crucial for ensuring system security and efficiency. Third-party inclusions can be various software modules, applications, or libraries that are compatible with the system but were not specifically developed for it. Incorporating such components can provide rapid and efficient system expansion, but they can also pose certain threats to system security and reliability. One possible risk of third-party inclusions is security vulnerabilities that can be exploited by attackers to target the system. Third-party inclusions may contain malicious code, such as viruses or spyware, that can modify the cluster's operation, harm the system, and its users.

In general, the localization and control of third-party inclusions are important steps in ensuring security in a communication cluster, as unauthorized use of such inclusions can lead to data confidentiality breaches, increased risk of cyber attacks, and other serious threats. Redundant hashing is an effective method to secure information exchange in robotic system clusters. By detecting potential third-party inclusions and data modifications, it ensures integrity and reliability of information exchange as the foundation for the system's sustainable functioning.

References

1. Pereira, T., Barreto, L., & Amaral, A. (2017). Network and information security challenges within Industry 4.0 paradigm. Procedia manufacturing, 13, 1253-1260.

2. Breiling, B., Dieber, B., & Schartner, P. (2017, April). Secure communication for the robot operating system. In 2017 annual IEEE international systems conference (SysCon) (pp. 1-6). IEEE.

3. Yarmilko, A., Rozlomii, I., & Kosenyuk, H. (2022, February). Hash Method for Information Stream's Safety in Dynamic Cooperative Production System. In Mathematical Modeling and Simulation of Systems: Selected Papers of 16th International Scientific-practical Conference, MODS, 2021 June 28–July 01, Chernihiv, Ukraine (pp. 173-183). Cham: Springer International Publishing.

UDC. 004

Svitlana Tsiutsiura, DSc (Eng.), Professor
Andrii Yerukaiev, PhD (Eng.), Associate Professor
Kyiv National University of Construction and Architecture, svtsutsura@gmail.com

PROTECTION OF INFORMATION IN ASSESSING THE FACTORS OF INFLUENCE

In today's intense problem of quality education, the recipient of educational services is faced with the problem of choosing among the available higher education institutions, which, when investing the most valuable human resources in the educational proces, will bring the greatest results from full, completed and quality education. But each of the considered HEI falls under the various factors of influence: social, administrative, economic, political, environmental, etc. These factors at least 10% measurable by standard methods, and all others are qualitative.

As mentioned above, the model considered by the authors in this article is the result of the most popular methods of strategic analysis and artificial intelligence combination. The general view of this model is presented on Fig. 1.

Videlicet soft computing as a section of artificial intelligence because of its simplicity and approach to the human thinking reflection was chosen to build a fuzzy model for HEI assessment.

The membership functions of fuzzy sets, which describe the SWOT categories, do not have a standard form, as they were used to build the opinions of experts in the HEI assessment to give the task more practicality. Relevant calculations were performed by such authors using the formula:

$$\mu_{l_j}(u_i) = \frac{1}{K} \sum_{k=\overline{1,K}} b_{j,i}^k,\ i = \overline{1,n}, \qquad (1)$$

where K – number of experts;

$b_{j,i}^k$ – thought of the k - expert about the presence in the element u_i of the properties of a fuzzy set $\tilde{l}_j$, $k = \overline{1,K}$, $i = \overline{1,n}$, $j = \overline{1,m}$;

$\tilde{l}_j = \left(\frac{\mu_{l_j}(u_1)}{u_1}, \frac{\mu_{l_j}(u_2)}{u_2}, \cdots, \frac{\mu_{l_j}(u_n)}{u_n} \right)$ – fuzzy set that describes a linguistic term l_j, $j = \overline{1,m}$ on the universal set *U*.

