Fuzzy logic system as a component of the web application security information system*

Mikolaj Karpinski[1,2,†], Oleksandr Revniuk[1,†], Dmytro Tymoshchuk[1,*,†], Ruslan Kozak[1,†] and Aizhan Tokkuliyeva[3,†]

[1] Ternopil Ivan Puluj National Technical University, 56, Ruska str., 46001 Ternopil, Ukraine
[2] University of the National Education Commission, 2 Podchorążych str, 30084 Krakow, Poland
[3] L.N. Gumilyov Eurasian National University, 2 Satpayev str, 010008 Astana, Kazakhstan

Abstract

An approach to enhance the objectivity of expert evaluation of web application security using fuzzy set theory and fuzzy logic methods is presented in this paper. The proposed methodology is intended to reduce the subjectivity and uncertainty that arise when determining the weight coefficients, which reflect the importance of security criteria and requirements. The system of weight coefficients is a part of an adaptive methodology developed based on the OWASP ASVS standard for the quantitative assessment of web application security, implemented in the information system. Within the fuzzy logic system, as a component of the information system, a three-stage mechanism for aligning expert assessments has been implemented. It includes fuzzification, aggregation of fuzzy sets, and defuzzification using the center of gravity method. The results demonstrate that the proposed approach enables the generation of balanced numerical assessments that reflect the collective opinion of experts. Such a system ensures increased reliability in the analysis of web application security levels and can be integrated into cybersecurity auditing and decision-making processes.

Keywords

Web applications, security, information system, weight coefficients, OWASP ASVS, expert assessment, fuzzy sets, fuzzy logic system

1. Introduction

Web applications have become an integral part of people's digital lives, processing billions of requests daily and storing vast amounts of confidential information: from personal user data to critical business processes data. However, as the functionality and complexity of these applications expand, so does the attack surface that malicious actors can exploit for unauthorized access, data theft, or service disruption. Cyber threats evolve every day, and successful attacks can cause millions of dollars in damage and irreparable harm to an organization's reputation. Therefore, ensuring web application security is not just a technical necessity, but a critically important element of digital strategy that determines user trust, business stability, and compliance with regulatory requirements in the cybersecurity domain.

There are few approaches to assess the security of web application, but the authors of [1, 2] substantiated the relevance of quantitative metrics for assessing web application security, and suggested an adaptive methodology for quantitative security assessment of web applications based on OWASP ASVS standard requirements. The assessment is conducted across 13 sections and a set of 133 selected requirements. The proposed methodology takes into account the variability of architecture, functionality, and specific features of different web applications, particularly in the context of security requirements, through adaptive requirement selection for each case.

Different web applications have different architectures and functionalities, which determine their security protection needs. For example, web applications that do not use API interfaces should

* CSDP'2025: Cyber Security and Data Protection, July 31, 2025, Lviv, Ukraine
* Corresponding author.
† These authors contributed equally.
mikolaj.karpinski@uken.krakow.pl (M. Karpinski); revo0708@gmail.com (O. Revniuk); dmytro.tymoshchuk@gmail.com (D. Tymoshchuk); ruslan.o.kozak@gmail.com (R. Kozak); tokkuliyeva_ak_1@enu.kz (A. Tokkuliyeva)
0000-0002-8846-332X (M. Karpinski); 0009-0005-0511-5354 (O. Revniuk); 0000-0003-0246-2236 (D. Tymoshchuk); 0000-0003-1323-0801 (R. Kozak); 0000-0002-5019-2413 (A. Tokkuliyeva)

not receive reduced scores for lack of API requirement implementation, as these requirements are irrelevant to them. There may be no authentication system for informational websites, making requirements for its assessment unnecessary. To formalize the evaluation of each requirement, a system of criteria sets was developed that ensures obtaining quantitative metrics of compliance level for each requirement. However, criteria, like requirements, may have different weights for each individual web application. For instance, the requirement "Verify that the password change function requires the user's current and new password" contains the criterion "Is there a mechanism to verify new passwords for compliance with security requirements?" which in most cases will have higher priority than the criterion "Is regular auditing conducted to verify the password change process?" Comparative analysis of criteria of different nature in the context of web security presents particular methodological complexity. It was proposed to introduce a system of weight coefficients to take into account the significance of each requirement within a section and criterion within a requirement. Weight coefficients have a direct impact on the resulting assessment of the product's security level, so proper establishment of numerical values for weight coefficients allows identification of strategically critical security parameters that require priority resource allocation and attention. In turn, incorrect quantitative interpretation of weights can lead to formation of wrong web application protection strategies.

