ISSN-L 2664-9969; E-ISSN 2706-5448

UDC 004.89:519.816
DOI: 10.15587/2706-5448.2024.318446

Oksana Mulesa,
Yurii Bohdan

DEVELOPMENT OF A FUZZY PRODUCTION MODEL FOR ASSESSING THE DEGREE OF INFORMATION SECURITY IN INTERNATIONAL COOPERATION

The object of research is the methods of assessing the information security indicator in the process of international cooperation.

The problem of unification and simplification of the processes of assessing the degree of information security is considered in order to reduce the involvement of human and material resources in them, using the apparatus of fuzzy set theory to take into account the conclusions of competent experts.

A fuzzy production model of assessing the degree of information security is developed, which is based on the use of expert knowledge and fuzzy logic methods. A step-by-step approach is proposed for identifying potential risks, classifying them by categories and calculating influence coefficients. An iterative assessment method is created, which allows obtaining a numerical indicator of the degree of information security. Heuristic rules for determining the effective assessment of the degree of information security are developed, taking into account the criticality factor and influence coefficients of different risk categories.

A classification of potential information security risks in international IT projects is proposed. An example of constructing production rules for a fuzzy knowledge base is demonstrated.

The results are explained by the use of systems analysis to take into account the relationships between different risk categories and the use of fuzzy logic to work with uncertain and incomplete data. The model is based on production rules that integrate expert judgment and allow for adaptive analysis in changing conditions of international cooperation.

The developed model can be used to assess information security in small and medium-sized international projects, where it is necessary to provide a quick and effective assessment of the level of security without involving significant resources. The model is especially useful in conditions where the data is fuzzy or incomplete, and the risks vary depending on the specifics of cooperation between different countries and organizations.

Keywords: *fuzzy production model, information security, international cooperation, potential risks, influence coefficients, risk categories.*

Received: 12.10.2024
Received in revised form: 02.12.2024
Accepted: 16.12.2024
Published: 23.12.2024

How to cite
Mulesa, O., Bohdan, Y. (2024). Development of a fuzzy production model for assessing the degree of information security in international cooperation. Technology Audit and Production Reserves, 6 (2 (80)), 6–10. https://doi.org/10.15587/2706-5448.2024.318446

1. Introduction

Globalization of many spheres of human activity leads to a rapid growth in the volume of international cooperation. Involving foreign partners in business, science, education or other spheres allows to increase their scale, increase the efficiency of functioning and exchange experience [1, 2]. A feature of such cooperation is the remoteness of partners in space, the difference in corporate cultures and languages, as well as differences in national legislation and traditions of carrying out a particular activity. To ensure the comfort and efficiency of such cooperation, simplification and unification of basic production and communication processes are relevant. An important characteristic of these processes is the degree of their information security, which expresses the level of protection of information and information systems from threats that may violate their confidentiality, integrity or availability [3, 4]. In view of this, it is the processes and methods of assessing the degrees of information security in such forms of cooperation that deserve attention.

There are many approaches to determine the level of information security of processes and phenomena. Among them are mathematical models, risk analysis methods, network infrastructure protection tools, and expert systems. In particular, statistical methods and machine learning methods [5–7] provide the basis for analyzing information security risks by assessing the dependencies between threats, their probability, and impact. However, their application requires large sets of input data, and their application is resource-intensive. In turn, determining the level of information security based on neural network methods requires the involvement of highly qualified analysts in this process [8, 9],

which is not advisable in processes that do not require complete information security and the data in which is not of high value. A separate group of methods is formed by adaptive methods [10, 11]. However, since these methods are based on a large number of complex mathematical calculations, their application requires the development and implementation of special software. Given that a large number of factors that need to be taken into account when assessing the level of information security are non-numerical in nature, methods that allow processing fuzzy data are of interest [12, 13]. In [14], a method for determining the level of information security in IIoT systems is proposed. The proposed approach has shown the effectiveness of using the fuzzy set apparatus and expert assessments for the problem under consideration, which can also be used to assess the information security of other processes and phenomena.

The aim of research is to develop a fuzzy production model for assessing the level of information security in international cooperation, the use of which will not require large expenditures of resources and time. The scientific part of research consists in formalizing the process of assessing the level of information security and in developing a method for assessing the level of information security based on the values of potential risks. The practical part involves the development of recommendations for the application of new models and methods in the analysis of processes and phenomena in international cooperation.

