Автоматизовані системи управління та прилади автоматики. 2025. № 4 (187)

UDC 004.7:004.38:621.373.8:621.391 **DOI:** https://doi.org/10.30837/0135-1710.2025.187.220

O. Petrenko, O. Petrenko, A. Bidun, Z. Ostrovskyi

MODEL FOR ASSESSING THE LEVEL AND PRIORITIZING MULTI-PARAMETER THREATS USING THE MAMDANI FUZZY LOGIC ALGORITHM OF THE FIRST TYPE

The subject of the study is a model for assessing threats and determining their priorities based on fuzzy logic methods. The first-type Mamdani algorithm was used to build the model. The developed threat assessment model was tested on a static scenario, as well as on dynamic real-time attack scenarios. The problem was solved using fuzzy logic methods. *The Fuzzy Logic Toolbox* (a MATLAB extension) was used to model the system, which contains tools for designing systems based on fuzzy logic. Block diagrams of the static and dynamic fuzzy threat assessment models are presented in the *Simulink* application. The purpose of the study is to develop and analyze a fuzzy model for assessing threats and determining their priorities in order to make decisions on the sequence of measures to counter these threats. **The objectives of the work** include justifying the feasibility and effectiveness of using fuzzy logical expressions and fuzzy logic operations for a formalized description of expert requirements for determining threat priorities. Fuzzy logic methods are widely implemented in various control systems, particularly in the following areas: nonlinear process control, self-learning systems, risk and critical situation analysis, pattern recognition, financial analysis, corporate repository information research, and management and coordination strategy optimization. **Methods used in the study:** probability theory, fuzzy logic theory, modeling. **Results achieved.** The possibility of using fuzzy logical expressions and fuzzy logic operations for a formalized description of expert criteria for determining threat priorities is considered. This approach provides numerical assessments of threats based on specified parameters, which contributes to accuracy and flexibility in the analysis process. The possibility of using fuzzy logical expressions and fuzzy logic operations for a formalized description of expert requirements for determining threat priorities is justified. This makes it possible to obtain numerical threat assessments based on specified input parameters, ensuring accuracy and adaptability in the analysis process. The article proposes an algorithm for rating threats on a scale from 0 to 1 using a fuzzy logic system, which contributes to accurate results. **Conclusions.** The developed procedure for prioritizing threats, based on a fuzzy set model, significantly expands the functionality and allows determining threat levels. This, in turn, creates the basis for making effective decisions on the implementation of measures to counter these threats and is the main result of the study.

Keywords: model; fuzzy logic; membership function; threat level assessment; threat prioritization; decision support; uncertainty; linguistic variables; fuzzy inference.

Introduction

Problem statement

In most cases, security specialists assess threats based on their own experience, converting threat levels into numerical values. However, this approach to assessing threat levels significantly limits the overall capabilities of the methodology, as the reliability of expert conclusions often gives rise to conflicting opinions. In today's world, the rapid development of information technology and the increasing complexity of decision-making processes bring to the fore methods that take into account factors of uncertainty and insufficient data. Approaches based on fuzzy logic, which allows for the formalization and analysis of complex systems where traditional methods lose their effectiveness, are particularly important in this context.

The article focuses on the development of methodological foundations and practical recommendations for the implementation of threat prioritization systems using fuzzy logic. Fuzzy set methods are particularly useful in situations where it is impossible to construct an accurate mathematical model of the system's functioning.

Thanks to fuzzy set theory, it becomes possible to use imprecise and subjective expert knowledge about the subject area to make decisions without the need to formalize them in the form of traditional mathematical models.

Thus, the implementation of fuzzy logic methods for assessing the level of threats with their subsequent prioritization for timely and balanced countermeasures is a relevant scientific task.

Analysis of recent studies and publications

Fuzzy logic first appeared in the mid-1960s thanks to the work of Lotfi Zadeh [1], an American mathematician and logician who first introduced the concept. Since then, its theoretical foundations and models have continued to evolve and remain one of the most widely used methods today.

The practical application of fuzzy set theory actually began in 1975, when E. Mamdani created the first fuzzy controller [2]. Fuzzy logic methods are widely used in various control systems, particularly in the following areas: control of nonlinear processes, self-learning systems, analysis of risky and critical situations, pattern recognition, financial analysis, research of data from corporate repositories, optimization of management strategies, and coordination of actions [3, 4].

Works [5, 6] discuss the development of an automated decision support system that uses fuzzy networks to analyze and assess the air situation from the perspective of threats.

An analysis of scientific literature demonstrates the active and effective application of fuzzy logic methods for threat assessment in various fields, including information security, cybersecurity, and critical infrastructure risk management [7, 8].

The main advantage of using fuzzy logic is its ability to effectively process inaccurate, fuzzy, or incomplete input data and expert assessments, which are often encountered during threat analysis.

Numerous studies [9, 10, 11, 12] consider the practical implementation of the presented models, in particular using the Fuzzy Logic Toolbox environment in MatLab, as well as the creation of test sets of fuzzy rules. Research shows that fuzzy logic methods are an important and effective tool for threat assessment, especially in situations with significant uncertainty. These methods facilitate the development of reliable and adaptive models that take expert knowledge into account, ensuring more informed decision-making in the field of security.