Therefore, the process of quantitatively determining the importance of criteria is one of the fundamental stages of multi-criteria analysis in web application security systems. Analysis of scientific papers [3, 4] indicates the existence of a complex of problems in the field of quantitative expert evaluation in general. Research [5] demonstrates the inherent subjectivity of the evaluation process, where each expert forms judgments based on individual professional experience, which causes significant variability in numerical assessments. One of the approaches to eliminate subjectivity in expert evaluation is the use of multiple experts' opinions [6]. An additional challenge is the complexity of precise numerical evaluation, when experts demonstrate instability in choosing between adjacent values [7]. To eliminate expert uncertainty, studies often apply the theory of fuzzy sets and fuzzy logic [8, 9]. Recent advances in minimizing hardware complexity for cryptographic components, such as the bitsliced representation of S-Boxes using ternary logic instructions, contribute to enhancing the security and efficiency of web applications [10]. Furthermore, the investigation of vulnerabilities related to broken authentication in web applications highlights the critical need for comprehensive security assessment frameworks capable of addressing diverse threat vectors [11]. These studies underscore the importance of robust and adaptive security evaluation methods, such as fuzzy logic systems, to improve the reliability of web application security assessments.

The goal of our paper is to design a fuzzy logic system as part of an information system for the quantitative security assessment of web applications, in order to overcome the uncertainty of expert evaluations of the weight coefficients of the importance of criteria and requirements, and to enhance the validity and reliability of the assessment results.

2. Design of fuzzy logic system

For evaluating all values of all weight coefficients that will be used in the developed information system by default, three experts were involved. Expert selection was carried out according to the following criteria:

- Professional competence in the field of web security.
- Practical experience in the field of at least 5 years.
- Absence of conflict of interest regarding the evaluated criteria and requirements.

To implement the developed methodology, an information system was built for assessing web application security [12]. The system supports modular architecture, personalized project management, and result visualization, enabling its use for information security audits [12–15]. One

of the key components of the developed system is the fuzzy logic subsystem, which is designed for processing and harmonizing expert assessments of weight coefficients for the importance of web application security criteria and requirements. Figure 1 presents the structural diagram of the proposed system for expert evaluation of weight coefficients for criteria and requirements.

