань, що базується на IDS. Однак ці системи все ще не здатні до обробки атак нульового дня. Визначити прийнятну поведінку при зміні середовища є складним завданням. Засновані на знаннях IDS не є надійними для невідомих атак. Поведінка кожної атаки відрізняється від інших, тому дослідник повинен зосередитись на виявленні моделі нападу. Тому дослідникам слід розробляти підходи для подальшого вдосконалення порогових методів моніторингу. У роботі [15] запропонована модель для динамічного формування правил для виявлення вторгнень у SCADA-системи. Ця порогова модель повинна бути динамічною, яка розпізнає за ступенем тяжкості минулих нападів.

4. Новий комунікаційний протокол: у комунікаційних протоколах основна увага приділяється додатку та захисту мережевого рівня. Протоколи мережевої безпеки повинні бути інтегровані в ці протоколи зв'язку. Протокол зв'язку для SCADA-систем на базі IoT-хмари, тобто надійний, безпечний, масштабований, відкритий, низька затримка протоколу зв’язку – це новий напрямок для дослідника. З концепцією Індустрії 4.0 протоколи IoT використовуються в SCADA-системах. Недоліком таких протоколів є надійність, що викликає потребу в надійному зв'язку. У випадку SCADA-систем, мережевих криптографічних рішень недостатньо для блокування атак. Тому актуальною проблемою є потреба у дослідженнях для більш надійних криптографічних рішень, методів аутентифікації, що входять до протоколу, механізми безпеки, які застосовуються до SCADA-систем.

5. Безпечна архітектура та операційна система: операційні системи DOS, VMS та UNIX, які мають різні уразливості, в основному використовувались у SCADA-системах. На сьогоднішній день працює операційна система Linux та MicrosoftWindows системи витіснили DOS із SCADA-систем на основі UNIX. Однак Linux і Windows страждають від своїх вразливостей, через великий вихідний код для операційних систем. Операційна система заснована на архітектурі мікроядра системи може бути використана для зменшення поверхні атаки для SCADA-систем. Окрім безпеки, безпеки рекомендацій завжди слід дотримуватися в максимальній мірі, щоб уникнути прийнятних ризиків. SCADA-системи можна захистити, використовуючи більш стійку до помилок архітектуру, безпечну та надійну операційну систему і використання захищених мов програмування. Безпека операційної системи є важливою проблемою. Протоколи безпеки повинні бути обов’язковими.

6. Фокус досліджень для IoT-Cloud SCADA-систем: у роботі [16] запропоновано декілька дослідницьких пропозицій щодо безпечного IoT-cloud SCADA-систем. Інтеграція IoT-хмари в традиційну SCADA-систему відкриває нові загрози та можливості обміну даними / інформацією / послугами через Інтернет. Існує гостра необхідність вирощувати нові стратегії, придатні для керування складними та масштабними структурами. Дослідження повинні бути зосереджені на постійну безпеку цих систем. У системі хмарних технологій IoT перевантаження смуги пропускання – це велика проблема. Ці параметри залежать від постачальників хмарних послуг. Затримка з прийняттям рішень може призвести до втрати виробництва. Тож дослідження слід зосередити, щоб зробити цю систему надійною та ефективною. Слід використовувати велику пропускну здатність та низьку затримку. Потенціал цих систем залежить від взаємозв’язку відповідальних платформ. У системі, що базується на Інтернеті речей, величезна кількість даних генерується. Отже, безпека, аналітика, зберігання та складність цих даних є головною проблемою.

Висновки. Встановлено, що для проєктування сучасних промислових багаторівневих систем керування використовуються програмно-технічні комплекси SCADA-системи, що представляють собою централізовані системи для моніторингу та керування всього технологічного процесу за допомогою програмного-апаратних компонентів. У сучасних промислових багаторівневих систем керування SCADA-системи проводять збір даних з віддаленого місця за допомогою датчиків та відправляють команди для керування технологічним процесом до програмованого логічного контролеру або людино-машинного інтерфейсу. Основна перевага SCADA-систем полягає, у тому, що вони конструктивно реалізовуються у різних галузях, а це в свою чергу призводить до зменшення людських зусиль та підвищення точності вимірювання, моніторингу та контролю даних об’єкта керування в режимі реального часу і з будь-якої точки світу.

Сучасні SCADA-системи четвертого покоління представляють собою складні відкриті системи, які є підключеними до Інтернету. Такій підхід робить SCADA-системи, вразливими для різних зловмисників, які здійснюють напади на системи промислових багаторівневих систем керування. Безперебійна та ефективна робота SCADA-систем є однією з актуальних та найважливіших проблем для сучасного виробництва, оскільки наслідки виходу з ладу сучасної промислової багаторівневої системи керування можуть варіюватися від фінансової катастрофи до природного збитку та втрати людського життя.

Для забезпечення ефективного проєктування промислових багаторівневих систем керування необхідно використовувати новий підхід до безпеки SCADA-систем, який поєднує різні аспекти безпеки, комплексний аналіз бази даних атак RISI, систем виявлення вторгнень та тестових стендів SCADA-систем, а також необхідно враховувати, те що, IoTization та хмарні SCADA-системи, розширили спектр проблем дослідження безпеки промислових багаторівневих систем керування.

На сьогодні підходи проектування промислових багаторівневих систем керування переходять до хмарних SCADA-систем. Переваги хмарних SCADA-систем є їх економічність, простота та масштабованість. Однак, незважаючи на ці переваги хмарні SCADA-системи мають ряд недоліків, такі як продуктивність, висока затримка та низька пропускна здатність, що призводить до погіршення ефективності промислових багаторівневих системах керування, тому існує актуальна потреба у розробці ефективних системних архітектур і систем для моделювання таких проблем.

References

1. Guide to Industrial Control Systems (ICS) Security. Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) / [K. Stouffer, V. Pillitteri, S. Lightman and other]. – Gaithersburg: National Institute of Standards and Technology Special Publication 800-82, Revision 2 Natl. Inst. Stand. Technol. Spec. Publ. 800-82, 2015. – 247 c.

2. Nasr P. M. An alarm based access control model for scada system / P. M. Nasr, A. Y. Varjani // Smart Grid Conference (SGC 2015), 2015. – p. 23–24.

3. Rezai A. Key management issue in scada networks: A review / A. Rezai, P. Keshavarzi, Z. Moravej // Engineering Science and Technology, an International Journal, 20(August). - 2016. – p.354–363.

4. Papa S. Securing wastewater facilities from accidental and intentional harm: A cost-benefit analysis. / S. Papa, W.Casper, T. Moore // International Journal of Critical Infrastructure Protection. - 013p. 96 – 106.

5. Miller B. A survey scada of and critical infrastructure incidents / B. Miller, D. Rowe. // In Proceedings of the 1st

6. Annual Conference on Research in Information Technology, RIIT '12 - New York: NY, USA, 2012.- p. 51–56.

7. The scada review: System components, architecture, protocols and future security trends / A.Shahzad, S. Musa, A. Aborujilah, M. Irfan. // American Journal of Applied Sciences. – 2014. – №11. – p.1418–1425.

8. Yadav G. Architecture and Security of Scada System: A Review / G. Yadav, K. Paul // arXiv:2001.02925v1 [cs.CR]. - 2020.

9. https://www.watelectronics.com/scada-systemarchitecture-types-applications.

10. Industry 4.0: the fourth industrial revolution –guide to industrie 4.0. / [Y. Yang, K. McLaughlin, S. Sezer and other]. // Multiattribute scadaspecific. – 2017.

11. https://instrumentationtools.com/applications-of-scada/.

12. Sommestad T. Scada system cyber security x2014; a comparison of standards. / T. Sommestad, G. Ericsson, J. Nordlander // Power and Energy Society General Meetingю - 2010 IEEE, 2010. - p.1–8.

13. Papa S. Securing wastewater facilities from accidental and intentional harm: A cost-benefit analysis. / S. Papa, W. Casper, T. Moore. // International Journal of Critical Infrastructure Protection.- 2013. - №6. – p. 96 – 106.

14. Lyu X. Safety and security risk assessment in cyber-physical systems. / X. Lyu. // IET Cyber-Physical Systems: Theory & Applications. - 2019. - №4. – p.221–232.

15. Mitchell R. A survey of intrusion detection techniques for cyber-physical systems / R. Mitchell, I. Chen // ACM Comput. Surv.- 2014. -№46. p. 1–29.

16. Zhu B. Scada-specific intrusion detection/prevention systems: A survey and taxonomy / B. Zhu, S. Sastry. - 2010.

17. Sajid A. Cloud-assisted iot-based scada systems security: A review of the state of the art and future challenges / A. Sajid, H. Abbas, K. Saleem. // IEEE SPECIAL SECTION ON THE PLETHORA OF RESEARCH IN NTERNET OF THINGS (IoT). - 2016. – №4.

Надійшла / Paper received: 05.10.2020 Надрукована / Paper Printed : 01.12.2020

УДК 004.896
DOI: 10.31891/2219-9365-2020-66-2-14

ПОТЕРЯЙЛО Л. О.
Івано-Франківський національний технічний університет нафти і газу

ІНТЕЛЕКТУАЛІЗАЦІЯ КОНТРОЛЮ ТА ПІДТРИМКА ПРИЙНЯТТЯ РІШЕНЬ У ПРОЦЕСІ БУРІННЯ

У статті означено сутність інтелектуального статистичного контролю процесів та прийняття рішень з застосуванням штучного інтелекту. Наведено результати дослідження, які визначають переваги використання інтелектуальної обробки даних з врахуванням даних про процес для створення окремих компонентів інтелектуальної системи прийняття рішень: контролю та підтримки прийняття рішень. Наведено теоретичні аспекти імітаційного моделювання та комп'ютерним в бурінні. Доведено доцільність використання міркувань на основі прецедентів при побудові цифрового нафтового родовища та зв'язаних виробничих середовищ та виявлено вплив такого підходу на підвищення надійності активів та уникнення простоїв. В статті розглянуто напрямки покращення стратегії технічного обслуговування, шляхом здійснення контролю на всіх етапах циклу виробництва, встановлення пріоритетів, щодо обслуговування активів, планування роботи. Штучний інтелект розглянуто як засіб, що дозволяє уникнути відволікання на непотрібні дані, створення покращеної видимості процесу, а відповідно покращення безпеки та підвищення ефективності процесу прийняття рішень.

Висвітлено особливості технологічних процесів буріння, що мають бути враховані при інтелектуальній підтримці прийняття рішення. Розглянуто залежність типу інформації яка була використана як основа для прийняття рішень на проміжок часу між її отриманням та здійсненням дії, на можливість використання рішення стратегічно, оперативно чи миттєво.

Ключові слова: міркування на основі знань, інтелектуальний контроль, підтримка прийняття рішень, буріння свердловин, інтелектуальна система.

POTERIAILO L.
Ivano-Frankivsk National Technical University of Oil and Gas

INTELLECTUALIZATION OF CONTROL AND SUPPORTING DECISION-MAKING IN THE DRILLING PROCESS

The article identifies the essence of intellectual statistical control of processes and decision-making using artificial intelligence. The results of the study are presented, which determine the advantages of using intelligent data processing taking into account the process data to create individual components of the intelligent decision-making system: control and support of decision-making. Theoretical aspects of simulation and computer drilling are presented. The expediency of using precedent-based considerations in the construction of a digital oil field and related production environments is demonstrated and the impact of such an approach on improving asset reliability and avoiding downtime is identified. The article considers the areas of improving the maintenance strategy by monitoring at all stages of the production cycle, setting priorities for asset maintenance, work planning. Artificial intelligence is seen as a means of avoiding distractions to unnecessary data, creating improved process visibility, and thus improving security and improving the efficiency of the decision-making process.

The peculiarities of drilling technological processes that should be taken into account in the intellectual support of decision making are highlighted. The dependence of the type of information that was used as a basis for decision-making for the period between its receipt and implementation of the action, the possibility of using the decision strategically, quickly or instantly.

Key words: knowledge - based reasoning, intellectual control, decision support, well drilling, intelligent system.

Постановка проблеми. Технологічне середовище буріння характеризується низкою етапів, які взаємодіють для отримання кінцевого продукту. Ці взаємодії ускладнюють діагностику проблем, які можуть виникнути у загальному виробничому процесі. Є кілька простих процесів, які є одноступеневими, проте навіть вони можуть виявляти особливості, які ускладнюють виявлення проблем та їх подальше вирішення, якщо не передбачено інтелектуальної автоматизації.

Статистичний контроль процесів (SPC) є одним із найефективніших інструментів повного управління якістю технологічних процесів, основною функцією якого є моніторинг та мінімізація варіацій процесу. Статистичний контроль процесів може науково розрізнити ненормальні відхилення в ході буріння.

Програми SPC включають три основні завдання послідовно:

1) моніторинг процесу;

2) діагностика відхиленого процесу;

3) вжиття коригувальних дій.

Аналіз останніх досліджень і публікацій. При рішенні проблем у предметній області, де є недосліджена частина проблеми ефективним є поєднання методології прецедентного міркування із специфікаціями теорії представлення та задоволення (дотримання) обмежень.

Нафтогазова галузь характеризується технологічною структурою, на вершині якої є корпоративні або вчені та інженери певного підрозділу з великим технічним досвідом та неглибокими знаннями технологій та процесів, що використовуються для виробництва. Під цією структурою знаходиться робоче середовище виробництва. Існує також група технічно кваліфікованих осіб, які мають офіційну підготовку,

інженерно-технічні та наукові знання у сфері буріння. В основі технологічної структури виробничого процесу є оператори, які зазвичай мають досвід та практичні знання, але яким загалом бракує глибини та широти навчання. Прийняття рішень щодо технологічних процесів буріння базується на методах основаних в першу чергу з інженерним досвідом та літологією родовища. Існує поріг, при якому типовий оператор більше не може сприяти ефективному рішенню, і потрібно використовувати інші технічні ресурси.

В області інтелектуальних систем прийняття рішень методології міркування на основі прецедентів є способом ефективного включення експертного досвіду у процес прийняття рішень [2–3].

Методи, що запропоновані згідно сучасних досліджень [4], поєднують моделі, орієнтовані на дані, які не мають апріорних знань про буріння, та традиційні фізичні моделі, що побудовані на знаннях.

Виділення невирішених раніше частин загальної проблеми. З рухом до комп'ютерно-інтегрованого виробничого середовища потрібно розробляти комп'ютерні додатки для автоматичного виконання всіх завдань SPC. Однак досвід показує, що майже всі дослідження в цій галузі зосереджені лише на автоматизації моніторингу процесу. Діагностику відхилень в ході процесу та рішення щодо вжиття коригувальних дій, виконують фахівці, які здійснюють роботу. Відкритою є аналітична проблема інтелектуальної функціональної підтримки прийняття рішень оператором, яку не можливо адекватно описати набором одночасних алгебраїчних рівнянь.

Формулювання цілі статті. Метою статті є вибір параметрів контролю процесів буріння в розпізнанні шаблонів при виникненні відхилень процесу буріння. Визначення структурної схеми, функціональних зв'язках та особливостей процесу буріння з метою визначення повного набору даних необхідних для прийняття рішення, шляхом створення бази знань, яка має деталі представленого виробничого середовища, її використання також повинно слугувати для підвищення кваліфікації, судження та рівня досвіду нових та існуючих операторів. Визначення методу формування рішення на основі комплексу контрольованих параметрів, що якісно розв'язується за допомогою експертних систем, що працюють на основі накопиченого досвіду.

Виклад основного матеріалу та отриманих наукових результатів

Інтелектуальний статистичний контроль процесів. Контроль експлуатації свердловини включає такі дослідження, як газовий каротаж, петрофізичні дослідження, виділення в розрізі нафтогазоперспективних пластів-колекторів, вивчення фільтраційно-ємнісних властивостей і характеру насичення по розрізу, експресному випробування.

Геолого-технологічні дослідження родовищ з використанням моделей, заснованих на штучному інтелекті (ШІ) проводяться з метою контролю в режимі реального часу за життєвим циклом будівництва:

– контроль режиму роботи бурових комплексів на родовищах;

– контроль технологічного стану обладнання бурової і об'єктів інфраструктури буріння і будівництва свердловин;

– контроль і облік витрат енергоресурсів;

– контроль за проведенням регламентних і планово-попереджувальних робіт;

– контроль екологічних характеристик середовища на об'єктах буріння та установках;

– контроль і автоматизоване управління в аварійних і позаштатних ситуаціях.