Other studies in this area cover such areas as guided fuzzy clustering [13], rule merging [14], and multi-criteria optimization.

The purpose of this article is to develop and analyze a fuzzy model for assessing threats and determining their priorities in order to make decisions on the sequence of measures to counter these threats.

Presentation of main material

To eliminate the shortcomings of existing risk analysis and assessment methods, the use of fuzzy logic methods is proposed. Fuzzy logic demonstrates high efficiency in cases where there is insufficient understanding of the characteristics of the system under study, limited access to the necessary amount of data, and risk assessment is based on expert information, where the input data may be insufficiently accurate or incorrectly presented. The flexibility and ease of use of fuzzy logic as a methodology for solving problems ensure its effective implementation in data control and analysis systems. At the same time, human intuition and operator experience are also involved [15, 16].

Fuzzy logical inference assumes that a set of rules must be applied to evaluate the activated membership function. In the context of fuzzy logical inference, such a set is called a rule base or knowledge base for a specific subject area. The use of a set of rules contributes to a more complete coverage of the reference space, while ensuring the reliability of the conclusions obtained [17]. Based on the set of rules, a fuzzy logical inference system is built, as shown in Fig. 1.

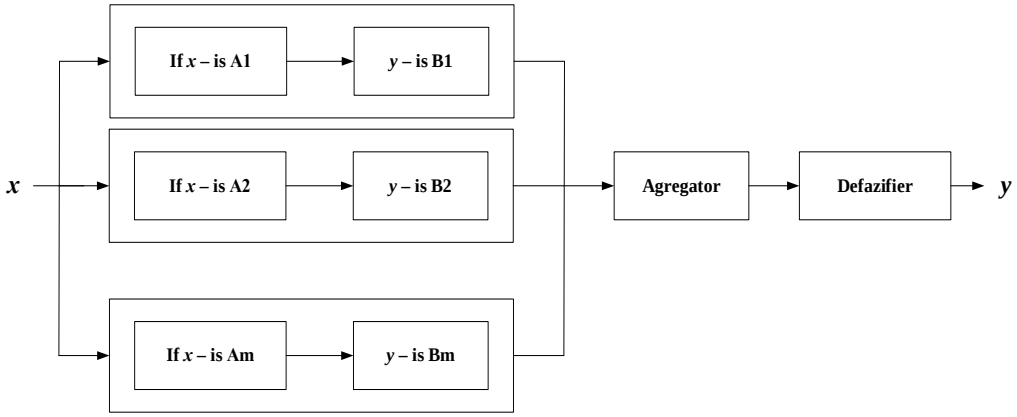

Fig. 1. Structural diagram of a fuzzy logic inference system
Source: [17]

The fuzzy inference process, based on fuzzy set theory, involves the use of fuzzy logic to form a correspondence between a given input signal and an output result. This mapping serves as the basis for decision-making or pattern recognition. This process takes into account all key elements: membership function, logical operations, and if-then rules [18]. This article proposes an algorithm based on fuzzy inference rules using the Mamdani algorithm, which is designed to assess the level of threat. In the algorithm, several arrays of input data are processed to determine the initial value of the threat level.

The Mamdani algorithm is one of the first to be successfully implemented in fuzzy inference systems. It was developed in 1975 by English mathematician Ebrahim Mamdani as an approach to controlling the operation of a steam engine [19]. Fuzzy inference using the Mamdani method was first proposed for the development of control systems based on the synthesis of linguistic rules formulated by experienced experts [2]. In this system, the output of each rule is represented as

a fuzzy set of all possible values of a linguistic variable. Mamdani systems, due to their intuitiveness and simpler rule base structure, are ideal for use in expert systems in which rules are formed based on the knowledge and experience of specialists.

The Mamdani algorithm works as follows:

- for each input parameter, the degree of its membership in the corresponding fuzzy set is determined;
- based on each fuzzy logical rule, the degree of correspondence of the rules to the obtained data is evaluated;
- the degree of membership of each conclusion derived from fuzzy logical rules is calculated;
- calculations are performed to determine the values of the conclusions.

The obtained values have the form of a fuzzy quantity representing the result of logical analysis. To convert this result into a clear value, a defuzzification procedure is used.

The inference process for the Mamdani system is summarized in Fig. 2.

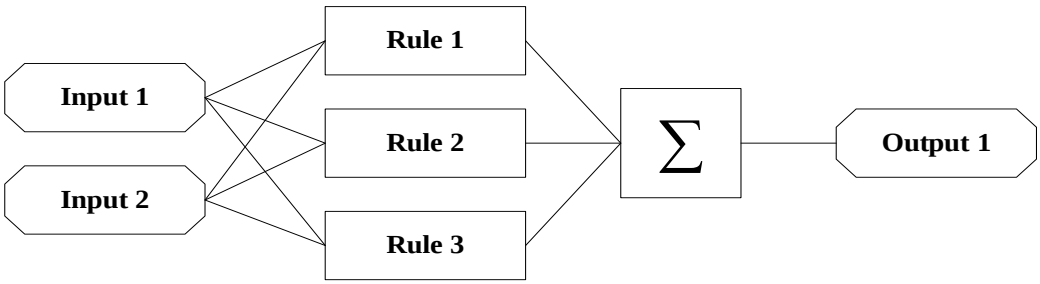

Fig. 2. Fuzzy inference process for the Mamdani system
Source: [20]

The MATLAB Fuzzy Logic Toolbox and Simulink extension package was used to model the system. A triangular shape was chosen for the membership functions. After defining the input variables, the graphical interface of the membership function editor is shown in Fig. 3.