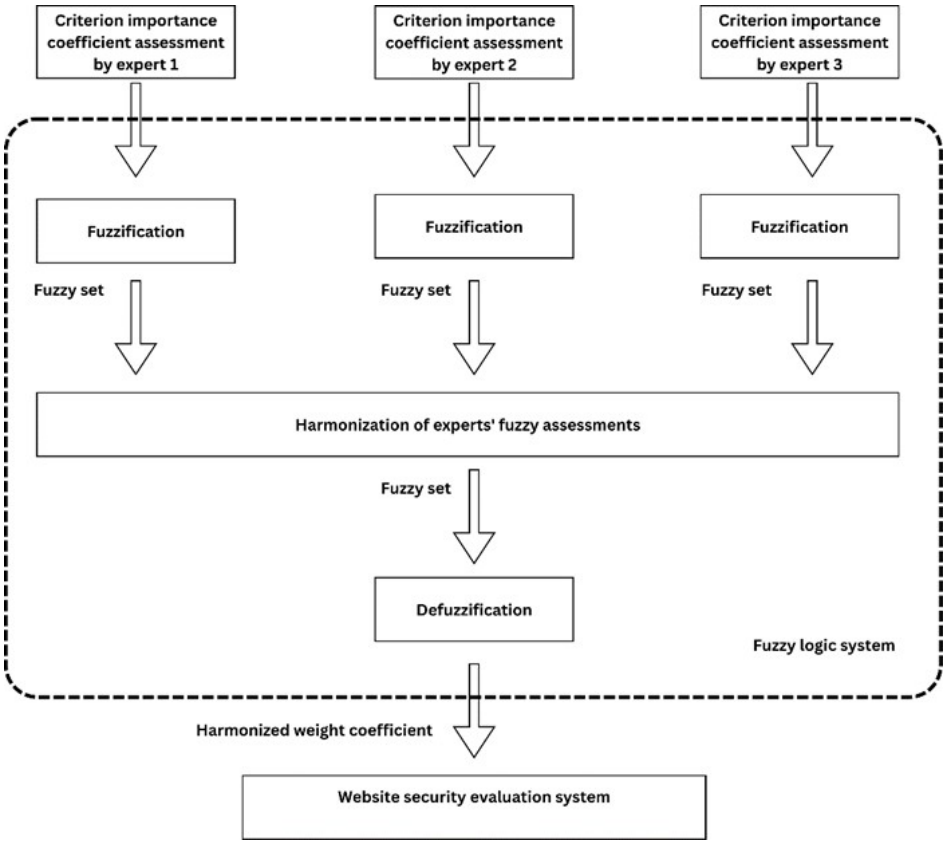

Figure 1: Fuzzy logic system structure

Fuzzification is the first and key step in most fuzzy logic systems. Replacing precise numerical assessments with fuzzy sets allows to model uncertainty, what helps to create more flexible systems.

Each expert conducted independent evaluation of the importance of criteria and requirements without the possibility of consulting with other members of the expert group, which ensured objectivity and reliability of the obtained results. Based on the results of expert evaluation, importance assessments of criteria and requirements were obtained on a 11-point scale from 0 to 10, where 0—absent functionality or absolutely unimportant criterion, 10—maximum importance of the criterion. Experts often hesitate between several adjacent assessments and eventually choose one of them. To account for expert uncertainty for intermediate scores from 1 to 9, we apply a triangular membership function to convert the quantitative assessment of expert criterion weight coefficients into fuzzy set:

$$\mu(x)=\begin{cases} 1, x=w \\ \frac{x-w+2}{2}, w-2<x<w \\ \frac{w+2-x}{2}, w<x<w+2 \\ 0, otherwise \end{cases}, x=\overline{1,9} \quad (1)$$

This membership function does not account for extreme assessment values, therefore in cases where an expert chose a weight coefficient value of 0, which implied the absence of certain

functionality and non-applicability of the requirement, the fuzzy set transformed into a classical set with a single coefficient of 0:

$$W=\{(0,1),(1,0),\dots,(w,0),\dots,(10,0)\}=\{0\} \quad (2)$$

If an expert assigns the maximum weight coefficient value of 10, the membership function is proposed to be determined using the corresponding formula:

$$W=\left\{(0,0),(1,0),\dots,(w,0),\dots,\left(9,\frac{1}{2}\right),(10,1)\right\} \quad (3)$$

Let us assume that after the first step, we have three fuzzy sets of expert assessments:

$$\widetilde{A}=\left\{x,\mu_{\widetilde{A}}(x)\right\},x\in X,X=\{x,0\le x\le 10,x\epsilon Z\},\mu_{\widetilde{A}}(x):X\longrightarrow[0,1]$$
$$\widetilde{B}=\left\{x,\mu_{\widetilde{B}}(x)\right\},x\in X,X=\{x,0\le x\le 10,x\epsilon Z\},\mu_{\widetilde{B}}(x):X\longrightarrow[0,1]$$
$$\widetilde{C}=\left\{x,\mu_{\widetilde{C}}(x)\right\},x\in X,X=\{x,0\le x\le 10,x\epsilon Z\},\mu_{\widetilde{C}}(x):X\longrightarrow[0,1]$$

When different experts assess the same coefficients, there is a need for special methods to aggregate and harmonize these judgments. In case if experts opinions scores were transformed into fuzzy sets, some specific methods are needed to obtain a single, consolidated assessment that reflects the collective opinion of the expert group.

The arithmetic mean method was chosen for harmonizing expert opinions. This method represents a compromise solution, as it provides a balance between conservative (intersection operation) and optimistic (union operation) approaches. By calculating the mean values of the membership function according to formula (4), we obtain a harmonized fuzzy set of expert assessments:

$$\mu_{\widetilde{A},\widetilde{B},\widetilde{C}}(x)=\frac{\mu_{\widetilde{A}}(x)+\mu_{\widetilde{B}}(x)+\mu_{\widetilde{C}}(x)}{3} \quad (4)$$

When harmonizing expert opinions, it is important to remember the inconsistency of expert opinions problem. It is crucial not only to aggregate assessments, but also to analyze the degree of disagreement among experts. If inconsistency is too large, this may indicate the need for additional discussions between experts or involvement of new specialists. In some cases, the harmonization process can be iterative. After the first aggregation, results can be provided to experts for discussion and possible correction of their initial assessments.