Інтелектуальний статистичний контроль процесів передбачає, що бурові системи на основі прецедентів пропонують робочі параметри процесів буріння в реальному часі співвідносяться з величезними обсягами даних про процес, що зберігаються у віртуальному середовищі. Завданням контролю є визначення можливих причин при виникненні відхилень процесу буріння:

1) недостовірність вхідної геолого-фізичної інформації;
2) неточність математичних моделей, що застосовані;
3) неправомірність застосування моделі до даних відповідної категорії.

Буровий супервайзінг передбачає виявлення бурових випадків, визначення причин відхилень від запланованих процесів, прогнозування параметрів буріння, аналіз поведінки буріння та консультування бурових дії, виявлення та оцінка можливих ризиків, розробку контрольних процедур (див. рис. 1).

Класи знань, які повинні бути декларативно та процедурно представлені, включають наступне: процес; методи статистичного контролю процесів (SPC); тести контролю якості; вхідні параметри;умови виконання процесів; цілі та завдання; обмеження; рекомендації; конфігурація управління.

Моделі на основі підходу орієнтованому на дані здатні використовувати інформацію прецедентів роботи свердловин являє собою великий і недостатньо використаний ресурс для більшості бурових робіт компанії. Модель, заснована на штучному інтелекті, орієнтована на дані, є економічно ефективним способом відображення складної динаміки свердловин, які не охоплюються існуючими моделями. З іншого боку, фізичні моделі є більш надійними при зіткненні з ситуаціями, які не спостерігались у попередніх часових рядах. Тому важко створити модель, орієнтовану на дані, яка перевершує фізичну модель у будь-який час, так само, як важко створити фізичну модель який фіксує кожну деталь свердловини та процес буріння. Гібридні системи можуть поєднувати найкращі з обох підходів. Це важливо для практики реалізації штучного інтелекту.

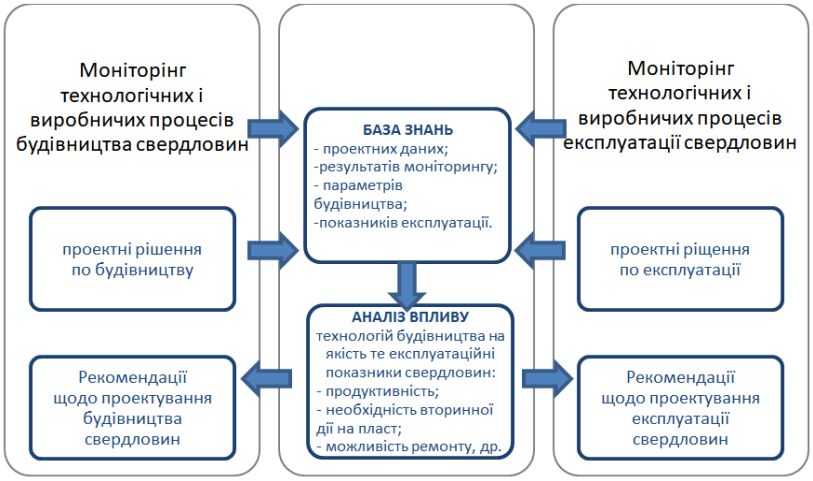


Рис. 1. Інформаційна система супервайзингу будівництва та експлуатації свердловин

Отже, слід розглядати застосування гібридної техніки штучного інтелекту при побудові системи SPC в режимі реального часу, в якій підсистема моніторингу контрольної карти на основі штучної нейронної мережі та підсистема інтерпретації сигналізації на основі експертної системи інтегровані для автоматичного комплексного виконання завдань SPC. Ця система надає спеціалісту з якості три типи інформації, що стосуються поточного стану процесу:

1) стан процесу (контрольний або позаконтрольний, якщо вийде з-під контролю, буде подано сигнал тривоги);

2) вірогідні причини ситуації, що не підлягає контролю;

3) ефективні дії проти ситуації, що не підлягає контролю.

Гібридний інтелект може бути корисно застосований для вирішення проблем у системі SPC в режимі реального часу. По-перше, навчальні та тестові дані генеруються за допомогою алгоритму моделювання. Потім параметри структури мережі та параметри навчання оптимізуються для отримання найкращого навчального ефекту. Нарешті, пропонований метод порівнюється з традиційними методами та іншими методами глибокого навчання.

Він має очевидні переваги перед іншими методами в точності розпізнавання:

– можна ефективно визначити ненормальні моделі даних у фактичному виробництві;

– параметри структури мережі та параметри навчання оптимізовані для отримання найкращого навчального ефекту;

– пропонований метод порівнюється з традиційними методами та іншими методами глибокого навчання.

Інтелектуальний статистичний контроль процесів (ISPC) дозволяє виявити аномальні показники технологічного процесу буріння, завдяки чому виконавці можуть вчасно вживати заходів для усунення відхилень та відновлення стабільності процесу, щоб досягти мети покращення та контролю якості.

Алгоритми машинного навчання мають потужні можливості розпізнавання зразків, їх застосуванням у галузі розпізнавання шаблонів контрольних діаграм (control chart pattern recognition – CCPR).

Усі компоненти процесу, що представляють виробничий процес, повинні бути змодельовані в базі знань структурованим чином. Ключові компоненти процесу, що визначають їх форму, придатність та функціональність, а також їх динаміку та поведінку в роботі, повинні бути представлені прямолінійно.

База знань використовує ряд методів для отримання інтелектуальних результатів управління статистичним процесом. Ці методи повинні бути конкретно та декларативно представлені в базі знань, що дозволить їх легко модифікувати, налаштовувати та вдосконалювати, враховуючи зміни в навколишньому середовищі. Зокрема, методи охоплюють прості одновимірні, багатовимірні, часові ряди та динамічні методи, які включають специфічний розвиток статистики випробувань, коефіцієнтів довіри, верхніх і нижніх меж контролю.

База знань має можливість міркувати на основі знань про застосування найбільш ефективного методу SPC для досягнення заданої мети та завдання навколишнього середовища.

При вивченні статистичних закономірностей, складних фізичних явищ, взаємозв'язку технологічних процесів, наступає момент, появи нової ідеї, коли сукупність параметрів надає підстави розглядати процес з нових позицій. Що дає можливість знайти рішення. Загалом, систему ISPC можна охарактеризувати як домен-залежну оболонку рішення, яка є гнучким та реконфігуруваним додатком для вирішення можливостей ISPC в режимі управління та управління процесами у промисловості (рис. 2).

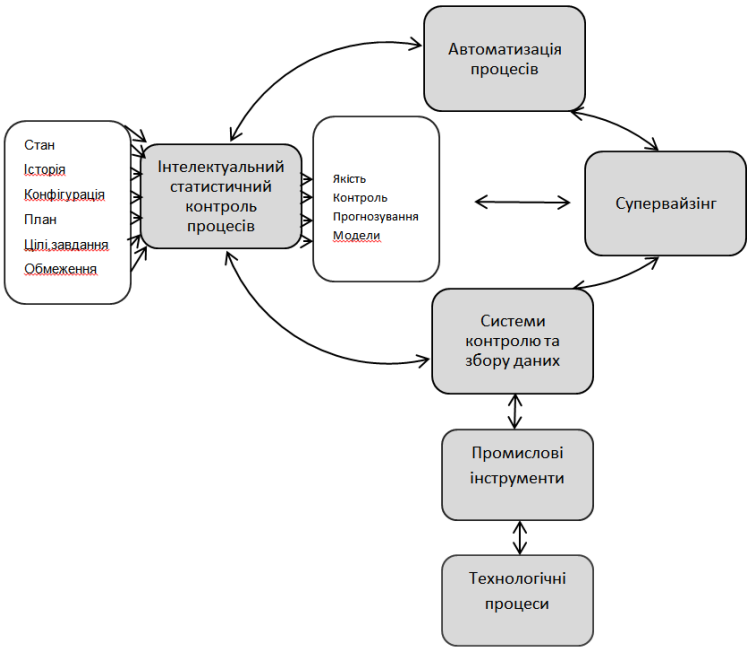


Рис. 2. Місце інтелектуального статистичного контролю як частина архітектури комп'ютерно-інтегрованого виробництва

Переповнення інформації може бути одною з головних причин серйозних аварій, тому необхідно встановити пріоритети, щоб визначити, які небезпеки насправді є важливими для відображення операторам.

Мета сучасних засобів управління та автоматики – забезпечити надійний ступінь стабільності та якості виробничого середовища. Найчастіше це досягається додаванням елементів прямого керування та зворотного зв'язку, застосовуючи закон управління пропорційними інтегральними та похідними режимами.

Інтелектуальна підтримка прийняття рішень. Дослідження аварій зазвичай вказують на недоліки у процесі прийняття рішень на певній стадії технологічного процесу. Це призводить до непослідовних, а іноді і нестабільних результатів виробництва. Іноді затримки часу можуть спричинити мінливість атрибутів відповідності технологічних процесів буріння, а також загальну втрату продуктивності та прибутку Більше того, серед операційного персоналу спостерігається природна плинність. Цей оборот призводить до поєднання рівнів кваліфікації на нижньому рівні управління виробництвом, що варіюється від операторів із десятиліттями майстерності, суджень та досвіду до новачків, які намагаються вчитися якнайкраще. Таким чином, покращення підтримки прийняття рішень є одним із заходів, який може запобігти аваріям та забезпечити безперебійний процес буріння.

Інтелектуальна система підтримки прийняття рішень оператором, яка містить набір інтелектуальних засобів, дозволяє усунути наведені проблеми. Впроваджуючи аналітику та інструменти інтелектуальної підтримки прийняття рішень дає можливість краще використовувати дефіцитний людський досвід, сприяти покращенню експлуатаційних показників та забезпечувати відповідність стандартам безпеки.

Вимоги та атрибути системи інтелектуальної підтримки прийняття рішень знаходяться в чотирьох сегментах: якість, організація, обмеження, модель (рис. 3).

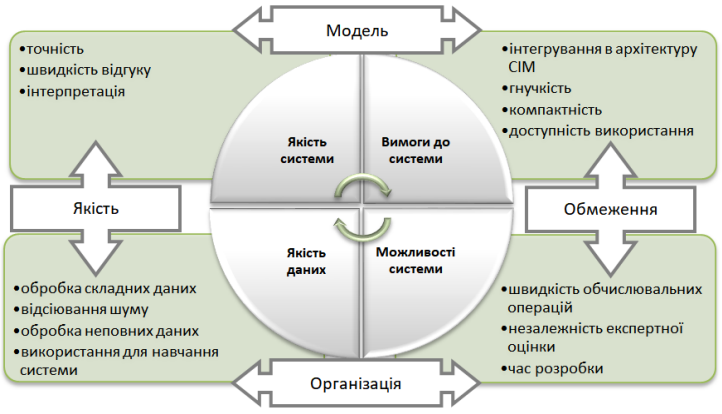


Рис. 3. Вимоги та атрибути системи інтелектуальної підтримки прийняття рішень

Інтелектуальна функціональність підтримки прийняття рішень є частиною архітектури CIM (computer-integrated manufacturing), а також архітектури розподіленої системи управління. Функціонал інтегрується так, щоб отримати поточний статус, цілі, завдання та обмеження. Ця інформація повинна бути автоматично розміщена в базі знань, що підтримує прийняття рішень оператором, не вимагаючи втручання оператора або регулярного обслуговування. Ця інтелектуальна функціональність створить середовище, яке підтримує, реагує та актуальне у своїх рекомендаціях.

Складність рішення при бурінні зумовлена кількома факторами: великі підземні невизначеності, неточні та ненадійні вимірювання, відсутність прогнозні моделі, суперечливі цілі між задіяні технічні дисципліни та труднощі, з якими стикаються люди рішення в ситуаціях, обмежених часом.

При прийнятті рішень використовують наступні теорії вибору:

1. Теорія раціонального вибору, яка передбачає чітко визначені та визначені ситуації, чіткі ролі та обов'язки, чітко визначені альтернативи та необмежений час та ресурсів.

2. Теорія обмеженої раціональності, яка передбачає чітко визначену та визначену ситуацій, але що враховує, що ролі та обов'язки можуть бути менш чіткими, це альтернативні рішення можуть бути розроблені лише частково, а також час і ресурси обмежена.

3. Теорія прийняття рішень, що базується на емпіричних дослідженнях прецедентів технологічних процесів – натуралістичне прийняття рішень.

Натуралістичне прийняття рішень – напрям досліджень, який є найбільш орієнтованим щодо рішень, коли вони розгортаються в реальних умовах і являє собою перехід від загального підходу до прийняття рішень до вирішення підходу, заснованого на знаннях особи, що приймають рішення зі значним досвідом.

Інтелектуальна підтримка прийняття рішення враховує такі характеристики процесу буріння, аварійних ситуацій зокрема, як:

1) невизначені цілі та неправильно структуровані завдання;
2) невизначеність, двозначність та відсутність даних;
3) зміна та конкуруючі цілі;
4) динаміка та постійні зміни умови;
5) цикли зворотного зв’язку дії (реакції в реальному часі на змінені умови);
6) стрес у часі;
7) високі ставки;
8) кілька гравців;
9) організаційні цілі та норми;
10) досвідчене рішення виробників.

Моделі імовірнісних рішень розроблені для цілого ряду типових проблем буріння, наприклад, зміна долота, корпусу, напливу газу тощо.

Рішення з інтелектуальною підтримкою поєднує в собі візуалізацію статусу буріння, ризику та прогресу на високому рівні з інструментами прийняття рішень, що базуються на загальній платформі соціальної співпраці, інтегрованій із існуючою галузевою стандартною IT-інфраструктурою компанії-оператора і базується на технологіях мереж, математичних моделях прийняття рішень та візуалізації даних.

Різні інструменти та методи надання інформації про ризики в якості підтримки прийняття рішень використовуються в переробних галузях, проте існуючі методи кількісного аналізу ризику не завжди забезпечують належну підтримку для оперативних рішень у нафтогазовій галузі. Однією з причин цього є те, що в основному проводиться аналіз, що охоплює технічні аспекти підтримки і відображає лише обмежені операційні та організаційні питання. Ці методи забезпечують підтримку рішень, що приймаються на основі експлуатаційних практик та інших рішень. Однією з причин цього є те, що в основному проводиться аналіз, що охоплює технічні аспекти і відображає лише обмежені операційні та організаційні питання. Ці методи дають корисне рішення підтримка вибору експлуатаційних практик. Однак ці методи не обов’язково дають хороші відповіді, якщо є необхідність вирішення, конкретної ситуації чи конкретної операції миттєво. Кількісний аналіз ризику також має значення у підготовці плану реагування на надзвичайні ситуації і є основним інструментом у процесі прийняття рішень. Він застосовується для прийняття рішень після виникнення інциденту. Важливим аспектом є робота спрямована на запобігання інцидентам.

Більшість операторів проходять певний ступінь навчання та ознайомлення з процесами, що з часом покращує їхні навички, судження та досвід. Однак вага інформації може бути значною, неорганізованою, нецілеспрямованою та складною для використання під час стресу в нестандартних ситуаціях.

Доцільно говорити про рішення, коли між розглядом і висновком існує проміжок часу та дії або результату рішення. Це проміжок відставання часу варіюється. У рішеннях, що стосуються стратегічних та оперативні питання, як правило, можуть бути вказані причини конкретного вибору між альтернативами до того, як відбудеться дія або до досягнення врегулювання. Прикладом є планування операції. В інших ситуаціях затримка часу мінімальна. Це може бути в надзвичайних ситуаціях, коли часу на систематичне

оцінювання альтернатив немає, оскільки дії повинні бути вжиті негайно та причини вибір може бути наданий лише ретроспективно.

Типи інформації слід розглядати як імовірнісну та фактичну рис. 4 [5].