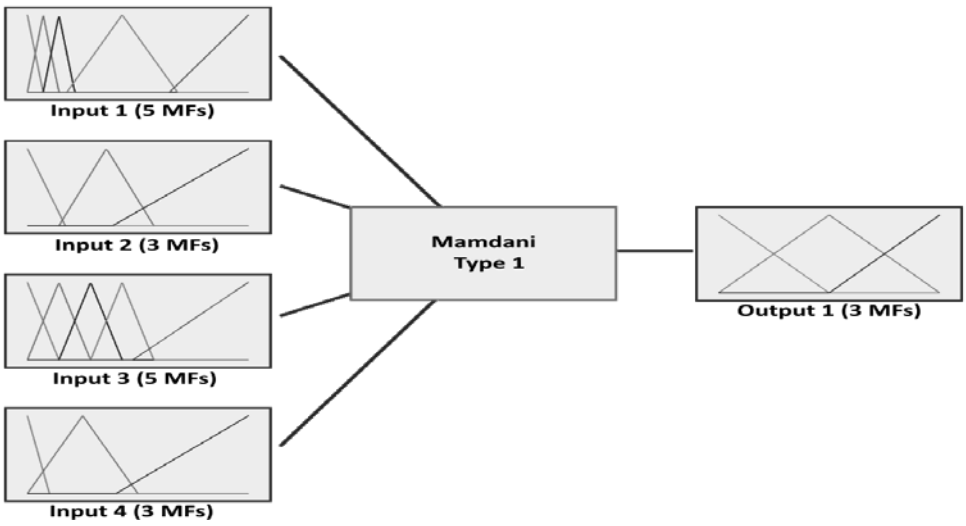

Fig. 3. Graphical interface of the membership function editor
Source: developed by the authors

Figure 4 shows the membership functions for four possible types of input parameters. These functions show how each point of influence of the input parameter determines the membership value in the range from 0 to 1.

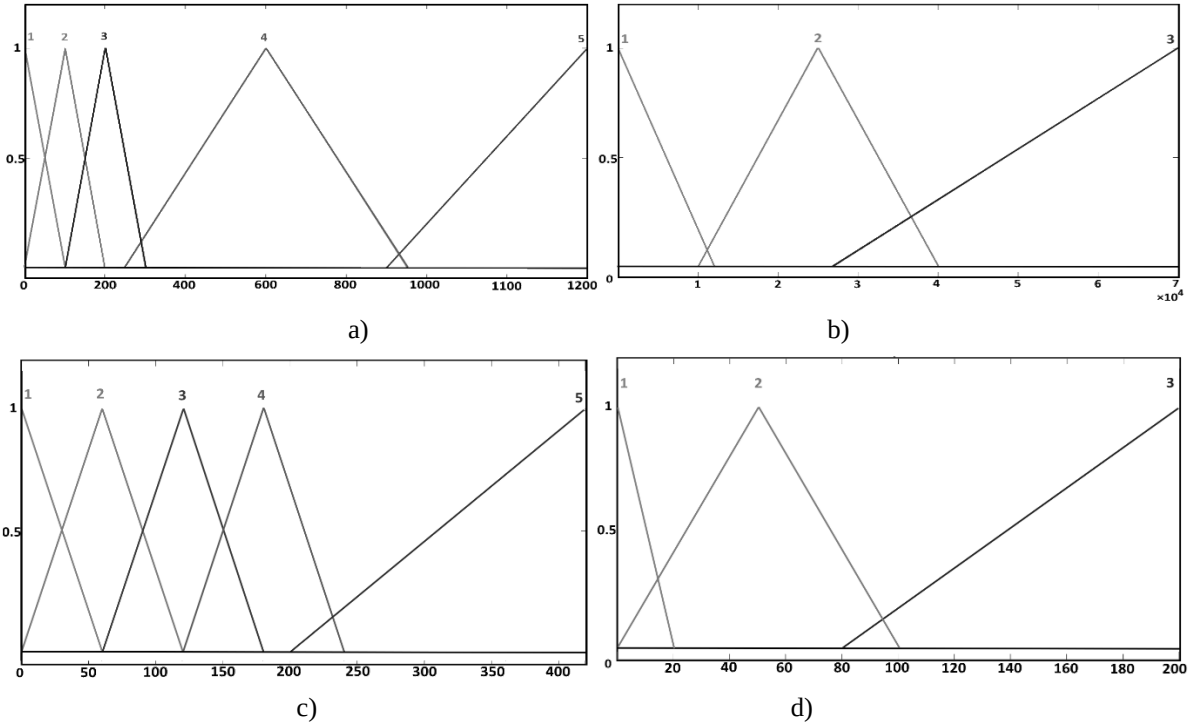

Fig. 4. Membership functions for input parameters of the first type (a), second type (b), third type (c), and fourth type (d)
Source: developed by the authors

The output parameter of the fuzzy model for threat assessment is the threat priority, which varies from 0 to 1. This is illustrated in Fig. 5.