Defuzzification is an integral part of fuzzy systems, as it allows converting fuzzy recommendations into usual actions. Without this stage, the conclusions of the fuzzy system would remain “blurred” and unsuitable for use in the real world. This is the final stage in the developed fuzzy logic system, which consists of converting the fuzzy set of harmonized expert assessments back into a precise, numerical value of the weight coefficient.

To obtain a balanced assessment, the system used the center of gravity method and calculated precise values of importance coefficients according to formula (5).

$$\omega=\frac{\sum_{i=0}^{N}x_i\cdot\mu(x_i)}{\sum_{i=0}^{N}\mu(x_i)},x_i=i,N=10 \quad (5)$$

This method calculates the “center” of the area under the membership function curve of the output fuzzy set.

3. Results and discussion

In our research, three experts were required to evaluate the importance of the studied criterion on an 11-point scale independently. Let us consider the case when the provided assessments were 7, 8, and 10 points, respectively. At the fuzzification stage, each integer value was converted into the corresponding fuzzy sets using membership functions. The assessments of the first and second experts were transformed into a fuzzy set by introducing a membership function according to formula (1). Formula (3) was used to transform the assessment of the third expert.

The process of converting the first expert's quantitative assessment of 7 into a fuzzy set is demonstrated below:

$$\mu(x)=\begin{cases} 1, x=7 \\ \frac{1}{2}, x=6 \\ \frac{1}{2}, x=8 \\ 0, \in other\ cases \end{cases},$$

A graphical representation of membership functions for all three expert's scores is shown in Figure 2.

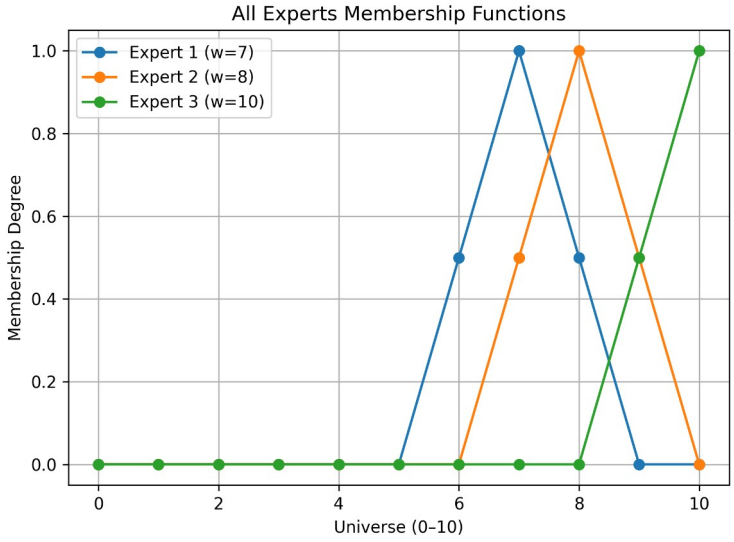

Figure 2: Graphical representation of membership functions for three experts' assessments

The next step involved aggregating the fuzzy sets to harmonize expert opinions according to formula (4). The results of calculating the harmonized membership function are presented as:

- x = 0...5: μ(0...5) = (0 + 0 + 0) / 3 = 0
- x = 6: μ(6) = (0.5 + 0 + 0) / 3 = 0.167
- x = 7: μ(7) = (1 + 0.5 + 0) / 3 = 0.5
- x = 8: μ(8) = (0.5 + 1 + 0) / 3 = 0.5
- x = 9: μ(9) = (0 + 0.5 + 0.5) / 3 = 0.333
- x = 10: μ(10) = (0 + 0 + 1) / 3 = 0.333

The harmonized fuzzy set has the form:

$$\tilde{W} = \{(0,0), (1,0), (2,0), (3,0), (4,0), (5,0), (6,0.17), (7,0.5), (8,0.5), (9,0.33), (10,0.33)\}$$

As shown in Figure 3, the obtained values show that the maximum degree of membership (μ = 0.5) is achieved for values 7 and 8, which indicates the concentration of expert assessments in this range and reflects the collective opinion regarding the priority of the estimated criterion.

