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

станів багатоканальної моделі M/M/s. У випадку, коли число заявок в черзі більше, ніж на сервері контролера, обробка буде відбуватися з тією ж частотою μ, при цьому контролер буде гранично заповнений (рис.1).

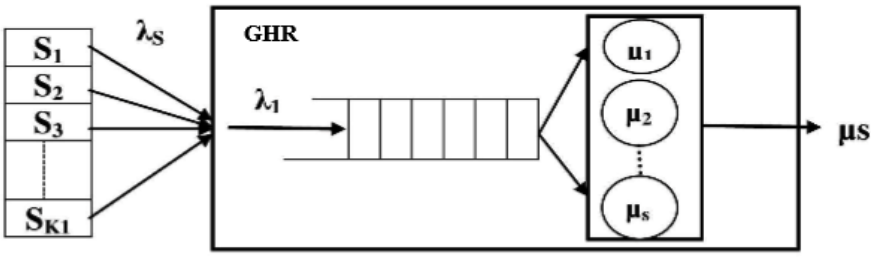

Рис. 1 – Представлення процесу дозволу ідентифікаторів на сервері GHR у вигляді об'єктів ЗМО

Частота отримання заявок λ_j реєстру GHR Gj розраховується як сума середніх частот отримання заявок на локальних реєстрах (L_i^j), приєднаних до реєстру G_j :

$$\lambda_j = \sum_{Li} \lambda_l. \quad (4)$$

Середнє навантаження на сервер-посередник G_j розраховується як середнє число отриманих і оброблених запитів. За допомогою формули Ерланга розраховується середнє навантаження L_j на реєстрах GHR:

$$L_j(\lambda) = s\gamma + \frac{\gamma}{1-\gamma} f\left(s, \frac{\lambda_j}{\mu}\right). \quad (5)$$

Таким чином, на основі отриманої формули Ерланга можна провести чисельний розрахунок середнього навантаження Lj на реєстрах GHR.

Список посилань

1. Recommendation ITU-T Y.2060 SERIES Y: Provides an overview of the Internet of things (IoT) (06/2012). 2. Internet of Things World Forum, IWF (https://www.iotwf.com/)
2. Інтернет ресурс: https://azure.microsoft.com/ru-ru/solutions/iot/iot-technology-protocols/.
3. Інтернет ресурс: https://habr.com/ru/post/299910/.

УДК 004.056

Розломій І.О., канд. техн. наук, ст. викладач
Воєводін Є.В., аспірант
Черкаський національний університет імені Богдана Хмельницького, inna-roz@ukr.net

ПРОБЛЕМА РЕТРОСПЕКТИВНОГО ДЕКОДУВАННЯ ДАНИХ: ОГЛЯД МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ НА БАЗІ КВАНТОВИХ ТЕХНОЛОГІЙ

Сучасні системи захисту інформації побудовані з використанням алгоритмів симетричного та асиметричного шифрування, таких як RSA чи то AES. Скажімо, TLS протокол, який використовується для безпечного обміну даних в мережі інтернет і не тільки, використовує асиметричне кодування для обміну секретним ключем, що дає змогу використати секретний ключ для подальшого симетричного кодування безпосередніх даних. Тобто має місце комбінація асиметричного та симетричного шифрування, що дозволяє досягти ефективного та безпечного обміну даними.

Перспектива розвитку науки та інформаційних технологій ставить під ризик надійність сучасних методів шифрування, так, маючи достатньо потужний квантовий комп'ютер, можна вирішити задачу факторизації та декодувати закодовані дані, використовуючи алгоритм Шора [1]. Це ставить під загрозу не тільки шифрування даних в майбутньому, але