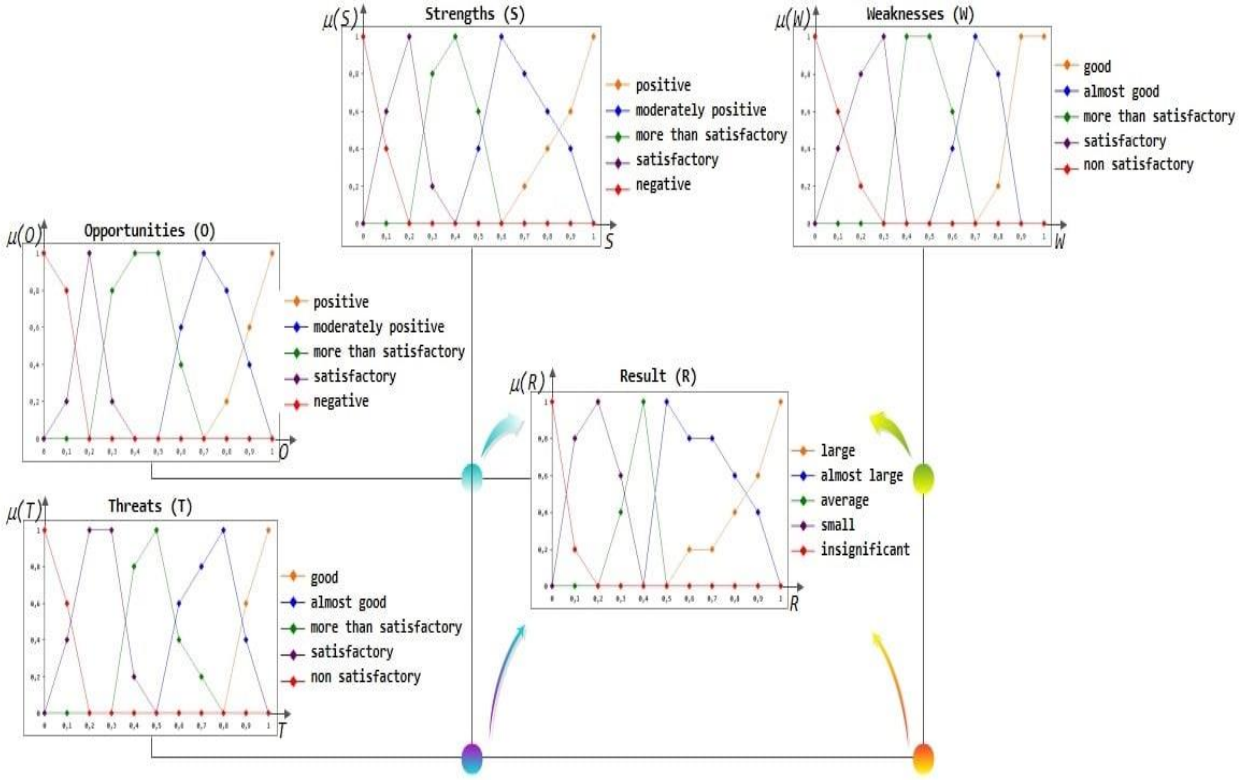

Fig. 1 – Protection of information in fuzzy model

Since there are many groups of influencing factors and in the process of research new ones will inevitably appear and old ones will be removed, it is necessary to group them in such a way that it is possible to work with them conveniently. For this purpose, a SWOT-analysis was chosen, due to which, regardless of the number of studied groups of factors, the work will be carried out with only four categories: strength (S), weakness (W), opportunity (O) and threat (T).

Each of the four SWOT categories is described as fuzzy sets according to the template. There are the following terms, in an amount equal to five [12, 17], which have the following common names:

- minimal (for S: negative, for W: non satisfactory, for O: negative, for T: non satisfactory and for R: insignificant);
- average minimum (for S: satisfactory, for W: satisfactory, for O: satisfactory, for T: satisfactory and for R: small);
- average (for S: more than satisfactory, for W: more than satisfactory, for O: more than satisfactory, for T: more than satisfactory and for R: average);
- average maximum (for S: moderately positive, for W: almost good, for O: moderately positive, for T: almost good and for R: almost large);
- maximum (for S: positive, for W: good, for O: positive, for T: good and for R: large)

Models in protection of information that include artificial intelligence technologies in combination with classical decision-making methods can be used not only in the HEI selection, but mainly in the areas of business management and planning in general. This greatly helps managers to increase investment flows and increase the likelihood of making an informed decision in the face of business uncertainty and variability.