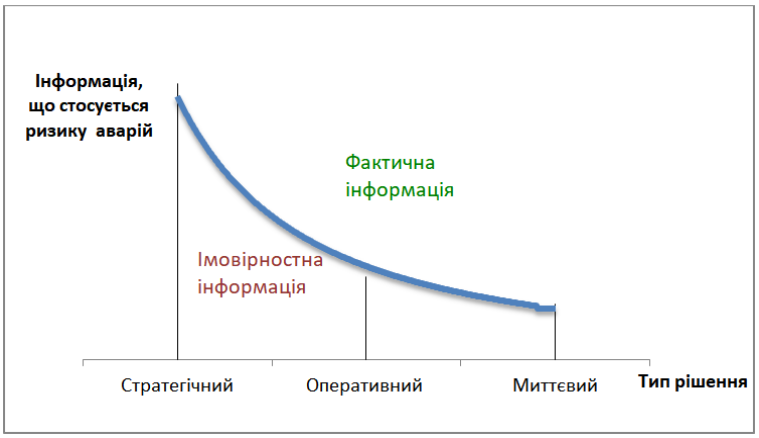


Рис. 4. Інформаційна основа для різних типів рішень, пов'язаних з ризиком аварій

Прийняття великих і малих рішень на ходу – це частина кожного робочого процесу. На загальному рівні існує три різні ситуації прийняття рішень (стратегічне, оперативне, миттєве) залежно від типу інформації, яка була використана як основа для прийняття рішень.

Для стратегічних довгострокових рішень значна частина основи для розгляду основних ризиків аварії буде імовірнісною інформацією.

Оперативні рішення базуються на поєднанні ймовірнісної та фактичної інформації.

Миттєві рішення, прийняті операторами, здебільшого базувалися на фактичній інформації.

Застосування різних типів інформації, описаних вище, має деякі наслідки для того, як рішення можуть бути підтримані. Стратегічні, оперативні та миттєві процеси прийняття рішень різні, не тільки щодо часового горизонту, але й коли справа стосується типу інформації, яка є застосовується та тип персоналу, який бере участь у процесах.

Принципи інтелектуальної підтримки прийняття рішень повинні відображати такі відмінності:

– покращення фактичної та імовірнісної інформаційної бази для прийняття миттєвих рішень;

– рішення підтримується засобами візуалізації небезпечних зв’язків між операціями технологічного процесу.

Функціональними областями, в яких підхід до бази знань для підтримки прийняття рішень оператором може бути розгорнутий є:

– посібники, стандарти та коригувальні дії;

– навчання;

– моделювання та прогнозування;

– процес, поради та розуміння.

Технологічний цикл управління процесом видобутку формується інформаційним циклом «Вимірювання – Корекція – Контроль – Прогноз – Вплив». Однак, прецеденти, не завжди використовуються ефективно для аналізу процесів через відсутність добре організованих даних, де існує величезний потенціал перетворення даних у знання [5]. В цих умовах важливим є створити базу знань, яка б структурувала та кодифікувала цю інформацію та дозволяла подавати та фокусувати потрібну інформацію з урахуванням стану виробництва. Базу знань, що містить стандартні посібники та документацію, технічні та технічні особливості, а також узгоджені стандарти та коригувальні дії. Ця інтелектуальна система документації є взаємопов’язана із загальним виробничим та обчислювальним середовищем. Коли виникає проблема, замість того, щоб оператору доводилося поспішати, намагаючись знайти належні знання, стандартні коригувальні дії або відповідь, база знань може розумно направити цю інформацію безпосередньо на оператора. Ця база знань повинна містити таку інформацію:

– специфіка процесу;

– особливості контролю;

– режим виробництва;

– стандартні посібники з експлуатації;

– стандартна операційна політика;

– стандартні коригувальні дії;

– неповерхневе розуміння технологій;
– навичка, судження та досвід оператора;
– спеціальні знання для сайту;
– цілі та завдання, як їх розуміють на даний момент;
– поточні обмеження;
– виготовлення рецептів та альтернатив;
– варіанти та альтернативи оператора.

Технологія експертних систем забезпечує загальну інтелектуальну логіку та структуру управління, що дозволяє цій програмі зосередитись на підтримці оператора, враховуючи певний стан. Важливим є ведення статистики та здійснення аналізу проблем, що мали місце в минулому, проведені коригувальні дії та подальші результати процесу. Ця інформація є дуже цінною як джерело аналізу для покращення загального виробничого середовища.

База знань, забезпечує такі функціональні можливості:
– конкретна логіка підтримки прийняття рішень, враховує поточний виробничий стан;
– презентує альтернативи, засновані на дослідженні інтерактивного оператора.
– здійснює статистичний та аналіз даних про процес, що підтримує функцію автономної підтримки прийняття рішень для вдосконалення та впорядкування операцій;
– формує послідовність реакцій, що пропонується оператору;
– уможливлює інтелектуальне отримання допоміжної інформації в інтернеті та в інтерактивному режимі.
– поширює дефіцитні виробничі знання до базового нижнього рівня виробництва.

Важливо передбачити оновлення бази знань подіями, які відбуваються в реальному виробничому середовищі. Це забезпечить постійний процес навчання, пов'язаний з усіма процесами, навіть процесами, що існували протягом значної кількості років.

На додаток до навчання операторів для надання їм розуміння процесів та практичного досвіду, існує величезна можливість у забезпеченні інтелектуального середовища моделювання, яке б імітувало навчальне середовище для підтримки прийняття рішень на рівні виробництва в цілому.

Основні параметри процесу буріння – це теоретичні міркування, спрямовані на введення понять, пов’язаних із імітаційним моделюванням та комп'ютерним моделюванням в бурінні. Аспекти параметризації мають важливе значення при прийнятті рішень у процесі буріння свердловин на нафту і газ. Пошук оптимального проектного рішення передбачає розгляд безлічі варіантів розробки, і на практиці фахівці спираються на минулий досвід, вибираючи об'єкти-аналоги з готовими рішеннями, які застосовуються до нового об'єкту [7].

Інтелектуальна підтримка прийняття рішень вимагає об’єднання різнорідних джерел інформації, які мають принципово різні уявлення, які потрібно розумно узгодити для побудови когнітивного та інтегрованого інтелектуального застосування. Завдяки евристичним методологіям, заснованим на знаннях, мета побудови такої системи може бути реалізована.

Моделювання, засноване на правилах, дуже вміло представляє вільні та відкриті моделі, які призводять до точних формалізмів для вирішення складних проблем, орієнтованих на перехід. Цілком природно використовувати правила в якості детекторів стану, ліва сторона яких чітко вказує на можливий стан, а права – втілення наслідків та дій, які слід вжити, якщо даний стан проявляється. Значна частина інтелектуальних функціональних можливостей підтримки прийняття рішень обертається навколо моделювання можливих станів і пов’язування з ними підтримки, необхідної для того, щоб оператор установки мав інформацію та своєчасні поради щодо прийняття правильного рішення. У декларативному компоненті бази знань необхідно побудувати структуровану таксономію, що представляє різні сутності, неоднакові джерела інформації та їх взаємозв'язки, необхідні для вирішення питань, які можуть мати місце в технологічному процесі.

Використовуючи об’єктно-орієнтоване представлення та методології, що базуються на правилах, стає можливою формування структури бази знань, яка може відповідати на безпосередні проблеми.

Кількість знань, пов’язаних із реальними системами підтримки прийняття рішень для допомоги операторам, занадто велика, щоб практично міститися в пам’яті або навіть у віртуальній пам’яті будь-якого традиційного комп’ютера. Розробити такий додаток стає абсолютно необхідним використання стійкої архітектури стабільного зберігання. Ідеальний кандидат для цього буде реляційною базою даних, яка підтримує SQL. Ця реляційна база даних фактично забезпечить функціональність глобальної бази знань, що містить всю інформацію, необхідну для побудови інтелектуального додатку. Потім ця інформація отримуватиметься на вимогу в базі знань в пам'яті для подальших міркувань для підтримки оператора.

Ця взаємодія між базою знань в пам'яті, що складається з об'єктів, правил та методів, та реляційною базою даних стабільного зберігання є ключовим фактором для створення відповідної та розширюваної інтелектуальної програми в цій галузі.

Висновки та перспективи подальшого розвитку в цьому напрямі. Побудова інтелектуального середовища моделювання на традиційному комп'ютері в поєднанні з пропонованими реляційними базами даних, дає можливість створити надзвичайно гнучку, інтегровану та розширювану інтелектуальну систему автоматизації. Доведено, що поєднуючи орієнтовані на дані моделі з фізичними моделями, можна отримати високі результати щодо використання даних прецедентів, показників експлуатації обладнання, запобігання ускладнень, тим самим покращити показники отримання віддачі від інвестицій у штучний інтелект.

Розроблено схему вимог та атрибутів системи інтелектуальної підтримки прийняття рішень з огляду на якість, організацію, обмеження та модель.

Отримані висновки вказують, що ефективно контролювати дані процесу та отримувати більш точний та поточний опис основних виробничих процесів дозволяє застосування засобів штучного інтелекту, концепцій, прийомів та методологій.

Майбутнім напрямком розвитку дослідження є шляхи інтеграції інтелектуалізації, як ієрархічно, в вертикальному напрямку, так і на горизонтальному рівні, обробки інформації, контролю та аналізу, прийняття рішень та можливість розширення запропонованої методології від окремих технологічних процесів до процесу буріння в цілому.

Література

1. Barták R., Dechter R. Constraint Processing. New-York: Morgan Kaufmann Publisher, 2003. 210 p.
2. Вовк Р.Б. Формалізація представлення технологічних проблем в інтелектуальній системі підтримки прийняття рішень / Р.Б. Вовк, М.С. Чесановський, Л.О. Потеряйло // Автоматизоване управління багатовимірними об'єктами на засадах обчислювального інтелекту, присвячена 50-річчю кафедри автоматизації та комп'ютерно-інтегрованих технологій: Всеукр. наук.-практ. конф., Івано-Франківськ, 17-19 жовтня 2018р. : тези доп. - Івано-Франківськ, 2018. - С. 46-47
3. Чесановський М.С. Формально-метричні аспекти кейс-базованих реалізацій при вирішенні технологічних проблем буріння/ Чесановський М.С., Шекета В.І., Потеряйло Л.О. // Науково-технічний журнал. Математичні машини та системи. – 2019. – №1.– С. 94–106.
4. G. Gola, R. Nybo, D. Sui, and D. Roverso, Improving management and control of drilling operations with artificial intelligence, SPE Intelligent Energy International (Utrecht, The Netherlands), Society of Petroleum Engineers, March 27–29 2012
5. Trond Kongsvik, Petter Almklov, Torgeir Haavik, Stein Haugen, Jan Erik Vinnem, Per Morten Schiefloe Decisions and decision support for major accident prevention in the process industries Journal of Loss Prevention in the Process Industries. Elsevier. May 2015
6. Потеряйло Л.О. Знання орієнтовані методи прийняття рішень в моделюванні тренажерів технологічних процесів/ Л.О. Потеряйло, В.В. Процюк, К.І. Кравців // Науково-технічний журнал. Методи та прилади контролю якості. – 2020. - №2.- рекомендовано до друку
7. Потеряйло Л.О. Моделювання імітаціонної моделі керування процесами буріння на основі прецедентів /Потеряйло Л.О., Процюк В.В.,. Кравців К.І// Всеукраїнська наук.-практ. конф. «Інформаційні технології в освіті, техніці та промисловості» - ІТОТП-2020 -Івано-Франківськ, 8 жовтня 2020. – С.224-227.

References

1. Barták R., Dechter R. Constraint Processing. New-York: Morgan Kaufmann Publisher, 2003. 210 p.
2. Vovk R.B. Formalizatsiia predstavlennia tekhnolohichnykh problem v intelektualnii systemi pidtrymky pryiniattia rishen / R.B. Vovk, M.S. Chesanovskyi, L.O. Poteriailo // Avtomatyzovane upravlinnia bahatovymirnymy obiektamy na zasadakh obchysliuvalnoho intelektu, prysviachena 50-richchiu kafedry avtomatyzatsii ta kompiuterno-intehrovanykh tekhnolohii: Vseukr. nauk.-prakt. konf., Ivano-Frankivsk, 17-19 zhovtnia 2018r. : tezy dop. - Ivano-Frankivsk, 2018. - S. 46-47
3. Chesanovskyi M.S. Formalno-metrychni aspekty keis-bazovanykh realizatsii pry vyrishenni tekhnolohichnykh problem burinnia/ Chesanovskyi M.S., Sheketa V.I., Poteriailo L.O. // Naukovo-tekhnichnyi zhurnal. Matematychni mashyny ta systemy. – 2019. – №1.– C. 94–106.
4. G. Gola, R. Nybo, D. Sui, and D. Roverso, Improving management and control of drilling operations with artificial intelligence, SPE Intelligent Energy International (Utrecht, The Netherlands), Society of Petroleum Engineers, March 27–29 2012
5. Trond Kongsvik, Petter Almklov, Torgeir Haavik, Stein Haugen, Jan Erik Vinnem, Per Morten Schiefloe Decisions and decision support for major accident prevention in the process industries Journal of Loss Prevention in the Process Industries. Elsevier. May 2015
6. Poteriailo L.O. Znannia oriientovani metody pryiniattia rishen v modeliuvanni trenazheriv tekhnolohichnykh protsesiv/ L.O. Poteriailo, V.V. Protsiuk, K.I. Kravtsiv // Naukovo-tekhnichnyi zhurnal. Metody ta prylady kontroliu yakosti. – 2020. - №2 - rekomendovano do druku
7. Poteriailo L.O. Modeliuvannia imitatsionnoi modeli keruvannia protsesamy burinnia na osnovi pretsedentiv /Poteriailo L.O., Protsiuk V.V.,. Kravtsiv K.I// Vseukrainska nauk.-prakt. konf. «Informatsiini tekhnolohii v osviti, tekhnitsi ta promyslovosti» - ITOTP-2020 - Ivano-Frankivsk, 8 zhovtnia 2020. – S.224-227.

Надійшла / Paper received: 15.10.2020 Надрукована / Paper Printed : 01.12.2020

УДК 004.622
DOI: 10.31891/2219-9365-2020-66-2-15

КОМАР М. П.
Західноукраїнський національний університет

МЕТОДИ ВІДНОВЛЕННЯ ВІДСУТНІХ ДАНИХ У ІНТЕРФЕЙСІ ВЕЛИКИХ ДАНИХ

У статті досліджено відомі методи та запропоновано новий метод відновлення відсутніх даних.

Найбільшою проблемою відомих методів відновлення відсутніх даних є лише обробка структурованих даних, тоді, коли напівструктуровані та неструктуровані дані домінують у реальних прикладних задачах сучасного світу. Крім того, дуже важливо аналізувати приховані залежності в наборі даних, а також враховувати характер набору даних та передбачати відсутність даних для кожного джерела даних окремо. Тому, перспективним є використання парадигми великих даних для попередньої обробки та обробки інформації з різних джерел, що складається з безперервних числових даних та категоріальних даних. Тим не менше, природа відсутніх даних у різних джерелах даних теж різна. Отже, основною ідеєю є аналіз даних з різних джерел на основі специфіки та природи цих джерел. Ідея запропонованого методу обчислення відсутніх даних полягає в обробці структурованих та напівструктурованих даних на основі ієрархії об'єктів, а також набору функціональних залежностей та розробки правил асоціації. Це питання дуже важливе для інтерфейсів великих даних, оскільки більша частина інформації доступна в напівструктурованому вигляді. Запропонований метод створює додаткові значення даних за допомогою доменних та функціональних залежностей на основі декількох методів обчислення та додає ці значення до наявних навчальних даних.

Ключові слова: великі дані, аналіз даних, обробка даних, відсутні дані, відновлення даних, функціональні залежності, правила асоціації, кластерний аналіз, машинне навчання, нейронна мережа.

KOMAR M.
West Ukrainian National University, Ternopil, Ukraine

METODS OF MISSING DATA IMPUTATION IN BIG DATA INTERFACE

Known methods are investigated and a new method of missing data imputation is proposed.