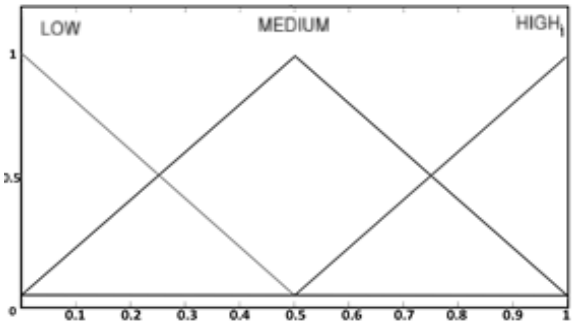

Fig. 5. Membership functions for threat prioritization
Source: developed by the authors

In the course of work, based on available standard data and expert comments on the relationship between input and output parameters, it is necessary to define fuzzy inference rules. Initial rules were formulated and evaluated for reliability in both static conditions and real-time scenarios. The input data allows the priority of threats to be adapted by applying specific rules.

Within the framework of the presented model, 226 rules were formulated, confirming its stability and effectiveness. Some of the fuzzy inference rules used are described in detail in Table 1.

Table 1. *Basic rules of fuzzy inference applied in this article*

Rule	Description
Rule 1 (low priority)	IF (Input1 is mf1) AND (Input2 is mf3) AND (Input3 is mf5) AND (Input4 is mf1) THEN (Output1 is mf1) (Weight: 1)
Rule 2 (low priority)	IF (Input1 is mf2) AND (Input2 is mf2) AND (Input3 is mf4) AND (Input4 is mf2) THEN (Output1 is mf1) (Weight: 1)
Rule 3 (low priority)	IF (Input1 is mf3) AND (Input2 is mf3) AND (Input3 is mf3) AND (Input4 is mf3) THEN (Output1 is mf1) (Weight: 1)
Rule 4 (medium priority)	IF (Input1 is mf4) AND (Input2 is mf2) AND (Input3 is mf3) AND (Input4 is mf3) THEN (Output1 is mf2) (Weight: 1)
Rule 5 (medium priority)	IF (Input1 is mf4) AND (Input2 is mf2) AND (Input3 is mf3) AND (Input4 is mf2) THEN (Output1 is mf1) (Weight: 1)
Rule 6 (high priority)	IF (Input1 is mf5) AND (Input2 is mf1) AND (Input3 is mf1) AND (Input4 is mf3) THEN (Output1 is mf3) (Weight: 1)
Rule 7 (high priority)	IF (Input1 is mf5) AND (Input2 is mf2) AND (Input3 is mf1) AND (Input4 is mf3) THEN (Output1 is mf3) (Weight: 1)
Rule 8 (high priority)	IF (Input1 is mf5) AND (Input2 is mf1) AND (Input3 is mf2) AND (Input4 is mf3) THEN (Output1 is mf3) (Weight: 1)

Let us assume that, after analyzing the system's performance, experts evaluated the input parameters according to the following indicators: first type – 70 points, second type – 30,000 points, third type – 180 points, and fourth type – 80 points. In accordance with the defined rules and using Mamdani's fuzzy inference algorithm, an initial threat assessment of 0.202 was obtained (Fig. 6).

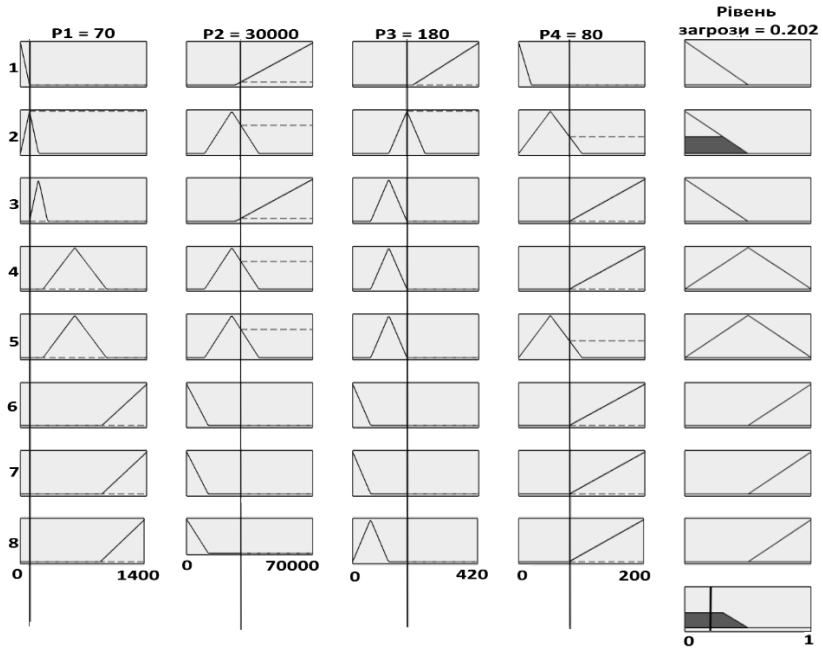

Fig. 6. Graphical interface of the program for viewing rules (Fuzzy Logic Designer Rule Inference) after completing the fuzzy inference procedure
Source: developed by the authors