The use of fuzzy SWOT-analysis to protect information allows you to choose among the many objects essential one, when the large influence of factors is no longer a problem in management decisions. Methods that reflect human thinking in solving these problems, their ease of understanding and implementation, which at the same time is based on the strict laws of mathematical logic, are widely used in business and management.

References

1. Tsiutsiura M.I. The structure of information flows in the information system of production HEI [Text] / M.I. Tsiutsiura, O.V. Kryvoruchko, T.M. Medinskaya // Management of complex systems development. - 2019. - Issue 37 - № 37. - P. 205 - 209.

2. Tsiutsiura, S.V. Formation of a generalized information model of a construction object / Tsiutsiura, S.V., Kyivska, K.I., Tsiutsiura, M.I., Kryvoruchko, O.V., Dmytrychenko, A.M. // International Journal of Mechanical Engineering and Technology. – 2019. – Volume 10, Issue 2. – Pages 69-79

3. Kyivska, K.I. A study of the concept of parametric modeling of construction objects / Kyivska, K.I., Tsiutsiura, S.V., Tsiutsiura, M.I., Kryvoruchko, O.V., Yerukaiev, A.V., Hots, V.V. // International Journal of Advanced Research in Engineering and Technology. – 2019. – Volume 10, Issue 2, 2019. – Pages 636-646/

4. Tsiutsiura M.I. A fuzzy model for assessing the impact of factors on free urban plots / Tsiutsiura M.I., Yerukaiev, A.V // Science and Education a New Dimension. Natural and Technical Sciences – 2018. – Volume VI(17), Issue 157. – Pages 636-646.

УДК 621.941-229.3:531.133

Морозова І.В., канд. техн. наук, доцент
Корчан В.М., аспірант
Національний авіаційний університет, м. Київ, korchan.vlad22@gmail.com

МАТЕМАТИЧНА МОДЕЛЬ СИСТЕМИ РЕЗОЛЮЦІЇ

Система резолюції складається з двох типів реєстрів GHR і LHR. Нехай група реєстрів GHR визначається символом *Gj*, де *j* = 1, 2, 3…*N*, де *N* – загальне число реєстрів GHR в системі. Кожен реєстр GHR об'єднує і контролює визначений набір локальних реєстрів. Набір локальних реєстрів, під'єднаних до *j*-го GHR, позначається символом *Lji*, де i = 1, 2, 3...*Mj*, де *Mj* – загальна кількість LHR, приєднаних до *j-го* GHR. Передані пакети потрапляють на сервер з визначеною частотою, відповідною Пуассонівському процесу, формуючи одиночну чергу на контролері. Така система може бути змодельована на основі багатоканальної моделі масового обслуговування (M/M/s).

Тоді середній час відповіді *Tj* реестру GHR *Gj* рівний сумі часу в черзі і часу обробки, і може бути прораховано за допомогою формули Ерланга, як функція частоти надходження *λi* запитів и частоти обслуговування μ:

$$T_j(\lambda) = \frac{f(s,\frac{\lambda_j}{\mu})}{s\mu_j - \lambda_j} + \frac{1}{\mu}. \quad (1)$$

Функція f (s, λ/μ) визначає вірогідність того, що всі сервери в системі використовуються, і любий з отриманих запитів потрапляє у чергу:

$$f\left(s,\frac{\lambda}{\mu}\right) = \frac{1}{1+\left(\frac{1}{1-\gamma}\right)\left(\frac{s!}{(s\gamma)^s}\right)\Sigma_{k=0}^{s-1}\frac{(s\gamma)^k}{k!}}, \quad (2)$$

$$\gamma = \frac{\lambda_j}{s.\mu}. \quad (3)$$

Функція γ показує використання системи, що відображує також її стабільність.

Система стабільно розподілена тільки якщо показник використання системи γ менше одиниці. Дана інформація може бути коректно інтерпретована за допомогою діаграми