The biggest problem of the known methods of missing data imputation is only the processing of structured data, when semi-structured and unstructured data dominate the real applications of the modern world. In addition, it is very important to analyze the hidden dependencies in the data set, as well as to take into account the nature of the data set and to assume the absence of data for each data source separately. Therefore, it is promising to use the big data paradigm for pre-processing and processing information from different sources, consisting of continuous numerical data and categorical data. However, the nature of the missing data in different data sources is also different. Thus, the main idea is to analyze data from different sources based on the specifics and nature of these sources.

The idea of the proposed method of calculating missing data is to process structured and semi-structured data based on a hierarchy of objects, as well as a set of functional dependencies and the development of association rules. This issue is very important for big data interfaces, as most of the information is available in a semi-structured form. The proposed method creates additional data values using domain and functional dependencies based on several calculation methods and adds these values to the existing training data.

Keywords: big data, data analysis, data processing, missing data, data recovery, functional dependencies, association rules, cluster analysis, machine learning, neural network.

Вступ. Постановка проблеми. Процеси прийняття рішень в різних галузях (науці, бізнесі, економіці) сильно залежать від наявності даних, з яких можна отримати корисну інформацію. В процесів прийняття рішень можна застосовувати прогнозні моделі, які використовують отримані дані в якості вхідних даних. Такі моделі не працюють, коли один або кілька входів відсутні. У багатьох рішеннях просто ігнорувати пропущені дані не можна. Це пов'язано головним чином з тим, що неповні дані можуть призвести до необ'єктивних результатів статистичного моделювання або навіть збитків при керуванні технологічними процесами. З цієї причини дуже важливо приймати рішення на основі повних даних. Оскільки, багато методів машинного навчання, таких як нейронні мережі, метод опорних векторів та багато інших методів обчислювального інтелекту не можуть бути використані для прийняття рішень, якщо дані не повні. У таких випадках оптимальний результат прийняття рішення все одно повинен зберігатися, незважаючи на відсутні дані. У випадках неповних векторів даних першим кроком до прийняття рішення є оцінка відсутніх значень. Після оцінки відсутніх значень можна використовувати інструменти відновлення, заповнення даних. Імпутація даних стає все більш важливою в таких сферах, де кількість зразків, як правило, невелика, а вартість отримання нових висока, що робить ігнорування неповних даних не правильним. Таким чином, створення теоретичних основ та методів, які можуть призвести до повноти даних, є важливою задачею. Метою роботи є дослідження та розробка методів відновлення відсутніх даних в інтерфейсах великих даних.

1. Механізм відсутніх даних. За механізмом відсутності дані визначають наступним чином [1–4]:

1. Дані відсутні абсолютно випадково (missing completely at random – MCAR) – відсутність значень в даних не залежить від будь-яких значень – наявних або відсутніх.

2. Дані відсутні випадково (missing at random – MAR) – відсутні значення умовно залежні від наявних значень, а не від відсутніх. Ймовірність того, що значення X_i опущено, не пов'язана з самим X_i, але вона залежить від інших змінних в аналізованій таблиці.

3. Дані відсутні не випадково (missing not at random – MNAR) – відсутність значень залежить від значення відсутньої змінної. Ймовірність того, що значення X_i опущено, пов'язана з самим X_i.

Загальна проблема MCAR полягає в тому, що дані за цією схемою на початку аналізу насправді можуть бути різними через невідомі або неприйнятні фактори. На цій підставі неповні дані часто мають схему, що не відповідає MCAR, але вони можуть бути віднесені до схеми з випадковими пропусками MAR у випадку, якщо неповні дані можуть мати місце залежно від відомих показників. Якщо неповні дані неможливо віднести ні до MCAR, ні до MAR, вони класифікуються як MNAR. Це означає, що результати моделювання на основі таких даних матимуть упереджені оцінки, якщо модель відсутнього значення невідома або не враховується.

Основним недоліком MCAR, MAR та MNAR є відсутність зв’язку з джерелом даних або структурою даних. Це означає неможливість передбачити місце пропущених даних, тоді як такий тип передбачення дуже важливий для потокових даних.

2. Методи та алгоритми відновлення відсутніх даних. В якості фундаментальної технології аналізу великих даних використовується кластеризація, яка поділяє об'єкти на різні кластери на основі подібності [5–7]. Традиційні алгоритми кластеризації даних зосереджені на повній обробці даних, таких як кластеризація зображень [8], кластеризація звуку [9] та кластеризація тексту [10]. Гетерогенні методи кластеризації даних, останнім часом, цікавлять науковців [11–13].

Крім того, було запропоновано багато алгоритмів – наприклад, в [14] оптимізовано уніфіковану цільову функцію за допомогою ітераційного процесу, і розроблено алгоритм спектральної кластеризації для кластеризації різнорідних даних на основі теорії графів. У [15] запропоновано алгоритм нечітких c-середніх значень високого порядку для розширення звичайного алгоритму нечітких c-середніх з векторного простору на тензорний простір. Для кластеризації даних в системах Інтернету речей (IoT) запропоновано алгоритм c-середніх значень високого порядку, заснований на тензорах [16]. Ці алгоритми ефективні для покращення продуктивності кластеризації неоднорідних даних. Однак вони можуть отримати лише результати кластеризації та позбавлені подальшого аналізу неповних даних з низькими розмірами. Тому їх продуктивність обмежена неоднорідними даними у середовищі великих даних. Що ще важливіше, інші існуючі алгоритми кластеризації об’єктів не враховують відновлення даних та відсутність даних.

Метод середнього заміщення (MS) дозволяє вирішити проблему неповноти даних, замінюючи кожну відсутність середньою змінною. Типи MS – це підміна медіани, моди, середнього значення підгрупи даних [17], значення з найвищою частотою (найбільш загальне значення), в деяких випадках замінює мінімальне/максимальне значення. Цей метод може призвести до багатьох небажаних результатів, таких як заниження реальної дисперсії, негативне упередження кореляцій та неправильне представлення загальної сукупності [18].

Проста hot-deck імпутація замінює кожне відсутнє значення випадковим значенням, взятим із існуючого набору даних [19]. Його суттєвим недоліком є спотворення кореляцій.

Імпутація Cold-deck (CD) реалізує заміну кожного проходу на деяке постійне значення із зовнішнього джерела [20]. Особливим випадком CD є нульова підміна. Як і послідовна та випадкова гаряча заміна, вона має ті ж недоліки, що і проста гаряча заміна.

Перевага підходів на основі заміщення полягає в тому, що вони дають внутрішньо узгоджений набір значень, але не можуть визначити взаємозв'язки між змінними. Методи заповнення прогалин на основі моделі оцінюють значення параметрів моделі, які послідовно використовуються для обчислення прогалин. Ці методи враховують взаємозв'язки між змінними, але вони досить складні, оскільки спричиняють помилки, коли всі параметри оцінюються одночасно.

Оцінка регресії (RE) передбачає заміщення прогалин даних прогнозованими значеннями, отриманими з рівняння регресії, побудованого з повного набору даних. Недоліки заповнення регресією включають наступне: необхідність точно ідентифікувати моделі регресії, перебільшення кореляції та коваріації, ймовірність виходу прогнозованих значень за межі логічного ряду та необхідність великих обсягів даних для отримання послідовних оцінок.

Метод максимальної ймовірності (ML) виводить оцінені параметри таким чином, що ймовірність відтворення даних на основі відомих значень максимізується. Метод ML розглядається як один із підходів до обробки неповних даних [21], і його широко рекомендують використовувати, оскільки він не призводить до упередженості при наявності відсутніх схем значень MCAR та MAR [22]. Однак метод ML не вирішує цього питання за наявності MNAR, хоча величина такого упередження, як правило, набагато менша, ніж традиційні підходи.

Метод максимізації очікувань (EM) заснований на загальному ітераційному алгоритмі, який реалізує послідовне заповнення відсутніх значень за їхніми оцінками та максимізує умовне сподівання

ймовірності отримання повних даних до процесу конвергенції [22]. Основним недоліком методів ML та EM є їх ітераційна властивість і висока часова складність в подальшому, особливо для обробки великих даних.

Метод k-найближчого сусіда (kNN) заснований на визначенні найближчого сусіда для кожного пропущеного значення за допомогою певної метрики [23]. Після пошуку k-найближчих сусідів за кожний прохід воно замінюється середнім значенням характеристик для сусідів, що містять повні дані. Окремим випадком методу kNN є зважений метод kNN [24]. Найбільша складність у його застосуванні полягає у визначенні адекватного ступеня близькості.

Алгоритм опорних векторних машин (SVM) [25] дозволяє уникнути оцінки ймовірності даних, які є стабільними. Вибір ядра впливає на якість обчислення відсутніх даних. Ось чому реалізація цього алгоритму залежить від набору даних та його параметрів.

Метод випадкових лісів (RF) [26] заснований на побудові класифікатора, сформованого групою дерев рішень, навчальним набором повних даних та прогнозуванням відсутніх значень у наборі тестів. На першому кроці всі прогалини в наборі тестів заповнюються середнім значенням на основі наявних даних. Далі розраховується матриця близькості для першого набору даних. Середні ваги, розраховані на матриці близькості для першої ітерації, використовуються для заміщення пропусків на наступній ітерації і т. д. до досягнення критерію зупинки [27]. Хоча цей метод є ітеративним, він дозволяє розпаралелювати обробку за рахунок зменшення часової складності.

Метод асоціативних правил (AR) передбачає побудову асоціативних правил щодо надмірності наявних даних [28, 29]. По-перше, усі отримані правила сортуються за якимись параметрами (наприклад, автентичністю). Потім здійснюється пошук набору даних за кожним пропуском та відповідним правилом, яке не суперечить іншим значенням, що знаходяться у відновлюваному рядку. Алгоритм AR має кілька модифікацій. Наприклад, один з них, FP-алгоритм може ефективно паралельно працювати, саме тому його можна використовувати для попередньої обробки великих даних. Однак часову складність цього методу доводиться вдосконалювати.

Метод багатошарового персептрону (MLP) використовує навчену мережу для оцінки відсутніх значень. Оскільки вхідними даними є непусті набори даних, виходами є неповні значення змінних, які потрібно визначити [22, 30, 31]. Заповнення відсутніх значень за допомогою MLP складається з трьох етапів:

– формування повного (навчального) та неповного (тестового) набору;

– побудова MLP на навчальному наборі, де значення змінної є значеннями прогалин, а вхідними значеннями, відповідно, є заповнені значення змінної;

– прогнозування невідомих значень для кожної неповної структури даних за допомогою навченої мережі.

Недоліком цього підходу є прив'язка до набору змінних, що містять відсутні значення, тому потрібно будувати окрему модель MLP для кожної комбінації.

Метод самоорганізованої карти (SOM) [32] дозволяє навчати мережу на основі неповного набору даних. Він запускається завдяки здатності алгоритму ігнорувати відсутні значення та обчислювати відстань між поточним спостереженням і вузлом та використовувати навчену карту для оцінки значень. Недолік SOM такий же, як і MLP.

Глибоке навчання (DL) активно застосовується у багатьох додатках завдяки його потужній здатності до імпутації даних [33]. Глибоко вбудована кластеризація (DEC) вчиться перетворювати з простору даних у простір об’єктів низьких розмірів [34]. У [35] показано здатність представлення ознак автокодера (VAE). VAE вивчає багатогранну структуру даних і досягає високих показників кластеризації [36]. Крім того, VAE має потужну здатність до вилучення та реконструкції функцій, і це може бути хорошим інструментом для обробки неповних даних.

У роботі [37] запропоновано алгоритм VAE, який може покращити ефективність кластеризації мультимедійних даних. На відміну від багатьох існуючих технологій, цей алгоритм вивчає функції даних, проектуючи вдосконалену мережу VAE, і використовує fuzzy c-means алгоритм на основі тензора для кластеризації даних у просторі функцій.

У роботі [38] пропонується розширення варіаційного автокодера (VAE), який називається варіаційним автокодером із зваженими втратами (VAE-WL). Він використовує спеціальну функцію втрат, яка більше підходить для обчислення відсутніх значень.

Найбільшою проблемою методів, проаналізованих вище, є обробка структурованих даних лише тоді, коли напівструктуровані та неструктуровані дані домінують у реальних ситуаціях [39]. Крім того, дуже важливо проаналізувати приховані залежності в наборі даних, а також врахувати характер набору даних та передбачити відсутність даних для кожного джерела даних окремо. Ось чому парадигма великих даних використовується для попередньої обробки та обробки інформації з різних джерел, що складається з безперервних числових даних та категоріальних даних. Тим не менше, природа відсутніх даних у різних джерелах даних теж різна. Отже, основною ідеєю є аналіз даних з різних джерел на основі специфіки та природи цих джерел.

3. Запропонований метод відновлення відсутніх даних. Ми пропонуємо проаналізувати структуру наборів даних, щоб знайти типи невизначеності та створити функцію ідентифікації (посередника) для загальної схеми великих даних на основі всіх джерел даних [39]. Після цього загальну схему можна використовувати для відновлення відсутніх даних безпосередньо у джерелі даних.

Запропонований метод відновлення відсутніх даних базується на функціональних залежностях та правилах асоціації та складається з двох частин:

– видобування ймовірнісних виробничих залежностей на основі інтерфейсу великих даних;

– використання ймовірнісних виробничих залежностей для відновлення відсутніх даних.

Видобування ймовірнісних виробничих залежностей.

Аналіз великих обсягів даних вимагає виявлення груп атрибутів, які утворюють функціональні залежності. Однак, е реальному світі набори даних набагато більш поширені, а важливі залежності визначені тільки на підмножині значень групи ключових атрибутів. Причому залежності можуть з'являтися не тільки для кортежів в реляційних джерелах даних, але і між різними частинами різних кортежів. Будемо називати їх імовірнісною виробничою залежністю (PPD).

Імовірнісна виробнича залежність – це виробниче правило у виборі базового співвідношення, яке діє для значного числа об'єктів в цьому виборі. Поріг значущості повинен визначатися фахівцями або на основі розрахунків ймовірності помилкового вибору цієї залежності. Основна відмінність між асоціативними правилами і PPD полягає в тому, що PPD буде згенеровано з існуючої функціональної залежності в наборі даних.

$$F_1 : K = \{a_i\}, a_i \in A, D = \{a_i\},$$
$$a_i \in A : P(k \in K \to d \in D) = p, \quad (1)$$

де *k* та *d* – набори груп атрибутів *K* і *D*, відповідно

Основним показником надійності такої залежності є відношення кількості об'єктів, які є в такій PPD, до кількості об'єктів у вибірці:

$$P(F_1) = \frac{|\sigma_{k \in K \wedge d \in D}(R)|}{|\sigma_{k \in K}(R)|}. \quad (2)$$

Правило класифікації називається ймовірнісним продуктивним зв'язком між підмножинами атрибутів *X* і *Y* в консолідованих великих даних *Bd*, яка зустрічається в навчальному наборі *bd* з рівнем довіри *s*, де:

$$(\mathrm{X} = \mathrm{x}) \to (Y - y) \quad (3)$$

Правило класифікації побудовано на навчальному наборі даних зі схемою *Bd* з відомими значеннями міток класів. Це правило створено для схеми *Bd*, тому на нього не вплине нова сутність, яка надходить у вибірку великих даних (перевірка незалежності набору даних).

Мітка класу називається лінгвістичною змінною або звичайною характеристикою об'єктів, які є значеннями підмножини атрибутів *Y* і позначають об'єкти з загальними (наприклад, ступенем довіри *s*) значеннями підмножини атрибутів *X*. Домени атрибутів, що належать підмножині атрибутів *Y*, $y \in dom(Y) = \pi_y(Bd)$ повинні містити кінцевий і відомий набір значень.

Мітки класів вибираються з відомого набору значень (в межах області дослідження є фіксованими), а клас об'єктів, який тільки що був введений в консолідоване сховище даних, заснований на правилах класифікації [29]. Теги будуть додаватися автоматично, так як нові джерела даних також додаються в каталог великих даних. Використання ймовірнісних виробничих залежностей для відновлення відсутніх даних. Щоб класифікувати об’єкти (або заповнити відсутні дані), потрібно побудувати правила класифікації. Як правило, великі дані можуть зберігати інформацію про декілька типів класів, і для кожного класу існує підмножина функцій. Цю саму функцію можна використовувати для визначення декількох типів класів.