The diagram of the proposed fuzzy model for threat assessment, developed using MATLAB software, is shown in Fig. 7. The figure shows a static scenario that processes input parameters as constant information for each moment in time. The basic fuzzy inference system assesses the threat level for each set of input parameters.

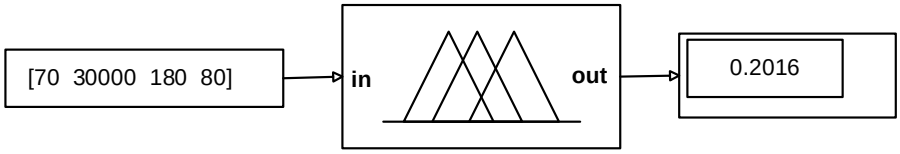

Fig. 7. Static model of fuzzy logic for threat assessment in the MATLAB environment
Source: developed by the authors

A threat with a higher priority characterizes a more dangerous set of input parameters. The threat priority value itself influences decisions on the use of protective measures to neutralize this threat. Table 2 presents the results of modeling in a static test scenario performed over eight time points for a set of four input parameters.

Table 2. *Results of modeling in a static test scenario with an 8-cycle run*

№	P_1	P_2	P_3	P_4	T
1	70	45000	250	80	0.202
2	187	38000	220	90	0.5
3	295	33700	150	100	0.4963
4	450	27700	100	150	0.5
5	792	17000	70	70	0.5
6	955	10200	45	65	0.7661
7	1110	7690	30	20	0.7942
8	1224	5960	20	15	0.8085

The results of testing this model with the parameters shown in Table 2 are shown in Fig. 8.

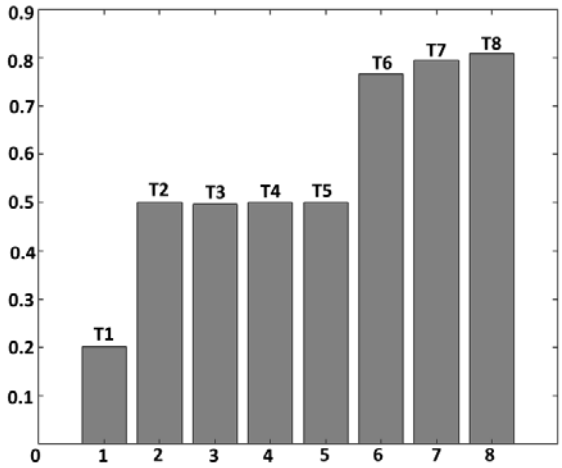

Fig. 8. Threat level assessment during static scenario testing

Assessing the threat level during static scenario testing is crucial for ensuring system security and reliability. It allows you to identify potential risks, detect weaknesses in the architecture or code, and predict possible damage scenarios.

Proper testing helps prevent critical problems, reduces the likelihood of failure, and promotes more informed decisions about protection, such as information or data.

Let's consider several scenarios for modeling dynamic attacks based on given input parameters in order to assess the threats that may arise within their limits. To study the stability and effectiveness of the fuzzy model, a comparison of the results obtained when implementing different scenarios was performed.

Figure 9 shows an example of a dynamic scenario that adaptively analyzes input parameters and uses them as data relevant to solving real-world problems that change over time.

The block diagram of this scenario was developed using the MATLAB software environment.

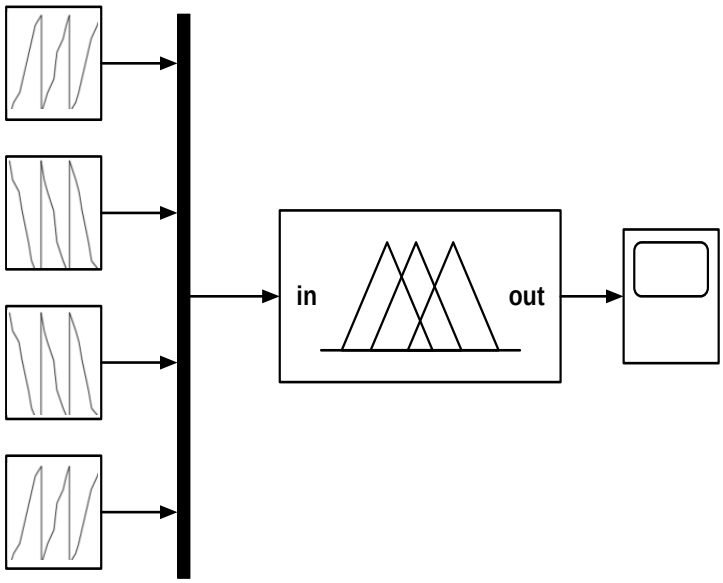

Fig. 9. Dynamic model of fuzzy logic for threat assessment in the MATLAB environment
Source: developed by the authors

In all scenarios considered, the input data of the fuzzy model is formed as a set of input parameters that are received in real time. In the first scenario, each of the parameters changes in a certain way.