2. Materials and Methods

The object of research is the methods of assessing the information security indicator in the process of international cooperation.

During the study, the features of the implementation of cross-border projects and the problems that arise when ensuring information security in them were analyzed. Factors affecting the level of information security in the processes of international cooperation were systematized, as well as the main risks that may arise in these processes. The model is based on fuzzy logic methods.

When developing a model for assessing the degree of information security, the principles of system analysis were used, which made it possible to take into account the relationship between different categories of risks and their impact on the overall level of security. Special attention was paid to the use of production models to take into account expert knowledge and ensure the adaptability of the system to changing environmental conditions.

3. Results and Discussion

3.1. Determination and detailing of stages for assessing the degree of information security

Let's depict the process of determining the degree of information security in the form of a sequential implementation of such stages in Fig. 1.

The details of the stages are as follows.

Stage 1. Solving the problem of determining the set of potential risks for information security violations in international cooperation is the first step in assessing the level of information security in international cooperation. The process of solving it is associated with performing a situational analysis, as well as studying recommendations and experts in the field of information security. The key persons in this case are competent analysts and experts. An important aspect is to take into account different threat scenarios and the specifics of international cooperation, where additional challenges may arise due to differences in legislation and security policies between partners.

Potential risks usually include poor data access control, lack of clear security policies, inconsistency in privacy policies of different partners, etc.

Stage 2. After forming a set of potential risks, they are divided into categories. Such a division is necessary in order to identify similar or related risks or risks, the simultaneous occurrence of which can lead to a deterioration in information security. Risk grouping, as well as their identification, should be performed by a group of experts.

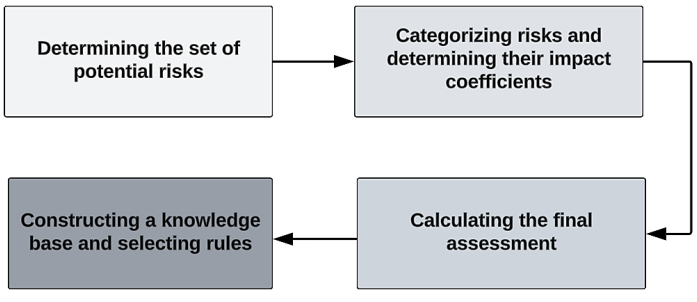

Fig. 1. Sequence of stages for assessing the level of information security

The task of determining the influence coefficients of different categories of risks on the degree of information security is also important. The methods for determining these coefficients include the following:

- the method of analysis of hierarchies [15], which allows to structure the task of selection or assessment and determine weight coefficients for different categories of risks based on expert assessments;
- the method of expert assessment [16], which consists in collecting the opinions of experts with further processing of the results to determine the influence coefficients;
- the entropy method [17], which allows to determine weight coefficients based on an objective analysis of available data on risks;
- methods based on fuzzy logic [18], which allow to take into account uncertainties and incompleteness of data;
- regression analysis methods [19], which allow determining the influence coefficients based on the dependence between the level of information security and various risk categories, etc.

Let the implementation of these stages result in a set of risk categories that have an impact on the resulting assessment of the degree of information security $(CR = \{R_1, R_2, ..., R_N\})$ and their influence coefficients $(\lambda_1, \lambda_2, ..., \lambda_N)$.

For *stages 3 and 4*, the method developed by the authors will be described below.

After implementing all stages from Fig. 1, a numerical value of the degree of information security IS will be obtained, which will express the safety of the conditions for implementing the studied process in percentages.