Правилами класифікації називають PPD, які виконуються для певної підмножини кортежів для консолідованих великих даних *bd*. Розроблено наступний алгоритм імпутації даних.

Для аналізу важлива також послідовність подій, які часто відбуваються. Якщо в таких послідовностях виявляються закономірності, можна з деякою мірою ймовірності передбачити виникнення подій в майбутньому.

Висновки. Запропоновано метод відновлення відсутніх даних у наборах великих даних, який на відміну від існуючих методів, створює додаткові значення даних на основі функціональних залежностей та правил асоціації та додає ці значення до наявних навчальних даних, що, в свою чергу, дало змогу підвищити ефективність подальшого аналізу даних.

Даний метод полягає в обробці структурованих та напівструктурованих даних на основі ієрархії об’єктів, а також набору функціональних залежностей та розробки правил асоціації. Це питання дуже важливе для інтерфейсів великих даних, оскільки більша частина інформації доступна в напівструктурованому вигляді. Запропонований метод створює додаткові значення даних за допомогою доменних та

функціональних залежностей на основі декількох методів обчислення та додає ці значення до наявних навчальних даних. Правильність обчислених значень перевіряється на класифікаторі, побудованому на вихідному наборі даних.

Література

1. He Y. Missing data analysis using multiple imputation. Circulation: Cardiovascular Quality and Outcomes. 2010. 3(1). 98-105.
2. Little R. J. A., Rubin D. B. Statistical analysis with missing data. John Wiley & Sons, 2019. 464 p.
3. Ahmat Zainuri, N., Jemain, A. A., Muda, N. A Comparison of Various Imputation Methods for Missing Values in Air Quality Data. JSM, 2015, 44, 449-456.
4. Leke, C. A., Marwala, T. Introduction to Missing Data Estimation. Deep Learning and Missing Data in Engineering Systems. 2019, 1-20. https://doi. org/10.1117/12.2053057 [Access 18.07.2020].
5. Zhang, S.; Yang, Z.; Xing, X.; Gao, Y.; Xie, D.; Wong, H.S. Generalized Pair-Counting Similarity Measures for Clustering and Cluster Ensembles. IEEE Access. 2017, 5, 16904–16918.
6. Hoecker, M.; Polsterer, K.L.; Kugler, S.D.; Heuveline, V. Clustering of Complex Data-Sets Using Fractal Similarity Measures and Uncertainties. In Proceedings of the 2015 IEEE 18th International Conference on Computational Science and Engineering, Porto, Portugal, 21–23 October 2015; pp. 82–91.
7. Zhou, L.;Wu, D.; Zheng, B.; Guizani, M. Joint physical-application layer security for wireless multimedia delivery. IEEE Commun. Mag. 2014, 52, 66–72.
8. Li, F.; Qiao, H.; Zhang, B. Discriminatively boosted image clustering with fully convolutional auto-encoders. Pattern Recognit. 2018, 83, 161–173.
9. Gebru, I.D.; Alameda-Pineda, X.; Forbes, F.; Horaud, R. EM Algorithms for Weighted-Data Clustering with Application to Audio-Visual Scene Analysis. IEEE Trans. Pattern Anal. Mach. Intell. 2016, 38, 2402–2415.
10. Abualigah, L.M.; Khader, A.T.; Al-Betar, M.A. Unsupervised feature selection technique based on genetic algorithm for improving the Text Clustering. In Proceedings of the 2016 7th International Conference on Computer Science and Information Technology (CSIT), Amman, Jordan, 13–14 July 2016; pp. 1–6.
11. Saadaoui, F.; Bertrand, P.R.; Boudet, G.; Rouffiac, K.; Dutheil, F.; Chamoux, A. A Dimensionally Reduced Clustering Methodology for Heterogeneous Occupational Medicine Data Mining. IEEE Trans. Nanobiosci. 2015, 14, 707–715.
12. Zhou, Q. Research on heterogeneous data integration model of group enterprise based on cluster computing. Clust. Comput. 2016, 19, 1275–1282.
13. Ramachandran, N.; Perumal, V. Delay-aware heterogeneous cluster-based data acquisition in Internet of Things. Comput. Electr. Eng. 2018, 65, 44–58.
14. Meng, L.; Tan, A.H.; Xu, D. Semi-Supervised Heterogeneous Fusion for Multimedia Data Co-Clustering. IEEE Trans. Knowl. Data Eng. 2014, 26, 2293–2306.
15. Li, P.; Chen, Z.; Yang, L.T.; Zhao, L.; Zhang, Q. A privacy-preserving high-order neuro-fuzzy C-means algorithm with cloud computing. Neurocomputing 2017, 256, 82–89.
16. Zhang, Q.; Yang, L.T.; Chen, Z.; Li, P. High-order possibilistic c-means algorithms based on tensor decompositions for big data in IoT. Inf. Fusion 2018, 39, 72–80.
17. Kowarik, A., Templ, M. Imputation with the R Package. VIM, 2016. https://doi.org/10.18637/jss.v074.i07 [Access 18.07.2020].
18. Lin, T. H. A Comparison of Multiple Imputation with EM Algorithm and MCMC Method for Quality of Life Missing Data. Quality and Quantity, 2010, 44, 277-287.
19. Myers, T. A. Goodbye, Listwise Deletion: Presenting Hot Deck Imputation as an Easy and Effective Tool for Handling Missing Data. Communication Methods and Measures, 2011, 5, 297-310.
20. Shakhovska, N., Strubytskyi, R. Model of Data Warehouse with Uncertain Consolidated Data. Applied Mathematics & Information Sciences, 2015, 9(4). http://dx.doi.org/10.12785/amis/090412 [Access 18.07.2020].
21. Pedersen, A. B., Mikkelsen, E. M., Cronin-Fenton, D., Kristensen, N. R., Pham, T. M., Pedersen, L., Petersen, I. Missing Data and Multiple Imputation in Clinical Epidemiological Research. Clinical Epidemiology, 2017, 9, 157-166.
22. Nelwamondo, F. V., Mohamed, S., Marwala, T. Missing Data: A Comparison of Neural Network and Expectation Maximisation Techniques, 2007, arXiv:0704.3474 [Access 18.07.2020].
23. Lim, S. Y., Mohamad, M. S., Chai, L. E., Deris, S., Chan, W. H., Omatu, S., Ibrahim, Z. Investigation of the Effects of Imputation Methods for Gene Regulatory Networks Modelling Using Dynamic Bayesian Networks. Distributed Computing and Artificial Intelligence, 13th International Conference, 2016, 413-421.
24. Aydilek, I. B., Arslan, A. A Hybrid Method for Imputation of Missing Values Using Optimized Fuzzy C-Means with Support Vector Regression and a Genetic Algorithm. Information Sciences, 2013, 233, 25-35.
25. Alhroob, A., Alzyadat, W., Almukahel, I., Altarawneh, H. Missing Data Prediction Using Correlation Genetic Algorithm and SVM Approach. Population, 2020, 11(2). https://doi.org/10.14569/IJACSA.2020.0110288 [Access 18.07.2020].
26. Siroky, D. S. Navigating Random Forests and Related Advances in Algorithmic Modeling. Statistics Surveys, 2009, 3, 147-163.
27. Rahman, Md. G., Islam, M. Z. Missing Value Imputation Using Decision Trees and Decision Forests by Splitting and Merging Records: Two Novel Techniques. Knowledge-Based Systems, 2013, 53, 51-65.
28. Raković, L., Sakal, M., Matković, P., Marić, M. Shadow IT-Systematic Literature Review. Information Technology and Control, 2020, 49(1), 144-160.
29. Shakhovska, N., Kaminskyy, R., Zasoba, E., Tsiutsiura, M. Association Rules Mining in Big Data. International Journal of Computing, 2018, 17(1), 25-32.
30. Jung, S., Moon, J., Park, S., Rho, S., Baik, S. W., Hwang, E. Bagging Ensemble of Multilayer Perceptrons for Missing Electricity Consumption Data Imputation. Sensors, 2020, 20(6). https://doi.org/10.3390/ s20061772 [Access 18.07.2020].
31. Sachenko A., Kochan V., Turchenko V. Instrumentation for Gathering Data. IEEE Instrumentation and Measurement Magazine, 2003, 6 (3), 34-40.
32. Jurgelevičius, A., Sakalauskas, L. Big Data Mining Using Public Distributed Computing. Information Technology and Control, 2018, 47(2), 236-248.
33. Mohammadi, M.; Al-Fuqaha, A.; Sorour, S.; Guizani, M. Deep Learning for IoT Big Data and Streaming Analytics: A Survey. IEEE Commun. Surv. Tutor. 2018, 20, 2923–2960.
34. Xie, J.; Girshick, R.; Farhadi, A. Unsupervised Deep Embedding for Clustering Analysis. arXiv 2015, arXiv:1511.06335 [Access 18.07.2020].

35. Kingma, D.P.;Welling, M. Auto-Encoding Variational Bayes. arXiv 2013, arXiv:1312.6114 [Access 18.07.2020].
36. Li, X.; Chen, Z.; Poon, L.K.M.; Zhang, N.L. Learning Latent Superstructures in Variational Autoencoders for Deep Multidimensional Clustering. arXiv 2018, arXiv:1803.05206 [Access 18.07.2020].
37. Yu X, Li H, Zhang Z, Gan C. The Optimally Designed Variational Autoencoder Networks for Clustering and Recovery of Incomplete Multimedia Data. *Sensors*. 2019; 19(4):809.
38. Ricardo Cardoso Pereira , Joana Cristo Santos , Jos´e Pereira Amorim , Pedro Pereira Rodrigues and Pedro Henriques Abreu. Missing Image Data Imputation using Variational Autoencoders with Weighted Loss // In Proceedings European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning (ESANN 2020), 2-4 October 2020. http://www.i6doc.com/en/ [Access 18.07.2020].
39. Shakhovska, N., Vovk, O., Kryvenchuk, Y. Uncertainty Reduction in Big Data Catalogue for Information Product Quality Evaluation. Eastern-European Journal of Enterprise Technologies, 2018, 1, 12-20.

References

1. He Y. Missing data analysis using multiple imputation. Circulation: Cardiovascular Quality and Outcomes. 2010. 3(1). 98-105.
2. Little R. J. A., Rubin D. B. Statistical analysis with missing data. John Wiley & Sons, 2019. 464 p.
3. Ahmat Zainuri, N., Jemain, A. A., Muda, N. A Comparison of Various Imputation Methods for Missing Values in Air Quality Data. JSM, 2015, 44, 449-456.
4. Leke, C. A., Marwala, T. Introduction to Missing Data Estimation. Deep Learning and Missing Data in Engineering Systems. 2019, 1-20. https://doi. org/10.1117/12.2053057 [Access 18.07.2020].
5. Zhang, S.; Yang, Z.; Xing, X.; Gao, Y.; Xie, D.; Wong, H.S. Generalized Pair-Counting Similarity Measures for Clustering and Cluster Ensembles. IEEE Access. 2017, 5, 16904–16918.
6. Hoecker, M.; Polsterer, K.L.; Kugler, S.D.; Heuveline, V. Clustering of Complex Data-Sets Using Fractal Similarity Measures and Uncertainties. In Proceedings of the 2015 IEEE 18th International Conference on Computational Science and Engineering, Porto, Portugal, 21–23 October 2015; pp. 82–91.
7. Zhou, L.;Wu, D.; Zheng, B.; Guizani, M. Joint physical-application layer security for wireless multimedia delivery. IEEE Commun. Mag. 2014, 52, 66–72.
8. Li, F.; Qiao, H.; Zhang, B. Discriminatively boosted image clustering with fully convolutional auto-encoders. Pattern Recognit. 2018, 83, 161–173.
9. Gebru, I.D.; Alameda-Pineda, X.; Forbes, F.; Horaud, R. EM Algorithms for Weighted-Data Clustering with Application to Audio-Visual Scene Analysis. IEEE Trans. Pattern Anal. Mach. Intell. 2016, 38, 2402–2415.
10. Abualigah, L.M.; Khader, A.T.; Al-Betar, M.A. Unsupervised feature selection technique based on genetic algorithm for improving the Text Clustering. In Proceedings of the 2016 7th International Conference on Computer Science and Information Technology (CSIT), Amman, Jordan, 13–14 July 2016; pp. 1–6.
11. Saadaoui, F.; Bertrand, P.R.; Boudet, G.; Rouffiac, K.; Dutheil, F.; Chamoux, A. A Dimensionally Reduced Clustering Methodology for Heterogeneous Occupational Medicine Data Mining. IEEE Trans. Nanobiosci. 2015, 14, 707–715.
12. Zhou, Q. Research on heterogeneous data integration model of group enterprise based on cluster computing. Clust. Comput. 2016, 19, 1275–1282.
13. Ramachandran, N.; Perumal, V. Delay-aware heterogeneous cluster-based data acquisition in Internet of Things. Comput. Electr. Eng. 2018, 65, 44–58.
14. Meng, L.; Tan, A.H.; Xu, D. Semi-Supervised Heterogeneous Fusion for Multimedia Data Co-Clustering. IEEE Trans. Knowl. Data Eng. 2014, 26, 2293–2306.
15. Li, P.; Chen, Z.; Yang, L.T.; Zhao, L.; Zhang, Q. A privacy-preserving high-order neuro-fuzzy C-means algorithm with cloud computing. Neurocomputing 2017, 256, 82–89.
16. Zhang, Q.; Yang, L.T.; Chen, Z.; Li, P. High-order possibilistic c-means algorithms based on tensor decompositions for big data in IoT. Inf. Fusion 2018, 39, 72–80.
17. Kowarik, A., Templ, M. Imputation with the R Package. VIM, 2016. https://doi.org/10.18637/jss.v074.i07 [Access 18.07.2020].
18. Lin, T. H. A Comparison of Multiple Imputation with EM Algorithm and MCMC Method for Quality of Life Missing Data. Quality and Quantity, 2010, 44, 277-287.
19. Myers, T. A. Goodbye, Listwise Deletion: Presenting Hot Deck Imputation as an Easy and Effective Tool for Handling Missing Data. Communication Methods and Measures, 2011, 5, 297-310.
20. Shakhovska, N., Strubytskyi, R. Model of Data Warehouse with Uncertain Consolidated Data. Applied Mathematics & Information Sciences, 2015, 9(4). http://dx.doi.org/10.12785/amis/090412 [Access 18.07.2020].
21. Pedersen, A. B., Mikkelsen, E. M., Cronin-Fenton, D., Kristensen, N. R., Pham, T. M., Pedersen, L., Petersen, I. Missing Data and Multiple Imputation in Clinical Epidemiological Research. Clinical Epidemiology, 2017, 9, 157-166.
22. Nelwamondo, F. V., Mohamed, S., Marwala, T. Missing Data: A Comparison of Neural Network and Expectation Maximisation Techniques, 2007, arXiv:0704.3474 [Access 18.07.2020].
23. Lim, S. Y., Mohamad, M. S., Chai, L. E., Deris, S., Chan, W. H., Omatu, S., Ibrahim, Z. Investigation of the Effects of Imputation Methods for Gene Regulatory Networks Modelling Using Dynamic Bayesian Networks. Distributed Computing and Artificial Intelligence, 13th International Conference, 2016, 413-421.
24. Aydilek, I. B., Arslan, A. A Hybrid Method for Imputation of Missing Values Using Optimized Fuzzy C-Means with Support Vector Regression and a Genetic Algorithm. Information Sciences, 2013, 233, 25-35.
25. Alhroob, A., Alzyadat, W., Almukahel, I., Altarawneh, H. Missing Data Prediction Using Correlation Genetic Algorithm and SVM Approach. Population, 2020, 11(2). https://doi.org/10.14569/IJACSA.2020.0110288 [Access 18.07.2020].
26. Siroky, D. S. Navigating Random Forests and Related Advances in Algorithmic Modeling. Statistics Surveys, 2009, 3, 147-163.
27. Rahman, Md. G., Islam, M. Z. Missing Value Imputation Using Decision Trees and Decision Forests by Splitting and Merging Records: Two Novel Techniques. Knowledge-Based Systems, 2013, 53, 51-65.
28. Raković, L., Sakal, M., Matković, P., Marić, M. Shadow IT-Systematic Literature Review. Information Technology and Control, 2020, 49(1), 144-160.
29. Shakhovska, N., Kaminskyy, R., Zasoba, E., Tsiutsiura, M. Association Rules Mining in Big Data. International Journal of Computing, 2018, 17(1), 25-32.
30. Jung, S., Moon, J., Park, S., Rho, S., Baik, S. W., Hwang, E. Bagging Ensemble of Multilayer Perceptrons for Missing Electricity Consumption Data Imputation. Sensors, 2020, 20(6). https://doi.org/10.3390/ s20061772 [Access 18.07.2020].
31. Sachenko A., Kochan V., Turchenko V. Instrumentation for Gathering Data. IEEE Instrumentation and Measurement Magazine, 2003, 6 (3), 34-40.