In particular, parameter P_1 is characterized by increasing variable values, which at eight time points take the form [70, 187, 295, 450, 792, 955, 1110, 1224].

Parameter P_2 shows a decrease in variable values, which at the same time points are equal to [45000, 38000, 33700, 27700, 17000, 10200, 7690, 5960]. In turn, parameters P_3 and P_4 also decrease over time.

Their values in eight time intervals are [250, 220, 150, 100, 70, 45, 30, 20] and [200, 170, 140, 110, 80, 50, 20, 10], respectively. The characteristics of changes over time for each of the four parameters – P_1, P_2, P_3, and P_4 – used in this scenario are clearly illustrated in Fig. 10.

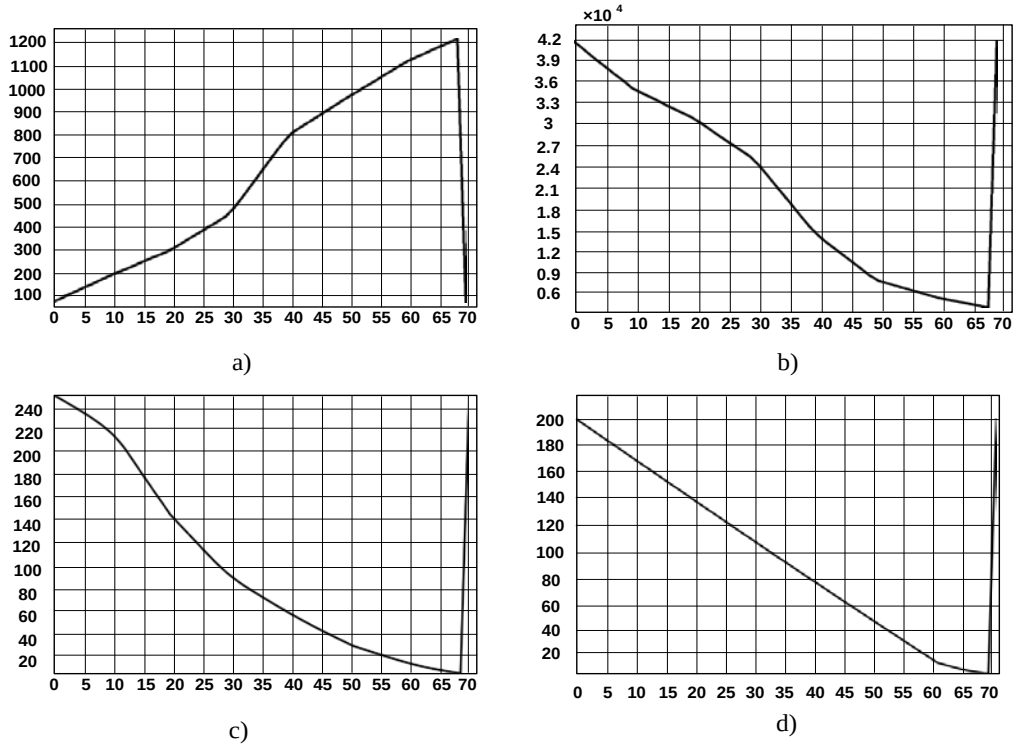

Fig. 10. Dependence of input parameters of the first type (a), second type (b), third type (c), and fourth type (d) on time

Source: developed by the authors

Fig. 11 shows the results of assessing the threat to a fuzzy system. As can be seen, the threat value increases significantly with the growth of parameter P_1, while the other three parameters show a downward trend. In the first scenario, the final threat value is 0.8014, which indicates a fairly high level of threat.

Fig. 11. Output of the fuzzy logic model for assessing threats for the first scenario

Source: developed by the authors

The second scenario assumes that each of the specified parameters changes according to certain patterns over eight different points in time. In particular, parameter P_1 shows a gradual decrease in its values, taking the following indicators: [1500, 1000, 800, 700, 300, 200, 100, 50]. At the same time, parameter P_2, on the contrary, is characterized by an increase in values and is determined by the following values: [2000, 3000, 7000, 10000, 12000, 15000, 16000, 19000]. As for parameters P_3 and P_4, both also show a tendency to increase in value over time, reaching values of [15, 25, 35, 75, 115, 140, 150, 160] for P_3 and [0, 5, 10, 15, 20, 30, 40, 50] for P_4. The dynamics of change for each of these four parameters – P1, P2, P3, and P4 – according to the scenario are illustrated in Fig. 12.