3.2. Development of a method for assessing the degree of information security based on the values of potential risks

To implement the method, it is necessary to specify a linguistic variable "Risk level", which will describe the degree

ISSN-L 2664-9969; E-ISSN 2706-5448

of risk of information security violation in the process under study [20]. For this linguistic variable, a term of the set $Y=\{\tilde{y}^1,\tilde{y}^2,\tilde{y}^3\}$ is specified, where $\tilde{y}^1$="High risk level", $\tilde{y}^2$="Low risk level", $\tilde{y}^3$="Average risk level" with membership functions of the form:

$$\mu_{C_1}(y)=\begin{cases}0, & \text{if } 0\le y<a,\\ 2\left(\dfrac{y-a}{1-a}\right)^2, & \text{if } a\le y\le\dfrac{a+1}{2},\\ 1-2\left(\dfrac{1-y}{1-a}\right)^2, & \text{if } \dfrac{a+1}{2}<y\le 1;\end{cases} \quad (1)$$

$$\mu_{C_2}(y)=\begin{cases}1-2\left(\dfrac{y}{1-a}\right)^2, & \text{if } 0\le y<\dfrac{1-a}{2},\\ 2\left(\dfrac{1-a-y}{1-a}\right)^2, & \text{if } \dfrac{1-a}{2}\le y\le 1-a,\\ 0, & \text{if } 1-a<y\le 1;\end{cases} \quad (2)$$

$$\mu_{C_3}(y)=\max\{0,1-2^b(y-0.5)^2\},\ y\in[0;1], \quad (3)$$

where $a\in(0;1)$, b – a natural number greater than 1, C_1,C_2,C_3 – fuzzy subsets.

An example of the graphs of functions (1)–(3) is shown in Fig. 2. The choice of the values of the parameters a and b depends on the features of the studied process and phenomenon.

The algorithm of the method for assessing the level of information security is iterative, each iteration is performed for a separate category of risks and can be represented as a sequence of steps.

The i-th iteration of the method.

Step 1. The category $R_i\in CR$ is considered. Let $r_{1i},r_{2i},...,r_{L_i i}$ be its elements, where $L_i=|R_i|$. For each element of this set r_{li}, it is possible to construct linguistic variables with the terms $\tilde{x}^1$="Strongly manifested", $\tilde{x}^2$="Weakly manifested".

Step 2. A fuzzy knowledge base is constructed in the form of production rules of the type "if ... then...". Moreover, those risks that are interconnected are combined into a production rule through the logical operation "and", and those that are unrelated – "or". An example of the rules of a fuzzy knowledge base is shown in (4).

$$\begin{aligned}&\text{if } r_{1i}\in A^1_{1i} \text{ and } r_{2i}\in A^1_{2i} \text{ ... and } r_{ki}\in A^2_{ki} \text{ then } y\in C_1,\\ &\text{if } r_{li}\in A^2_{li} \text{ then } y\in C_3,\\ &\text{... .}\end{aligned} \quad (4)$$

Step 3. For the given values of potential risks $r_{1i},r_{2i},...,r_{L_i i}$, the Mamdani fuzzy inference procedure is performed. Let $\mu_C(y)$ be the resulting fuzzy set.

Step 4. The resulting set is defuzzified according to rule (5).

$$\eta_i=\frac{\int_0^1 y\mu_C(y)\mathrm{d}y}{\int_0^1 \mu_C(y)\mathrm{d}y}. \quad (5)$$

The value η_i obtained as a result of execution of (5) will express the probability of information security violation at given values of potential risks of category R_i.

As a result of execution of N iterations of the described algorithm, a vector of probability values $(\eta_1,\eta_2,...,\eta_N)$ will be obtained. To calculate the information security (IS) assessment of the studied process or phenomenon, depending on its features, it is proposed to apply one of the following rules:

$$IS=(1-\max(\eta_1,\eta_2,...,\eta_N))\cdot 100\ \%, \quad (6)$$

$$IS=(1-\max_{i=\overline{1,N}:\lambda_i>\Delta}(\eta_i))\cdot 100\ \%, \quad (7)$$

$$IS=\left(1-\frac{\sum_{i=1}^N\lambda_i\eta_i}{\sum_{i=1}^N\lambda_i}\right)\cdot 100\ \%, \quad (8)$$

$$IS=\begin{cases}100\ \%, & \text{if } \bar{\exists} i\in\{1,2,...,N\}:\ \eta_i>\delta,\\ \left(1-\dfrac{\sum_{i=\overline{1,N}:\eta_i>\delta}\lambda_i\eta_i}{\sum_{i=\overline{1,N}:\eta_i>\delta}\eta_i}\right)\cdot 100\ \%, & \text{otherwise,}\end{cases} \quad (9)$$

where Δ, δ – the given threshold values of the corresponding indicators.