32. Jurgelevičius, A., Sakalauskas, L. Big Data Mining Using Public Distributed Computing. Information Technology and Control, 2018, 47(2), 236-248.

33. Mohammadi, M.; Al-Fuqaha, A.; Sorour, S.; Guizani, M. Deep Learning for IoT Big Data and Streaming Analytics: A Survey. IEEE Commun. Surv. Tutor. 2018, 20, 2923–2960.

34. Xie, J.; Girshick, R.; Farhadi, A. Unsupervised Deep Embedding for Clustering Analysis. arXiv 2015, arXiv:1511.06335 [Access 18.07.2020].

35. Kingma, D.P.;Welling, M. Auto-Encoding Variational Bayes. arXiv 2013, arXiv:1312.6114 [Access 18.07.2020].

36. Li, X.; Chen, Z.; Poon, L.K.M.; Zhang, N.L. Learning Latent Superstructures in Variational Autoencoders for Deep Multidimensional Clustering. arXiv 2018, arXiv:1803.05206 [Access 18.07.2020].

37. Yu X, Li H, Zhang Z, Gan C. The Optimally Designed Variational Autoencoder Networks for Clustering and Recovery of Incomplete Multimedia Data. *Sensors*. 2019; 19(4):809.

38. Ricardo Cardoso Pereira , Joana Cristo Santos , Jos´e Pereira Amorim , Pedro Pereira Rodrigues and Pedro Henriques Abreu. Missing Image Data Imputation using Variational Autoencoders with Weighted Loss // In Proceedings European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning (ESANN 2020), 2-4 October 2020. http://www.i6doc.com/en/ [Access 18.07.2020].

39. Shakhovska, N., Vovk, O., Kryvenchuk, Y. Uncertainty Reduction in Big Data Catalogue for Information Product Quality Evaluation. Eastern-European Journal of Enterprise Technologies, 2018, 1, 12-20.

Надійшла / Paper received: 28.09.2020 Надрукована / Paper Printed : 01.12.2020

УДК 004.421.5:004.942
DOI: 10.31891/2219-9365-2020-66-2-16

ОРЛЕНКО В. С., ЧЕШУН В. М., АНДРОЩУК О. С.
Хмельницький національний університет
КАТАЄВА А. І.
Донецький національний університет імені Василя Стуса

МОДЕЛЬ ГЕНЕРАТОРА КРИПТОКЛЮЧІВ З ДЖЕРЕЛАМИ ЕНТРОПІЇ ДЛЯ СИСТЕМИ КЛІЄНТ-БАНК

Однією із важливих складових безпеки системи клієнт-банк є механізми захисту, що базуються на використанні криптоключів. Стійкість криптоключів є запорукою надійності системи і, в свою чергу, базується на механізмах генерації псевдовипадкових чисел із застосуванням джерел первинної ентропії, для ефективного використання яких необхідною є наявність адекватних моделей і математичного апарату.

У роботі представлено елементи математичної моделі джерел ентропії і узагальнену графічну модель процесу генерації псевдовипадкових двійкових кодів, які орієнтовані на реалізацію генератора криптоключів для системи клієнт-банк з використанням одного або декількох джерел первинної ентропії. Описано особливості реалізації основних етапів процесу генерації криптоключів підвищеної ентропії та надані рекомендації щодо використання функцій математичної моделі, доведено адекватність запропонованих моделей вирішуваним задачам.

Моделі орієнтовані на реалізацію методу та засобів генерації псевдовипадкових чисел підвищеної ентропії і можуть бути застосовані для зменшення ризиків отримання несанкціонованого доступу до клієнтської інформації в системі клієнт-банк через розкриття криптоключів. В якості джерел ентропії можуть бути використані датчики мобільного телефона або інші пристрої та явища, які характеризуються здатністю формувати пул значень з високим рівнем ентропії.

Ключові слова: система клієнт-банк, криптографічний ключ, генератор псевдовипадкових чисел, ентропія.

ORLENKO V., CHESHUN V., ANDROSHCHUK O.
Khmelnytskyi National University
KATAIEVA A.
Vasyl' Stus Donetsk National University

MODEL OF CRYPTOGRAPHIC KEYS GENERATOR WITH ENTROPY SOURCES FOR THE CLIENT-BANK SYSTEM

One of the important components of the security of the client-bank system is the protection mechanisms based on the use of cryptographic keys. The stability of cryptographic keys is a guarantee of system reliability and, in turn, is based on the mechanisms of generating pseudo-random numbers using primary entropy sources, for the effective use of which it is necessary to have adequate models and mathematical apparatus.

The paper presents elements of the mathematical model of entropy sources and a generalized graphical model of the process of generating pseudo-random binary codes, which are focused on the implementation of the cryptographic keys generator for the client-bank system using one or more primary entropy sources. Peculiarities of realization of the main stages of the process of generating cryptographic keys of high entropy are described and recommendations on the use of functions of the mathematical model are given, the adequacy of the offered models to the solved problems is proved.

The models are focused on the implementation of the method and means of generating pseudo-random numbers of high entropy and can be used to reduce the risk of unauthorized access to customer information in the client-bank system through the disclosure of cryptographic keys. Mobile phone sensors or other devices and phenomena, that are characterized by the ability to form a pool of values with a high level of entropy, can be used as sources of entropy.

Keywords: client-bank system, cryptographic key, pseudo-random number generator, entropy.

Вступ і загальна постановка проблеми. В сучасних умовах абсолютно неможливо уявити діяльність банківської системи України та світу без застосування засобів автоматизації, комп'ютеризації та інформатизації. Основою механізму автоматизованого надання послуг клієнтам банківських установ стала система клієнт-банк – комплекс програмно-апаратних засобів для забезпечення безпечної взаємодії між банком та клієнтом. Враховуючи масштабне вторгнення в сферу банківських послуг інтернет технологій і неможливість існування системи клієнт-банк без їх застосування, останню досить часто ідентифікують як систему електронного банкінгу (e-banking), онлайн-банкінгу (online banking), інтернет-банкінгу або веб-банкінгу [1, 2].

Загалом, систему клієнт-банк можна розглядати як комплекс сервісів і механізмів захисту, які орієнтовані на забезпечення максимальної зручності і безпеки роботи клієнтів з системою.

На прикладі системи «iBank 2 UA» [2, 3] до типових сервісів системи клієнт-банк можна віднести різні види організації доступу до банківських послуг:

– з персонального комп'ютера через пряме з'єднання з банківською мережею (PC banking);
– з телефону в режимі телефонного зв'язку (Phone banking);
– з мобільного телефону клієнта із застосуванням SMS-повідомлень (SMS-банкінг);

– з мобільного телефону із застосуванням спеціалізованих протоколів безпровідної передачі даних WAP GPRS (WAP-банкінг);

– з мобільного телефону із застосуванням спеціального додатку мобільного банкінгу (Mobile-банкінг);

– із застосуванням ресурсів мережі Інтернет (Internet-банкінг, WEB-банкінг, Online-банкінг) тощо.

Для захисту сервісів системи [3–5] використовуються механізми електронного цифрового підпису, хеш функцій, розповсюдження ключів сесії із застосуванням алгоритмів асиметричного шифрування, симетричне шифрування та захищений протокол передачі і автентифікації.

Більшість із зазначених механізмів базується на використанні криптоключів (ключів сесії, ключів підпису тощо), для генерації яких використовуються різні способи і засоби генерації псевдовипадкових чисел як основа забезпечення випадковості, непередбачуваності і криптостійкості значень криптоключів. Це робить систему клієнт-банк як об’єкт захисту в умовах існування ризиків та загроз банківській діяльності в кіберпросторі значною мірою залежною від якості і зручності застосовуваних генераторів криптоключів, що зумовлює актуальність і підвищену зацікавленість у розробці ефективних методів та засобів генерації криптоключів підвищеної ентропії.

Аналіз стану досліджень та публікацій. Генерація криптоключів системи клієнт-банк базується на використанні псевдовипадкових чисел та засобів їх генерації.

Генератори псевдовипадкових чисел (ГПВЧ) набули широкого застосування в різноманітних технічних задачах [6], що зумовило появу великої кількості методів та засобів генерації випадкових і псевдовипадкових чисел. В засобах банківської безпеки, зокрема, випадкові числа широко застосовуються в схемах взаємної аутентифікації. У більшості сценаріїв аутентифікації й розподілу ключа для запобігання атак повторного відтворення (replay-атак) використовуються одноразові коди nonces (від англійського «number that can only be used once» – число, яке може бути використане один раз). Застосування дійсно випадкових чисел у якості кодів nonces не дає супротивникові можливості обчислити або вгадати їх значення.

Генерація якісної випадкової послідовності чисел – найскладніша частина багатьох криптографічних операцій [6].

Спеціалізовані криптографічно сильні ГПВЧ в якості джерел ентропії використовують радіоактивний розпад, фізичні явища оптично-квантової механіки, електричні шуми [7–9]. Хоча подібні ГПВЧ і дають якісні характеристики ентропії послідовності чисел, для масового використання в системах типу клієнт-банк вони не є зручними і доступними.

Базисом ГПВЧ електронних систем, як правило, є програмні або апаратні методи генерації та їх комбінації [6].

Програмні ГПВЧ базуються на певному методі генерації, реалізованому алгоритмічно. До алгоритмічних методів відносять[6,10]:

– метод середини квадрата Джона фон Неймана;

– метод лінійного конгруента Лехмера;

– підвиди алгоритмів Фібоначчі;

– алгоритм Блюма–Блюма–Шуба;

– вихор Мерсенна (генератор Мацумото і Нишимури) тощо.

Апаратні ГПВЧ представлені різноманітними моделями, серед яких можна виділити ряд базових[7, 10, 11]:

– генератори на регістрах зсуву з зворотним зв'язком (FSR);

– генератори на регістрах зсуву з лінійним зворотним зв'язком (LFSR);

– ГПВЧ Геффа;

– ГПВЧ «стій–рушай» («stop-and-go») тощо.

Хоча апаратні генератори і не передбачають програмної реалізації алгоритму, в генерованій послідовності чисел наявні залежності, які можуть бути описані алгоритмічно.

Наявність алгоритмічної залежності між числами (певного закону розподілу чисел) в псевдовипадкових послідовностях дозволяє говорити про їх випадковість і непередбачуваність лише в певному обмеженому аспекті, що зумовлює їх вразливості до методів криптоаналізу [7].

Окремий клас ГПВЧ утворюють криптографічні генератори [10, 12]:

– ГПВЧ з циклічним шифруванням;

– ГПВЧ із застосуванням режиму Output Feedback DES;

– ГПВЧ генератор ANSI X9.17 тощо).

Робота криптографічних ГПВЧ базується на методах та алгоритмах сучасної криптографії. Надійність криптографічні ГПВЧ забезпечується не лише набором і послідовністю криптографічних операцій, а і вибором стартових значень (вектор ініціалізації, майстер-ключ), з яких починається виконання цих операцій. Стартові значення для запуску алгоритму генерації криптографічного ГПВЧ формуються із застосуванням явищ або засобів, оцінювані параметри яких можуть розглядатися як випадкові. Зазначені

явища та засоби використовуються для збільшення ентропії генерованих в різних сеансах послідовностей чисел і розглядаються як джерела первинної ентропії ГПВЧ [6, 7, 13].

До джерел первинної ентропії, що використовуються роботі систем клієнт-банк, відносяться специфічні властивості технічних засобів безпосередньо або у взаємодії з людиною: показники системного годинника, специфічні особливості набору на клавіатурі або роботи з «мишею», параметри локальної або глобальної комп'ютерної мережі, параметри інтегрованих компонентів системи, зміни часу доступу до жорсткого диску тощо [6, 14]. В [6] також зазначається, що такі джерела мають недостатню ентропію і низьку продуктивність, що унеможливлює використання їх як ГПВЧ безпосередньо, але дозволяє їх розгляд як слабких криптографічно джерел первинної ентропії.¤

Стрімке вторгнення на ринок банківських послуг мобільного банкінгу створює не лише нові загрози, але і нові можливості. Зокрема, в [15, 16] описується технологія застосування датчиків мобільних пристроїв в якості ГПВЧ.

Аналіз специфіки роботи датчиків мобільних пристроїв, характерна змінюваність складу датчиків між моделями та різна їх продуктивність – сукупність факторів, які не дозволяють розглядати зазначені датчики як стабільні і високопродуктивні генератори криптоключів системи клієнт банк. В той же час, отримані в ході аналізу результати надають можливість висунення гіпотези про перспективність їх використання в якості ефективних джерел первинної ентропії.

Формулювання цілі статті. Для якісного розв'язування задачі генерації криптоключів системи клієнт-банк із застосуванням датчиків мобільних пристроїв в якості джерел первинної ентропії, в умовах надзвичайно високої складності застосовуваних алгоритмів і методів, великої актуальності набуває вибір математичної моделі для формалізованого представлення даних і ефективної організації їх обробки.

Базові елементи моделі джерел ентропії. Для отримання якісного криптографічного генератора псевдовипадкових чисел необхідне виконання ряду умов [6, 12]:

– наявність джерела первинної ентропії;

– визначення способу формування числового представлення вимірюваних параметрів джерела первинної ентропії;

– алгоритм обробки, перетворення і накопичення даних, що містять ентропію;

– спосіб формування послідовності чисел із якісними показниками випадковості на основі даних первинної ентропії.

Для отримання джерела первинної ентропії з достатніми характеристиками невизначеності в формованому цифровому значенні, яке стане основою для генерації псевдовипадкових векторів двійкового коду, першчергово необхідно мати інструментарій кількісної оцінки ентропії джерела.

Мінімальна ентропія Hmin(X) характеризує найгірший з можливих варіант невизначеності щодо об'єкта X: якщо об'єкту X властива мінімальна ентропія h, то імовірність появи певного значення (будь-якого з можливих) не перевищує 2-h.

Припустимо, що qi – цифрове представлення отримуваного від джерела ентропії вектора. Утворимо множину отримуваних від джерела ентропії значень:

Qдж.:{q1, q2,…, qi,…, qp} – множина вихідних значень з джерела ентропії, представлених в цифровому вигляді.

В багатьох реалізаціях ГПВЧ для збільшення ентропії самого генератора використовується одразу декілька джерел початкової ентропії. Якщо умовно прийняти, що таких джерел для реалізації ГПВЧ застосовано в кількості n, то вони утворюють множину джерел ентропії:

D : {d1, d2,…, dj,…, dn} – множина використовуваних джерел ентропії (датчиків мобільного пристрою).

За таких умов різноманіття вихідних значень з джерел ентропії можна описати сукупністю множин:

Qдж.1:{q1.1, q1.2,…, q1.i,…, q1.p} – множина представлених в цифровому вигляді векторів вихідних значень з першого джерела ентропії;

Qдж.2:{q2.1, q2.2,…, q2.i,…, q2.p} – множина представлених в цифровому вигляді векторів вихідних значень з другого джерела ентропії;

…

Qдж.j:{qj.1, qj.2,…, qj.i,…, qj.p} – множина представлених в цифровому вигляді векторів вихідних значень з j-го джерела ентропії (1< j < n);

…

Qдж.n:{qn.1, qn.2, …, qn.i, …, qn.p} – множина представлених в цифровому вигляді векторів вихідних значень з n-го джерела ентропії.