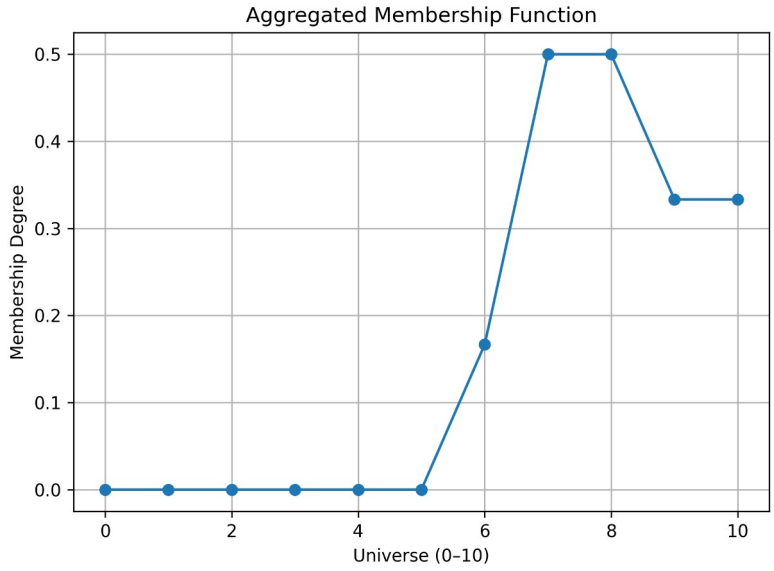

Figure 3: Fuzzy set aggregation function

The final stage was defuzzification, which describes the procedure for converting the resulting fuzzy set into a single real number with subsequent rounding for use as a weight coefficient in the decision support system. According to formula (5), this is the weighted average of all possible output values for the obtained aggregated fuzzy set. Substituting the values of the harmonized fuzzy set, we get:

$$\omega = \frac{0 \cdot 0 + \ldots + 5 \cdot 0 + 6 \cdot 0.167 + 7 \cdot 0.5 + 8 \cdot 0.5 + 9 \cdot 0.333}{0 + 0 + 0 + 0 + 0 + 0 + 0.167 + 0.5 + 0.5 + 0.333 + 0.333} = \frac{14.829}{1.833} = 8.09$$

As a result of applying the fuzzy logic system for harmonizing expert assessments of criterion importance, an importance coefficient of 8.09 was obtained, as shown in Figure 4.

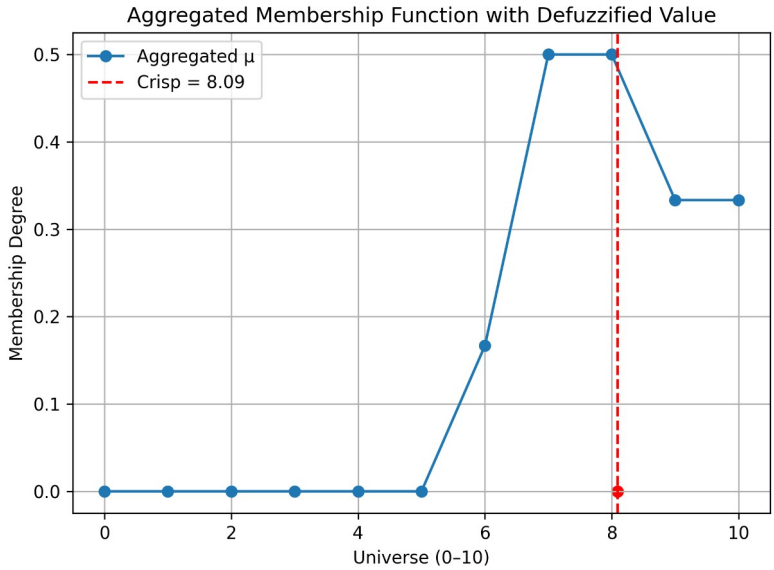

Figure 4: Defuzzification function

For practical use in the developed information system, the importance coefficient value was rounded to the integer 8.

This result reflects the harmonized opinion of three experts, taking into account the uncertainty of their judgments, and demonstrates the high importance of this criterion for ensuring web application security. Such methodology allows accounting for the uncertainty of expert judgments and provides more substantiated harmonization of different viewpoints when forming a system of weight coefficients.