3.3. Discussion of the research results

As a result of the research, a fuzzy production model for assessing the degree of information security in international cooperation was developed, which includes the formalization of a multi-stage approach and an iterative method for assessing the degree of information security in international cooperation.

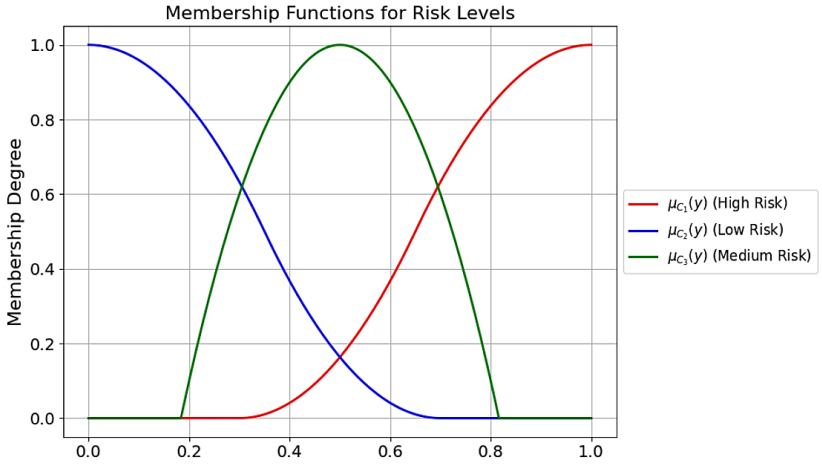

Fig. 2. Graphs of membership functions of the terms of the linguistic variable "Risk level" at $a=0.3$, $b=5$

The analysis of the problem made it possible to formalize the stages of assessing the degree of information security as shown in Fig. 1. Such visualization and subsequent detailing of the stages makes them understandable for users who are not specialists in the field of information security.

The method developed in the work integrates an approach to processing a knowledge base designed as a set of production rules. These rules are synthesized taking into account the results of expert surveys and allow processing not only numerical but also textual data. The idea of the method is to gradually determine the probability of information security violations for different categories of potential risks. Then, at the final stage, using the selected heuristics, it is proposed to calculate the degree of information security. The choice of heuristic depends on the presence of serious risks of vulnerability in the studied processes and phenomena, for example:

– rule (6) is recommended to be used in cases where it is necessary to take into account the greatest threat in conditions of the highest criticality;
– rule (7) – in situations where not all risks are equally important, and it is necessary to focus on the most significant threats (for example, to optimize resources in systems with limited resources);
– rule (8) allows to obtain the average value of the complex assessment and can be used for strategic planning or long-term forecasts;
– rule (9) is a combined approach that takes into account only the probability values greater than a given threshold.

The authors also analyzed a number of international projects in the IT sector and formed a set of potential risks that affect the degree of information security. The elements of this set and the method of dividing them into categories are given in Table 1.

Table 1

Categorizing potential risks

Category	Reasons for occurrence	Risks
Technological risks	Vulnerability in technological infrastructure	Outdated software
		Imperfect authentication system
		Presence of vulnerabilities in network protocols
Organizational risks	Security policies and procedures in organizations	Lack of clear security policies
		Poor data access control
		Insufficient staff training
Legal risks	Differences in legislation and regulations between partner countries	Inconsistency between national laws and international standards
		Inconsistencies in privacy policies
Socio-psychological risks	User actions or errors	Non-compliance with security rules
		Success of phishing attacks or social engineering
Political risks	Geopolitical situation or conflicts of interest between states	Sanctions or restrictions on access to technologies
		Political instability

Examples of production rules for such categories are as follows:

"If the system protection is low and there are many vulnerabilities, then the technological risk is high."
"If the system protection is high and the number of vulnerabilities is low, then the technological risk is low."
"If security policies are absent and the staff is not trained, then the organizational risk is very high."
"If compliance with legislation is low, then the legal risk is high."
"If the level of staff awareness is low and phishing attacks are frequent, then the socio-psychological risk is high."
"If the geopolitical situation is tense and cooperation is limited, then the political risk is very high."
"If the geopolitical situation is unstable, but cooperation continues, then the political risk is average"

Thus, the developed model and its components can be used in small international projects without the need to attract large amounts of financial and human resources for this.