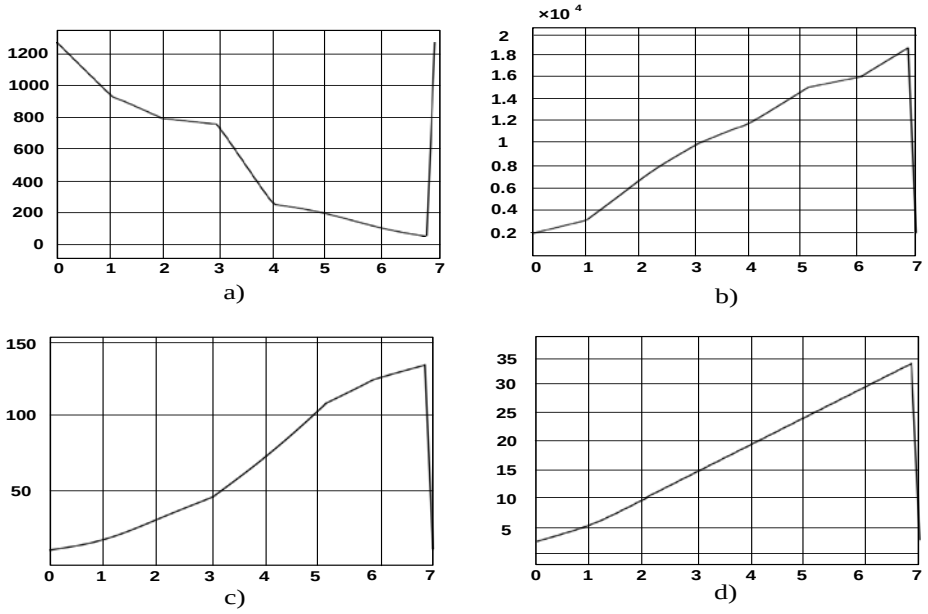

Fig. 12. Dependence of input parameters of the first type (a), second type (b), third type (c), and fourth type (d) on time
Source: developed by the authors

Fig. 13 shows the results of the fuzzy system threat assessment. Given the above conditions, the threat value is significantly reduced, as parameter P_1 tends to decrease, while the other three parameters show an increase.

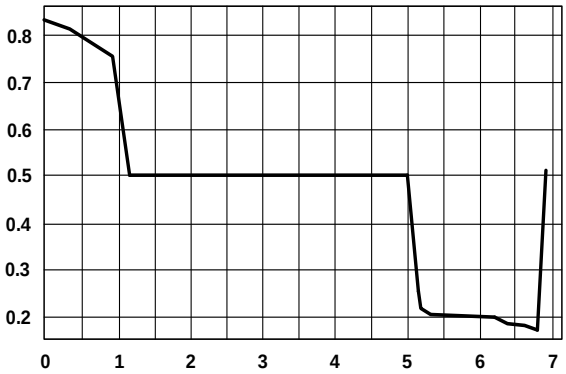

Fig. 13. Output of the fuzzy logic model for assessing threats for the second scenario
Source: developed by the authors

Conclusions

The study presents a detailed description of the approach to threat assessment using fuzzy set theory. An analysis of the parameters necessary for calculating the threat level was carried out, and a multifunctional approach to decision-making based on fuzzy logic was determined. Such a system is an effective tool that optimizes the decision support process, greatly facilitating the work of the specialist conducting the assessment.

The article proposes an algorithm for rating threats on a scale from 0 to 1 using a fuzzy logic system, which ensures high accuracy of results. The developed threat assessment model was tested on a static scenario, as well as on dynamic real-time attack scenarios. A comparison of the simulation results in Table 2 for static threats with the results in Figure 11 for the dynamic scenario demonstrates the high accuracy, reliability, and minimal error rate of the created model. This indicates its effectiveness and potential for use in various conditions.

The developed threat prioritization procedure, based on a fuzzy set model, significantly expands the functionality and allows determining threat levels. This, in turn, creates a basis for making informed decisions on the implementation of measures to counter these threats.

The use of the obtained results as statistical data for calculating the probability of a threat and the method of refining the probabilities of events is appropriate when constructing a functional model for threat detection based on a Bayesian network [21, 22], which will allow refining the probability of its occurrence.

References

1. Zadeh, L. A. (2015), "Fuzzy logic – a personal perspective", *Fuzzy Sets and Systems*. Vol. 281. DOI: https://doi.org/10.1016/j.fss.2015.05.009.
2. Mamdani, E.H., Assilian, S. (1975), "An Experiment in Linguistic Synthesis with a Fuzzy Logic Controller", *International Journal of Man-Machine Studies*. Vol. 7, No. 1, P. 1-13. DOI: https://doi.org/10.1016/S0020-7373(75)80002-2.
3. Chen G., Trung T. (2000), "Introduction to fuzzy sets", *fuzzy logic, and fuzzy control systems*, Boca Raton, London, New York, No. 1, P. 316. DOI: https://doi.org/10.1201/9781420039818.
4. Espinosa, J., Vandewalle, J., Wertz, V. (2005), "Fuzzy Logic, Identification and Predictive Control", *Vincent Wertz*. – USA: Springer-Verlag London Limited, P. 263. DOI: https://doi.org/10.1007/b138626.
5. Volkov, A., Bazilo, S., Tokar, O., Horbachov, K., Lutsyshyn, A., Zaitsev, I., Iasechko, M. (2022), "Automated assessment of the air situation during the preparation and conduct of combat operations using a decision support system based on fuzzy networks of target installations", *International Journal of Computer*, Vol. 22, No. 11, P. 184–188. DOI: https://doi.org/10.22937/IJCSNS.2022.22.11.26.
6. Volkov, A., Stadnichenko, V., Yaroshchuk, V., Halkin, Y., Tokar, O. (2024), "Proposals for the implementation of a decision support system for air defence fire control based on fuzzy networks of targets", *Systemy Logistyczne Wojsk*, No. 61, P. 211-228. DOI: https://doi.org/10.37055/slw/203558.