Conclusions

The proposed fuzzy logic system is a part of the developed information system, which is used for harmonizing expert assessments of weight coefficients. It demonstrates high efficiency in solving problems of subjectivity and uncertainty in expert evaluation. The three-stage process (fuzzification, harmonization, and defuzzification) allowed transforming expert judgments into substantiated quantitative metrics. Integration of the developed subsystem into the overall architecture of the information system ensures objectivity in establishing security priorities. The case when standard coefficients do not meet the specific requirements of a particular web application is taken into consideration under development of information system. To ensure methodology adaptability, the user of system has the ability to modify any weight coefficients depending on the architecture and functionality of the web application.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] O. A. Revniuk, N. V. Zahorodna, A Methodology for the Quantitative Assessment of Web Application Security of an E-Commerce System at the Operation Stage, Scientific Bulletin of Ivano-Frankivsk National Technical University of Oil and Gas, 2(57) (2024) 107–119. doi:10.31471/1993-9965-2024-2(57)-107-119

[2] O. Revniuk, N. Zagorodna, O. Ulichev, Adaptive Methodology for Computing the Quantitative Security Status Indicator of Web Applications, Cent. Ukr. Sci. Bull. Tech. Sci. 2.10(41) (2024) 3–10. doi:10.32515/2664-262x.2024.10(41).2.3-10

[3] H. Liao, S. Yang, E. Kazimieras Zavadskas, M. Škare, An Overview of Fuzzy Multi-Criteria Decision-Making Methods in Hospitality and Tourism Industries: Bibliometrics, Methodologies, Applications and Future Directions, Econ. Res. Istraz. (2022) 1–42. doi:10.1080/1331677x.2022.2150871

[4] A. O. Abdulraheem, S. A. Adepoju, A. O. Ojerinde, O. A. Abisoye A Brief Overview on Applications of Multi-Criteria Decision Making Methods in Web Application Security, Adv. Multidiscip. Sci. Res. J. Publ. 2.2 (2023) 59–66. doi:10.22624/aims/csean-smart2023p8

[5] J. Levy, A Fuzzy Logic Evaluation System for Commercial Loan Analysis, Omega 19.6 (1991) 651–669. doi:10.1016/0305-0483(91)90014-k

[6] A. Shameli-Sendi, Fuzzy Multi-Criteria Decision-Making for Information Security Risk Assessment, Open Cybern. & Syst. J. 6.1 (2012) 26–37. doi:10.2174/1874110x01206010026

[7] A. Shameli-Sendi, Fuzzy Multi-Criteria Decision-Making for Information Security Risk Assessment, Open Cybern. & Syst. J. 6.1 (2012) 26–37. doi:10.2174/1874110x01206010026

[8] R. Kumar, A. Baz, H. Alhakami, W. Alhakami, A. Agrawal, R. A. Khan, A Hybrid Fuzzy Rule-based Multi-Criteria Framework for Sustainable-Security Assessment of Web Application, Ain Shams Eng. J. 12.2 (2021) 2227–2240. doi:10.1016/j.asej.2021.01.003

[9] A. Mardani, A. Jusoh, E. K. Zavadskas, Fuzzy Multiple Criteria Decision-Making Techniques and Applications—Two Decades Review from 1994 to 2014, Expert Syst. With Appl. 42.8 (2015) 4126–4148. doi:10.1016/j.eswa.2015.01.003

[10] Y. Sovyn, V. Khoma, I. Opirskyy, V. Kozachok, Minimization of Bitsliced Representation of 4×4 S-Boxes based on Ternary Logic Instruction, in: Cybersecurity Providing in Information and Telecommunication Systems, 3421, 2023, 12–24.

[11] Y. Lakh, E. Nyemkova, A. Piskozub, V. Yanishevskyi, Investigation of the Broken Authentication Vulnerability in Web Applications, in: Proc. 11th IEEE Int. Conf. IDAACS, Cracow, Poland, 1, 2021, 928–931.

[12] O. Revniuk, N. Zagorodna, R. Kozak, B. Yavorskyy, Development of an Information System for the Quantitative Assessment of Web Application Security based on the OWASP ASVS Standard, Sci. J. TNTU (Tern.) 118(2) (2025) 56–65.

[13] S. Shevchenko, Y. Zhdanova, O. Kryvytska, H. Shevchenko, Fuzzy Cognitive Mapping as a Scenario Approach for Information Security Risk Analysis, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3826, 2024, 356–362.

[14] Y. Kostiuk, P. Skladannyi, V. Sokolov, M. Vorokhob, Models and Technologies of Cognitive Agents for Decision-making with Integration of Artificial Intelligence, in: Modern Data Science Technologies Doctoral Consortium (MoDaST), vol. 4005 (2025) 82–96.

[15] O. Milov et al., Development of Methodology for Modeling the Interaction of Antagonistic Agents in Cybersecurity Systems, Eastern-European J. Enterp. Technol. 2.9 (98) (2019) 56–66. doi:10.15587/1729-4061.2019.164730