The next stage of the research may be the development of an architecture and software components to automate the processes of assessing the degree of information security.

Limitations of research: the fuzzy production model relies heavily on expert judgment to formulate rules and determine risk impact factors. This can lead to subjectivity in the results, especially if the experts involved have different experiences or knowledge.

Martial law conditions did not affect the course of the research.

4. Conclusions

This research is devoted to solving the problem of assessing the degree of information security in international cooperation. During the study, factors that can affect information security indicators were analyzed. Based on the analysis performed, a fuzzy production model was constructed, the components of which are a formalized approach and an iterative method for assessing the degree of information security in international cooperation. Heuristic rules were developed that ensure the presence of a comprehensive approach to determining the assessment of information security based on data on risks of different categories. The choice of rules depends on the criticality of the problem under study, as well as on the presence of influence coefficients of different risk categories.

Also, during the practical part of the study, risks that can affect information security in international IT projects were systematized, which demonstrated the simplicity and clarity of the described approach.

Conflict of interest

The authors declare that they have no conflict of interest in relation to this study, including financial, personal, authorship, or any other, that could affect the study and its results presented in this article.

ISSN-L 2664-9969; E-ISSN 2706-5448

Financing

The study was conducted within the framework of the implementation of the state budget topic DB-921M "Information security protection in the management of international cooperation projects on the basis of ensuring the national security of Ukraine" with the support of the Ministry of Education and Science of Ukraine.

Data availability

The manuscript has no associated data.

Use of artificial intelligence

The authors confirm that they did not use artificial intelligence technologies when creating the presented work.