Неважко побачити, що при n=1 наведена модель зведеться до початкового опису множини вихідних значень з єдиного джерела ентропії. Таким чином, при розгляді задачі створення ГПВЧ доцільно використовувати модель з n джерелами ентропії, окремим варіантом реалізації якої є модель з єдиним джерелом ентропії при n = 1.

Для кожного значення qj.i ∈ Qдж.j можна визначити статистичну імовірність p(qi) того, що воно буде отримане від джерела в будь-якій операції зчитування вектора даних з джерела ентропії.

Таким чином, ми можемо сформувати множину статистичних даних імовірності отримання різноманітних значень показників датчиків:

Qдж.j:{p(qj.1), p(qj.2), …, p(qj.i), …, p(qj.m)} – множина імовірнісних характеристик появи вихідних значень qj.i ∈ Qдж.j з j-го джерела ентропії ($1 \le j \le n$).

За таких умов мінімальна ентропія джерела Qдж.j буде визначатися за формулою:

$$H_{\min}\left(Q_{\text{дж}.j}\right) = \min\left(-\log_2 p\left(q_{j.i}\right)\right) = -\log_2\left(\max p\left(q_{j.i}\right)\right). \quad (1)$$

У ідеального джерела ентропії імовірності появи всіх значень qj.i ∈ Qдж.j мають бути однаковими:

$$p(qj.i) = p(qj.k)\ \forall\ (qj.i \in Qдж.j,\ qj.k \in Qдж.j,\ i \neq k). \quad (2)$$

Умова (2) описує ідеальне джерело ентропії за показниками імовірності отримання різних значень за умови, що вказані значення qj.i ∈ Qдж.j не є взаємозалежними. На основі (1) і (2) може бути здійснено відбір якісних джерел ентропії і відсів слабких джерел.

Основою джерела ентропії є джерело шуму – певний елемент або явище, що характеризується недетермінованою характеристикою, яка задає ентропію і відповідає за невизначеність значень qj.i ∈ Qдж.j. Якщо джерело шуму і, як наслідок, утворюване ним джерело ентропії неякісні, жоден механізм ГПВЧ не зможе компенсувати брак ентропії.

Класичне джерело ентропії формує випадкові значення у вигляді цифрових векторів, отриманих з недетермінованого процесу. Якщо використовуваний недетермінований процес джерела шуму не формує одразу цифрові вектори, а видає певні аналогові різновиди досліджуваного сигналу, процедура формування зазначених векторів включає операцію оцифровування (дискретизації).

В ідеалі значення, отримувані від джерела шуму, повинні бути представлені двійковими кодами (векторами двійкових кодів) однакової розрядності, яка визначається потребами реалізації методу генерації псевдовипадкових чисел.

До джерел ентропії висувається ряд вимог [8, 16], які, з урахуванням елементів моделі, можна уточнити:

– вихідні вектори qj.i ∈ Qдж.j повинні бути незалежними і не підпорядковуватись законам, що можуть бути описані алгоритмічними процедурами будь-якої складності;

– джерело ентропії має бути зручним у використанні за призначенням;

– джерело ентропії повинно бути придатним до випробувань на функціональність;

– процес зняття вихідних значень qj.i ∈ Qдж.j не повинен впливати на загальну роботу джерела;

– джерело ентропії повинне бути незалежним від зовнішніх факторів і впливів.

Модель процесу генерації псевдовипадкових двійкових векторів підвищеної ентропії.

Робочий процес генерації випадкових значень згідно з наведеними описами і отриманими в ході досліджень результатами можна розділити на послідовні етапи:

– первинне отримання показників датчиків qj.i ∈ Qдж.j;

– виділення з коду векторів qj.i ∈ Qдж.j розрядів, що несуть максимальну ентропійну складову;

– перетворення векторів qj.i ∈ Qдж.j в вектор двійкового коду фіксованої розрядності, необхідної для реалізації криптографічного методу генерації псевдовипадкових чисел;

– реалізація криптографічного методу генерації псевдовипадкових чисел.

Для математичного опису процесу генерації псевдовипадкових значень введемо позначення перелічених функцій перетворення ентропійних шумів:

F1 – оператор отримання показників датчиків (операція аналого-цифрового перетворення при використанні аналогових датчиків тощо);

F2 – оператор виділення з вектора (векторів) цифрового коду розрядів, що несуть максимальну складову ентропії;

F3 – функція перетворення складових векторів з виходу функції F2 в єдиний вектор з максимальним збереженням ентропійних властивостей, отримуваних від джерел ентропії;

F4 – оператор перетворення вектора з виходу функції F3 в вектор двійкового коду фіксованої розрядності, необхідної для реалізації криптографічного методу генерації псевдовипадкових чисел;

F5 – функція криптографічного методу генерації псевдовипадкових чисел (криптоключів тощо).

За наведеним переліком і описом операцій розроблено узагальнену графічну модель роботи генератора (рис. 1).

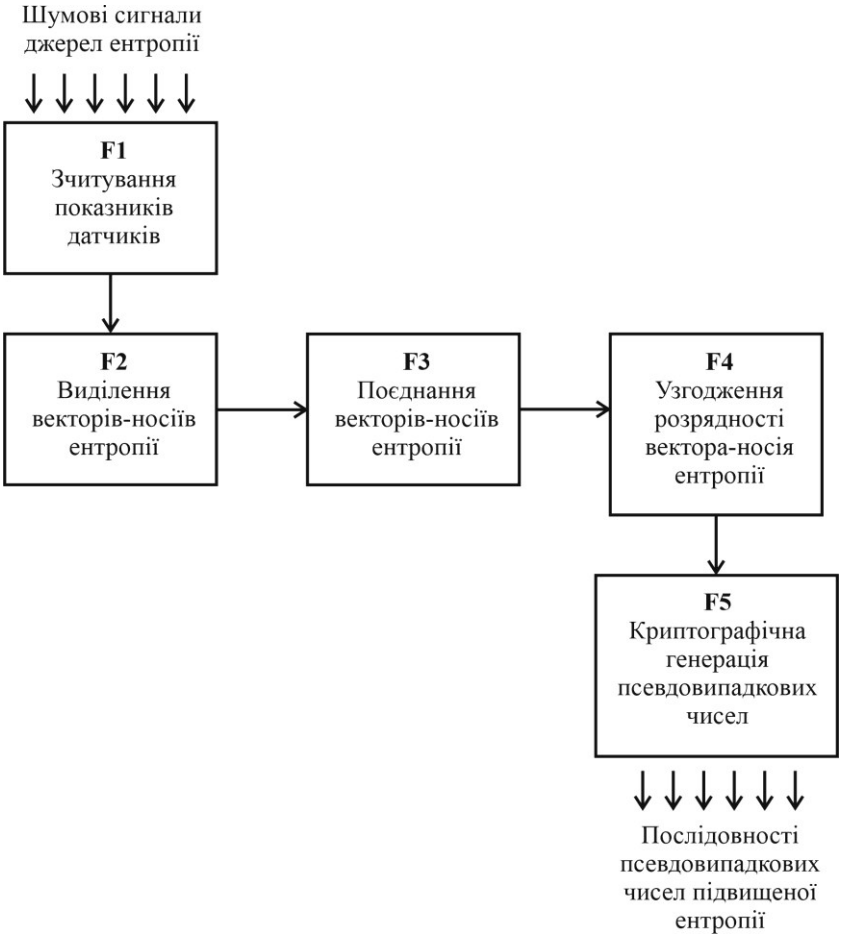


Рис. 1. Узагальнена модель процесу генерації псевдовипадкових чисел підвищеної ентропії

Три рівні наведеної на рис. 1 моделі відповідають розподілу функцій F1–F5 за загальним цільовим призначенням:

– перший рівень представлений функцією F1 і відповідає за сприйняття даних від джерела ентропії і представлення їх у формі, придатній для обробки цифровими програмно-апаратними системами, до числа яких відноситься і система клієнт-банк;

– другий рівень представлений групою функцій F2–F4 і відповідає операціям перетворення початкових цифрових даних, сформованих за недермінованими сигналами від джерела ентропії функцією F1, з метою отримання формату їх представлення, потрібного для реалізації обраного криптографічного алгоритму генерації псевдовипадкових значень;

– третій рівень представлений функцією F5 і відповідає етапу реалізації обраного криптографічного алгоритму генерації псевдовипадкових значень на основі вхідних даних підвищеної ентропії.

Слід відзначити абсолютну значимість всіх перелічених етапів для отримання якісного результату від робочого процесу ГПВЧ.

Дослідимо особливості реалізації кожного етапу функціональних перетворень за наведеною на рис. 1 блок-схемою з метою вироблення рекомендацій щодо реалізації методу генерації псевдовипадкових чисел підвищеної ентропії для системи клієнт-банк.

На першому етапі шумові сигнали від джерел ентропії, як основні носії зазначеної ентропії, проходять процедуру зчитування показників датчиків, а за потреби – процедуру аналого-цифрового перетворення сигналів з аналогових датчиків (дискретизації) з метою зручності їх подальшої обробки в цифровому вигляді (вхідних векторів-носіїв ентропії). Особливості функції аналого-цифрового перетворення залежать від характеру використовуваного в якості джерела ентропії явища і застосовуваних методів (засобів) перетворення характеристик цього явища в цифрові вектори-описи.

Оскільки на даному етапі джерела ентропії нами ще не ідентифіковано, можна сформулювати лише загальні вимоги щодо реалізації функції аналого-цифрового перетворення F1.

В першу чергу, функція аналого-цифрового перетворення F1 повинна мати достатню чутливість для збереження властивостей ентропії вхідного шумового сигналу у його описах векторами двійкових кодів, тобто, крок дискретизації функції аналого-цифрового перетворення F1 повинен забезпечувати необхідну

точність вимірювання оцінюваного параметра перетворюваного аналогового сигналу в квантовані моменти часу і, як наслідок, точні відображення оцінюваного параметра перетворюваного аналогового сигналу в цифровому представлені.

Операція первинного перетворення аналогового сигналу від джерел ентропії в вектор цифрового коду є традиційною і полягає в дискретизації аналогового значення недетермінованого шумового сигналу з метою отримання його цифрового представлення. Як і для дискретизації будь-якого аналогового сигналу, тут важливим є крок дискретизації і період квантування як передумова одержання якісного відображення властивостей початкового сигналу в його дискретному (цифровому) описі. Саме крок дискретизації визначає точність вимірювання оцінюваного параметра перетворюваного аналогового сигналу в квантовані моменти часу і, як наслідок, точність відображення оцінюваного параметра-носія ентропії перетворюваного аналогового сигналу в цифровому представлені.

Для дискретизації аналогового сигналу від джерела шуму як носія первинної ентропії ГПВЧ важливою є саме шумова зона сигналу з найбільшою ентропією. Це зумовлено тим, що більшість джерел шуму характеризуються неоднорідністю ентропійних характеристик сигналу в різних зонах. Так, наприклад, використовуваний в якості джерела ентропії для ГПВЧ шумовий діод має досить невелику зону вольт-амперної характеристики з непередбачуваною поведінкою сигналу, в той час як на інших ділянках поведінка сигналу в номінальному режимі є абсолютно передбачуваною і непридатною для використання в якості джерела первинної ентропії ГПВЧ.

З іншої сторони, крок дискретизації у відношенні до амплітуди зміни оцінюваного параметра перетворюваного аналогового сигналу безпосередньо визначає вимоги щодо розрядності цифрового вектора опису для однократного виміру. Якщо прийняти амплітуду рівною A, а крок дискретизації рівним Δa, то отримуємо кількість можливих відліків (допустимих оригінальних значень) перетворюваного сигналу:

$$K = \frac{A}{\Delta a}, \tag{3}$$

що визначає вимоги щодо розрядності двійкового коду вектора опису для кожного однократного виміру:

$$R = \log_2 \frac{A}{\Delta a} \tag{4}$$

Враховуючи наявність великої кількості цифрових датчиків, здатних одразу формувати достатньо точні оціночні вектори вимірюваних параметрів, з метою забезпечення максимальної зручності реалізації пропонованого методу в системі клієнт-банк доцільно використовувати джерело ентропії, оснащене цифровими датчиками з потрібними властивостями для вимірювання використовуваних характеристик шумового сигналу як носія ентропії.

За наявності векторів цифрових описів шумового сигналу саме вони стають носіями складової ентропії цього сигналу.

Як зазначалося в попередньому описі функції F2, на етапі реалізації функції аналого-цифрового перетворення F1 не завжди виходить співставити актуальну для ГПВЧ зону найвищої ентропії сигналу з зоною дискретизації, тому отримувані з F1 вектори-носії ентропії, в більшості випадків, складаються з розрядів, що містять різне навантаження за ентропією. Наприклад, якщо джерело ентропії базується на вимірюванні температури зовнішнього середовища, а для системи клієнт-банк, зокрема, таким середовищем можна вважати приміщення з системами клімат-контролю, то марно очікувати якісної ентропії в цілих розрядах показників датчика температури. Через це при реалізації функції F2 потрібно виділити з векторів цифрового коду саме ті розряди, що несуть максимальну складову ентропії.

Особливості функції F2 визначаються на підставі дослідження властивостей сигналу джерела ентропії за результатами, отримуваними після багатократного застосування функції первинного перетворення F1, із широкомасштабним застосуванням методів статистичного аналізу.

На даному етапі зарано говорити про застосуванням методів статистичного аналізу через відсутність статистичних даних для їх дослідження.

Результатом застосування функції F2 є множина векторів з складовою ентропії, отриманих перетвореннями на попередніх етапах сигналів від одного або декількох джерел ентропії. В багатьох випадках отримуваного з функції F2 одиничного вектора недостатньо для реалізації подальших операції, що зумовлює потребу поєднання декількох таких векторів в одному без втрат або з мінімально допустими втратами їх ентропійних властивостей. Для виконання відповідного синтезу єдиного вектора з вхідної множини векторів реалізується функція F3.

Стосовно функції F3 слід зазначити, що вона займає проміжне місце між функціями перетворення двійкових кодів F2 і F4 та є залежною від них, тому має бути узгодженою з ними.

Аналіз дозволяє визначити суть функцій F2–F4:

– F2 виділяє складову ентропії з векторів qj.i ∈ Qдж.j;

– F3 поєднує ентропію декількох векторів qj.i ∈ Qдж.j в одному векторі;

– F4 має передати сумарну ентропію «універсального» вектора на вхід криптографічного алгоритму генерації псевдовипадкових значень в заданій розрядності, тобто, виконати стиснення «універсального» вектора до потрібної розрядності без втрат ентропійних властивостей.

Головне призначення функцій перетворення двійкових кодів F2–F4 – підготувати двійкові дані, що передають характеристики ентропії джерела, до передачі в криптографічний алгоритм генерації псевдовипадкових значень без втрат зазначених властивостей (з мінімізацією втрат).

Стосовно функцій перетворення-поєднання двійкових кодів F3 слід зазначити, що вона може бути реалізована математично або алгоритмічно, але обов'язково з орієнтацією на функцію стиснення F4.

Зазначимо, що в багатьох реалізаціях функції перетворень F3 і F4 можуть поєднуватися між собою і тому не розглядаються окремо. При цьому слід також зазначити можливість поєднання і інших функцій з наведеного в моделі переліку.

Для оптимального вибору типу перетворення двійкових даних за функцією F3 проведемо аналіз вимог щодо функції стиснення F4.

Призначенням функції F4 є стиснення вектора двійкового коду великої розрядності до фіксованого розміру, необхідного для реалізації обраного криптографічного алгоритму генерації псевдовипадкових значень.

Узагальнюючи опис призначення функції F4 можна дати наступне тлумачення – стиснення вектора двійкового коду довільної розрядності до вектора двійкового коду фіксованої розрядності із збереженням ентропійних властивостей початкового значення.

Аналіз останнього опису вказує на однотипність задач функції F4 з задачами створення хеш-функцій.