References

1. Mulesa, O., Yakob, E., Valko, P., Sviezhentseva, O., Marhitych, D. (2024). Development of decision-making technology for the provision of services in project implementation. *Technology Audit and Production Reserves, 2 (2 (76))*, 13–17. https://doi.org/10.15587/2706-5448.2024.301317
2. Mulesa, O., Horvat, P., Radivilova, T., Sabadosh, V., Baranovskyi, O., Duran, S. (2023). Design of mechanisms for ensuring the execution of tasks in project planning. *Eastern-European Journal of Enterprise Technologies, 2 (4 (122))*, 16–22. https://doi.org/10.15587/1729-4061.2023.277585
3. Vedadi, A., Warkentin, M., Dennis, A. (2021). Herd behavior in information security decision-making. *Information & Management, 58 (8)*, 103526. https://doi.org/10.1016/j.im.2021.103526
4. Georg-Schaffner, L., Prinz, E. (2021). Corporate management boards' information security orientation: an analysis of cybersecurity incidents in DAX 30 companies. *Journal of Management and Governance, 26 (4)*, 1375–1408. https://doi.org/10.1007/s10997-021-09588-4
5. Banitalebi Dehkordi, A., Soltanaghaei, M., Boroujeni, F. Z. (2020). The DDoS attacks detection through machine learning and statistical methods in SDN. *The Journal of Supercomputing, 77 (3)*, 2383–2415. https://doi.org/10.1007/s11227-020-03323-w
6. Ashok, K., Gopikrishnan, S. (2023). Statistical Analysis of Remote Health Monitoring Based IoT Security Models & Deployments From a Pragmatic Perspective. *IEEE Access, 11*, 2621–2651. https://doi.org/10.1109/access.2023.3234632
7. Radivilova, T., Kirichenko, L., Alghawli, A. S., Ageyev, D., Mulesa, O., Baranovskyi, O. et al.; Oliynykov, R., Kuznetsov, O., Lemeshko, O., Radivilova, T. (Eds.) (2022). Statistical and Signature Analysis Methods of Intrusion Detection. *Information Security Technologies in the Decentralized Distributed Networks. Vol. 115*. Cham: Springer International Publishing, 115–131. https://doi.org/10.1007/978-3-030-95161-0_5
8. Viktoriia, H., Hnatienko, H., Babenko, T. (2021). An intelligent model to assess information systems security level. *2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4)*. London, 128–133. https://doi.org/10.1109/worlds451998.2021.9514019
9. Ganguli, C., Shandilya, S. K., Izonin, I. (2023). Design and implementation of adaptive network stabilization based on artificial bees colony optimization for nature inspired cyber security. *Journal of King Saud University – Science, 35 (5)*, 102713. https://doi.org/10.1016/j.jksus.2023.102713
10. Jin, X., Lü, S., Qin, J., Zheng, W. X., Liu, Q. (2023). Adaptive ELM-Based Security Control for a Class of Nonlinear-Interconnected Systems With DoS Attacks. *IEEE Transactions on Cybernetics, 53 (8)*, 5000–5012. https://doi.org/10.1109/tcyb.2023.3257133
11. Chen, H., Galteland, Y. J., Liang, K.; Guo, J., Steinfeld, R. (Eds.) (2023). CCA-1 Secure Updatable Encryption with Adaptive Security. *Advances in Cryptology – ASIACRYPT 2023. Vol. 14442*. Singapore: Springer Nature Singapore, 374–406. https://doi.org/10.1007/978-981-99-8733-7_12
12. Lizunov, P., Biloshchytskyi, A., Kuchansky, A., Andrashko, Y., Biloshchytska, S. (2019). Improvement of the method for scientific publications clustering based on n-gram analysis and fuzzy method for selecting research partners. *Eastern-European Journal of Enterprise Technologies, 4 (4 (100))*, 6–14. https://doi.org/10.15587/1729-4061.2019.175139
13. Saatchi, R. (2024). Fuzzy Logic Concepts, Developments and Implementation. *Information, 15 (10)*, 656. https://doi.org/10.3390/info15100656
14. Kerimkhulle, S., Dildebayeva, Z., Tokhmetov, A., Amirova, A., Tussupov, J., Makhazhanova, U., Adalbek, A., Taberkhan, R., Zakirova, A., Salykbayeva, A. (2023). Fuzzy Logic and Its Application in the Assessment of Information Security Risk of Industrial Internet of Things. *Symmetry, 15 (10)*, 1958. https://doi.org/10.3390/sym15101958
15. Vaidya, O. S., Kumar, S. (2006). Analytic hierarchy process: An overview of applications. *European Journal of Operational Research, 169 (1)*, 1–29. https://doi.org/10.1016/j.ejor.2004.04.028
16. Paz, F., Moquillaza, A., Lecaros, A., Falconi, F., Aguirre, J., Ramos, C. (2023). Applying Heuristic Evaluation with Different Evaluator Profiles: A Comparative Study Between Novice and Expert Specialists. *Proceedings of the XI Latin American Conference on Human Computer Interaction*. Puebla: ACM, 1–7. https://doi.org/10.1145/3630970.3631063
17. Zhu, Y., Tian, D., Yan, F. (2020). Effectiveness of Entropy Weight Method in Decision-Making. *Mathematical Problems in Engineering, 2020*, 1–5. https://doi.org/10.1155/2020/3564835
18. Božanić, D., Pamučar, D., Milić, A., Marinković, D., Komazec, N. (2022). Modification of the Logarithm Methodology of Additive Weights (LMAW) by a Triangular Fuzzy Number and Its Application in Multi-Criteria Decision Making. *Axioms, 11 (3)*, 89. https://doi.org/10.3390/axioms11030089
19. Balboa, A., Cuesta, A., González-Villa, J., Ortiz, G., Alvear, D. (2024). Logistic regression vs machine learning to predict evacuation decisions in fire alarm situations. *Safety Science, 174*, 106485. https://doi.org/10.1016/j.ssci.2024.106485
20. Herrera-Viedma, E., Palomares, I., Li, C.-C., Cabrerizo, F. J., Dong, Y., Chiclana, F., Herrera, F. (2021). Revisiting Fuzzy and Linguistic Decision Making: Scenarios and Challenges for Making Wiser Decisions in a Better Way. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 51 (1)*, 191–208. https://doi.org/10.1109/tsmc.2020.3043016

✉***Oksana Mulesa,*** *Doctor of Technical Science, Professor, Department of Physics, Mathematics and Technologies, University of Presov, Presov, Slovakia; Department of Software System, Uzhhorod National University, Uzhhorod, Ukraine, ORCID: https://orcid.org/0000-0002-6117-5846, e-mail: mulesa.oksana@gmail.com*

Yurii Bohdan, *PhD Student, Department of Software System, Uzhhorod National University, Uzhhorod, Ukraine, ORCID: https://orcid.org/0009-0001-0337-7079*

✉*Corresponding author*