Хеш-функції – функції, вхідним значенням яких є повідомлення довільної довжини, а вихідним значенням – повідомлення фіксованої довжини) [16, 17]. Хеш-функції володіють рядом властивостей, які дозволяють із високою ймовірністю визначати зміни вхідного повідомлення. Мета хеш-функції – відносно безпечна передача інформації. Прикладом її реалізації є шифрування, при якому повідомлення змінюється таким чином, щоб супротивник не зміг його прочитати, а також доповнення повідомлення контрольним кодом (хеш-кодом), що отримується з повідомлення за певним алгоритмом і призначається для аутентифікації відправника і перевірки цілісності повідомлення.

З подібним призначенням використовують також укорочений цифровий підпис) [17]. Укорочений цифровий підпис може бути отриманий шифруванням певної частини повідомлення обмеженої розмірності (розрядності). Такий фрагмент називається аутентифікатором. Якщо аутентифікатор зашифрований закритим ключем відправника, він є цифровим підписом, за допомогою якого можна перевірити вхідне повідомлення. Недоліком аутентифікаторів, які отримуються шифруванням фрагменту повідомлення, є неможливість перевірки цілісності інших фрагментів передаваного відкритого тексту повідомлення. Більш ефективним визнане застосування аутентифікатора, що є функцією від всього повідомлення, тобто, хеш-функції повідомлення.

Стосовно нашої задачі укорочений цифровий підпис не може розглядатися як ефективний метод стиснення двійкового вектора як носія ентропійних властивостей джерела ентропії, оскільки повторне урізання вектора-носія після функції F2 майже гарантовано призведе до втрат властивостей ентропії цього вектора.

Хеш-функція класифікується як стиснене відображення повідомлення з майже однозначною відповідністю функції до коду повідомлення. Тобто, хеш-функції властиве наслідування властивостей оригінального коду, що є визначальним в нашій задачі.

На користь хеш-функцій як способу реалізації функції стиснення векторів-носіїв характеристик ентропії джерел F4 свідчать і крипторгафічні методи створення цих функцій, що є притаманним задачам системи клієнт-банк.

До переваг криптографічних хеш-функцій слід віднести і те, що хеш-функція здатна протистояти атакам із використанням криптоаналізу.

Це досягається за рахунок наступних властивостей:

– хеш-функція є односторонньою (незворотною). Тобто, майже для всіх варіантів вихідного коду функції неможливо алгоритмічно або обчислювально відновити початковий варіант коду повідомлення;

– стійкість до колізій першого роду. Для заданого повідомлення обчислювально неможливо підібрати інше повідомлення з аналогічною хеш-функцією;

– стійкість до колізій другого роду. Обчислювально неможливо підібрати пару повідомлень, що мають однакову хеш-функцію.

Наведені аргументи свідчать на користь використання в якості функції стиснення векторів-носіїв ентропійних характеристик джерел ентропії F4 саме криптографічних хеш-функцій.

Повертаючись до аналізу функції F3, орієнтованої на об'єднання декількох векторів з складовою ентропії в єдиний вектор, слід зазначити, що реалізація функції стиснення векторів-носіїв ентропійних характеристик джерел ентропії F4 як криптографічної хеш-функції усуває потребу операцій стиснення при

виконанні функції F3. Навпаки, для збереження максимуму ентропійних властивостей вхідних у функцію векторів доцільно зберегти їх у початковому стані і передати на вхід хеш-функції F4. Тобто, оптимальним варіантом функції F3 можна визнати символьну операцію поєднання двійкових кодів векторів-носіїв ентропії в єдиний вектор беж жодних математичних перетворень, що дасть нам результуючий вектор з розрядністю, рівною сумарній розрядності вхідних до функції F3 початкових векторів. Задача ж стиснення вектора двійкового коду великої розрядності з виходу функції F3 до фіксованого розміру, необхідного для реалізації обраного криптографічного алгоритму генерації псевдовипадкових значень, повністю підпадає під функцію F4.

Результатом реалізації функції F4 є вектор з розрядністю, визначеною потребами обраного криптографічного алгоритму генерації псевдовипадкових значень.

Криптографічний алгоритм генерації псевдовипадкових значень реалізує завершальні операції в досліджуваній моделі, позначені як функція криптографічного методу генерації псевдовипадкових чисел F5, що забезпечує очікуваний результат роботи ГПВЧ.

Таким чином, в запропонованій моделі описано і досліджено всі етапи функціонування ГПВЧ підвищеної ентропії для системи клієнт банк. Результати проведених досліджень свідчать про відповідність властивостей моделі наявним потребам, тобто, про її адекватність модельованим процесам.

Висновки. За результатами дослідження загальних принципів застосування джерел ентропії в роботі генераторів псевдовипадкових чисел запропоновано математичну модель джерела ентропії, адаптовану для вирішення завдань генерації криптоключів системи клієнт-банк, а також створено узагальнену модель процесу генерації псевдовипадкових двійкових векторів підвищеної ентропії. Проведене дослідження властивостей запропонованої моделі дозволило підтвердити її адекватність процесу генерації псевдовипадкових двійкових векторів підвищеної ентропії. В роботі також надані рекомендації щодо застосування запропонованої моделі в практичних реалізаціях генераторів псевдовипадкових двійкових векторів підвищеної ентропії для синтезу криптоключів системи клієнт-банк, що були використані для апробації моделей генераторів у [18]. Отримані результати є основою для реалізації методу та засобів генерації псевдовипадкових чисел в системі клієнт-банк і удосконалення алгоритмів функціонування зазначеної системи.

Література

1. Геселева Н.В. Інформаційна система підтримки електронних платежів через Інтернет / Н.В. Геселева, Г.В. Пронюк, В.В. Добровольський// Економіка і суспільство, 2018. – Випуск №14. – С. 1005–1010.

2. Умови надання банківських послуг з використанням систем дистанційного обслуговування [Електронний ресурс]. – Режим доступу: https://www.bisbank.com.ua/wp-content/uploads/2020/08/dodatok-7-umovy_system_dist_obslugov_z–11.05.2019-do-05.07.2019.pdf

3. Система «iBank 2» для корпоративних клієнтів. [Електронний ресурс]. – Режим доступу: https://ibank.otpbank.ru/Corporate_Internet–Banking_Guide.pdf.

4. Безпека Інтернет–банкінгу в Україні: практичні аспекти [Електронний ресурс]. – Режим доступу: https://bankchart.com.ua/e_banking/statti/bezpeka_internet_bankingu_v_ukrayini_praktichni_aspekti.

5. Гребенюк Н. О. Фінансова безпека банків: система розпізнання загроз та усунення ризиків / Н. О. Гребенюк // Вісник Харківського національного університету імені В. Н. Каразіна. Серія : Економічна. – 2016. – Вип. 91. – С. 53–64.

6. Горицький В.М. Генерація випадкових послідовностей для систем управління ключами / В.М. Горицький, О.В. Снєжок, М.С. Височіненко // Сучасний захист інформації, 2012. – №4. – С. 88–95.

7. Гріненко Т. О. Квантові генератори випадкових чисел в криптографії / Т. О. Гріненко, О. П. Нарєжній // Системи обробки інформації. – 2015. – Вип. 10. – С. 86–89.

8. Heat transfer and entropy generation in a microchannel with longitudinal vortex generators using nanofluids / Amin Ebrahimia, Farhad Rikhtegarb, Amin Sabaghana, Ehsan Roohia Energy // Energy. – Volume 101, 15 April 2016. – P. 190–201.

9. Круліковський О. В. Особливості вибору хаотичних систем для побудови генераторів псевдовипадкових послідовностей / О. В. Круліковський, С. Д. Галюк, Л. Ф. Політанський // Телекомунікаційні та інформаційні технології. – 2017. – № 2. – С. 31–40.

10. Слеповичев И.И. Генераторы псевдослучайных чисел / И.И. Слеповичев. – Саратов: издательство СГУ, 2017. – 118 с.

11. Реверсивний генератор кодових послідовностей на FPGA / Д. Гаврілов, А. Воловик, О. Звягін, Д. Яровий // Вісник Вінницького політехнічного інституту. – 2019. – № 4. – С. 100–106.

12. Фауре Е. В. Синтез і аналіз псевдовипадкових послідовностей на основі операцій криптографічного перетворення / Е. В. Фауре, С. В. Сисоєнко, Т. В. Миронюк // Системи управління, навігації та зв'язку. – 2015. – Вип. 4. – С. 85–87.

13. Стасєв Ю. В. Метод формування псевдовипадкових послідовностей з поліпшеними автокореляційними властивостями / Ю. В. Стасєв, Д. О. Медведєв, Д. О. Грабенко, Д. В. Жуйков // Збірник наукових праць Харківського університету Повітряних Сил. – 2017. – № 4. – С. 115–118.

14. Sun Y. Random number generation using inertial measurement unit signals for on–body IoT devices / Y. Sun and B. Lo // in Proc. Living Internet Things, Cybersecur. IoT. – 2018. – P. 1–9.

15. Toward sensorbased random number generation for mobile and IoT devices / K. Wallace, K. Moran, E. Novak, G. Zhou, K. Sun // IEEE Internet Things J. – Dec. 2016. – Vol. 3, № 6. – P. 1189–1201.

16. Демський О.О. Метод реалізації генератора випадкових чисел / О.О. Демський, В.О. Бойчук // «Інтелектуальний потенціал – 2018» - збірник наукових праць молодих науковців і студентів з нагоди 30-річчя підготовки ІТ- фахівців в ХНУ. – Хмельницький: ПВНЗ УЕП, 2018. – Ч.3: Кібербезпека та актуальні проблеми комп'ютерних систем і мереж. – С. 40–44.

17. Lane Wagner, How SHA-2 Works Step-By-Step (SHA-256) / Published July 8, 2020. [Електронний ресурс]. – Режим доступу: https://qvault.io/2020/07/08/how-sha-2-works-step-by-step-sha-256.

18. Чешун В. М. Оцінка ефективності роботи генератора криптоключів підвищеної ентропії для системи клієнт–банк / В. М. Чешун, В. І. Чорненький, В. В. Яцків // Збірник наукових праць молодих науковців і студентів «Інтелектуальний потенціал – 2020». – Хмельницький: ПВНЗ УЕП, 2020. – Частина 2. – С. 84–93.

References

1. Gheseleva N.V. Informacijna systema pidtrymky elektronnykh platezhiv cherez Internet / N.V. Gheseleva, Gh.V. Pronjuk, V.V. Dobrovoljsjkyj// Ekonomika i suspiljstvo, 2018. – Vypusk #14. – S. 1005–1010.

2. Umovy nadannja bankivsjkykh poslugh z vykorystannjam system dystancijnogho obslughovuvannja [Elektronnyj resurs]. – URL: https://www.bisbank.com.ua/wp-content/uploads/2020/08/dodatok-7-umovy_system_dist_obslugov_z–11.05.2019-do-05.07.2019.pdf

3. Systema «iBank 2» dlja korporatyvnykh klijentiv. [Elektronnyj resurs]. – URL: https://ibank.otpbank.ru/Corporate_Internet–Banking_Guide.pdf.

4. Bezpeka Internet–bankinghu v Ukrajini: praktychni aspekty [Elektronnyj resurs]. – URL: https://bankchart.com.ua/e_banking/statti/bezpeka_internet_bankingu_v_ukrayini_praktichni_aspekti.

5. Ghrebenjuk N. O. Finansova bezpeka bankiv: systema rozpiznannja zaghroz ta usunennja ryzykiv / N. O. Ghrebenjuk // Visnyk Kharkivsjkogho nacionaljnogho universytetu imeni V. N. Karazina. Serija : Ekonomichna. – 2016. – Vyp. 91. – S. 53–64.

6. Ghorycjkyj V.M. Gheneracija vypadkovykh poslidovnostej dlja system upravlinnja kljuchamy / V.M. Ghorycjkyj, O.V. Snjezhok, M.S. Vysochinenko // Suchasnyj zakhyst informaciji, 2012. – #4. – S. 88–95.

7. Ghrinenko T. O. Kvantovi gheneratory vypadkovykh chysel v kryptoghrafiji / T. O. Ghrinenko, O. P. Narjezhnij // Systemy obrobky informaciji. – 2015. ¬– Vyp. 10. – S. 86–89.

8. Heat transfer and entropy generation in a microchannel with longitudinal vortex generators using nanofluids / Amin Ebrahimia, Farhad Rikhtegarb, Amin Sabaghana, Ehsan Roohia Energy // Energy. – Volume 101, 15 April 2016. – P. 190–201.

9. Krulikovsjkyj O. V. Osoblyvosti vyboru khaotychnykh system dlja pobudovy gheneratoriv psevdovypadkovykh poslidovnostej / O. V. Krulikovsjkyj, S. D. Ghaljuk, L. F. Politansjkyj // Telekomunikacijni ta informacijni tekhnologhiji. – 2017. – # 2. – S. 31–40.

10. Slepovichev I.I. Generatoryi psevdosluchaynyih chisel / I.I. Slepovichev. – Saratov: izdatelstvo SGU, 2017. – 118 s.

11. Reversyvnyj ghenerator kodovykh poslidovnostej na FPGA / D. Ghavrilov, A. Volovyk, O. Zvjaghin, D. Jarovyj // Visnyk Vinnycjkogho politekhnichnogho instytutu. – 2019. – # 4. – S. 100–106.

12. Faure E. V. Syntez i analiz psevdovypadkovykh poslidovnostej na osnovi operacij kryptoghrafichnogho peretvorennja / E. V. Faure, S. V. Sysojenko, T. V. Myronjuk // Systemy upravlinnja, navighaciji ta zv'jazku. – 2015. – Vyp. 4. – S. 85–87.

13. Stasjev Ju. V. Metod formuvannja psevdovypadkovykh poslidovnostej z polipshenymy avtokoreljacijnymy vlastyvostjamy / Ju. V. Stasjev, D. O. Medvedjev, D. O. Ghrabenko, D. V. Zhujkov // Zbirnyk naukovykh pracj Kharkivsjkogho universytetu Povitrjanykh Syl. – 2017. – # 4. – S. 115–118.

14. Sun Y. Random number generation using inertial measurement unit signals for on–body IoT devices / Y. Sun and B. Lo // in Proc. Living Internet Things, Cybersecur. IoT. – 2018. – P. 1–9.

15. Toward sensorbased random number generation for mobile and IoT devices / K. Wallace, K. Moran, E. Novak, G. Zhou, K. Sun // IEEE Internet Things J. – Dec. 2016. – Vol. 3, # 6. – P. 1189–1201.

16. Demskyi O.O. Metod realizatsii heneratora vypadkovykh chysel / O.O. Demskyi, V.O. Boichuk // «Intelektualnyi potentsial – 2018» - zbirnyk naukovykh prats molodykh naukovtsiv i studentiv z nahody 30-richchia pidhotovky IT- fakhivtsiv v KhNU. – Khmelnytskyi: PVNZ UEP, 2018. – Ch.3: Kiberbezpeka ta aktualni problemy kompiuternykh system i merezh. – S. 40–44 .

17. Lane Wagner, How SHA-2 Works Step-By-Step (SHA-256) / Published July 8, 2020. [Elektronnyj resurs]. – URL: https://qvault.io/2020/07/08/how-sha-2-works-step-by-step-sha-256.

18. Cheshun V. M. Ocinka efektyvnosti roboty gheneratora kryptokljuchiv pidvyshhenoji entropiji dlja systemy klijent–bank / V. M. Cheshun, V. I. Chornenjkyj, V. V. Jackiv // Zbirnyk naukovykh pracj molodykh naukovciv i studentiv «Intelektualjnyj potencial – 2020». – Khmeljnycjkyj: PVNZ UEP, 2020. – Chastyna 2. – S. 84–93.

Надійшла / Paper received: 16.10.2020 Надрукована / Paper Printed : 01.12.2020

За зміст повідомлень редакція відповідальності не несе

Підп. до друку 26.11.2020. Ум. друк. арк. – 10,12. Обл.-вид. арк. – 9,68.
Формат 30×42/4, папір офсетний. Друк різографією.
Наклад 100, зам. № 212/20

Тиражування здійснено з оригінал-макета редакційно-видавничим відділом
Хмельницького національного університету.
29016, м. Хмельницький, вул. Інститутська, 7/1, тел. (0382) 77-33-63.
Свідоцтво про внесення в Державний реєстр, серія ДК № 4489 від 18.02.2013 р.