7. Azimirada, E., Haddadniab, J. (2015), "Target threat assessment using fuzzy sets theory", *International Journal of Advances in Intelligent Informatics*, Vol 1, No. 2, P. 57–74. DOI: https://doi.org/10.26555/ijain.v1i2.18.
8. Coskun, M., Tasdemir, S. (2022), "Fuzzy logic-based threat assessment application in air defense systems", *IEEE Transactions on Aerospace and Electronic Systems*, No. 59 (3), P. 2245–2251. DOI: https://doi.org/10.1109/TAES.2022.3212032.
9. Murasov, R., Nikitin, A., Meshcheriakov, I. (2024), "Mathematical model of risk assessment of the operation of critical infrastructure objects based on the theory of fuzzy logic", *Social Development and Security*, No. 14 (5), P. 166-174. DOI: https://doi.org/10.33445/sds.2024.14.5.17.
10. Хавіна, І.П., Цуранов, М.В. (2023), "Дослідження механізму нечіткої логіки для оцінки інформаційних ризиків підприємства", *Modern research in science and education*: The 4th International scientific and practical conference (Chicago, USA, December 7-9, 2023), P. 329–335. DOI: https://dspace.univd.edu.ua/handle/123456789/19547.
11. Кочетков, О.В., Гаур, Т.О., Машін, В.М. (2019), "Система оцінки ризиків інформаційної безпеки підприємства на основі нечіткої логіки", *Наукові праці ОНАЗ ім. О. С. Попова*, № 1, С. 97–104. http://nbuv.gov.ua/UJRN/Nponaz_2019_1_14.
12. Amini, A., Jamil, N., Ahmad, A.R., Sulaiman, H. (2017), "A Fuzzy Logic Based Risk Assessment Approach for Evaluating and Prioritizing Risks in Cloud Computing Environment", *Recent Trends in Information and Communication Technology Lecture Notes on Data Engineering and Communications Technologies*, P. 650-659. DOI: https://doi.org/10.1007/978-3-319-59427-9_67.
13. Tuncer, O., Cirpan, H.A. (2023), "Adaptive fuzzy based threat evaluation method for air and missile defense systems", *Information Sciences*, Vol. 643, P. 119-191. DOI: https://doi.org/10.1016/j.ins.2023.119191.
14. Bhattacharyya R., Mukherjee S. (2021), "Fuzzy Membership Function Evaluation by Non-Linear Regression", *An Algorithmic Approach, Fuzzy Information and Engineering*, No. 4, P. 412-434. DOI: https://doi.org/10.1080/16168658.2021.1911567
15. Kecman V. (2001), "Learning and Soft Computing", *Support Vector Machines, Neural Networks, and Fuzzy Logic Models, Massachusetts Institute of Technology Press, Cambridge, MA*, P. 578. DOI: https://doi.org/10.1016/S0925-2312(01)00685-3.
16. Ross T. J. (2004), "Fuzzy Logic with Engineering Applications", P. 628. DOI: https://doi.org/10.1002/9781119994374.
17. Шубін, І.Ю., Ашурова, О. (2020), "Нечіткі множини та нечітка логіка як інструмент формалізації вимог", *Інформаційні системи та технології*: матеріали 9-ї Міжнар. наук.-техн. конф., 17-20 листопада 2020 р. Харків: Друкарня Мадрид, С. 64–68. DOI: https://openarchive.nure.ua/handle/document/16161.
18. Yun, J., Hong, S.-S., Han, M.-M. (2012), "A dynamic neuro fuzzy knowledge-based system in threat evaluation", 13th International Symposium on Advanced Intelligent Systems (ISIS), P. 1601-1605. DOI: https://doi.org/10.1109/SCIS-ISIS.2012.6505178.
19. Mamdani E.H. (1974), "Application of fuzzy algorithms for the control of a simple dynamic plant", In Proc IEEE, P. 121-159. DOI: https://doi.org/10.1049/piee.1974.0328.
20. Fuzzy Inference Process https://www.mathworks.com/help/fuzzy/fuzzy-inference-process.html.
21. Петренко О.С., Петренко О.Є., Бідун А.К. (2025), "Виявлення загроз з застосуванням мережі Байєса", *Системи озброєння і військова техніка*, № 3 (83), С. 129-134. DOI: https://doi.org/10.30748/soivt.2025.83.15.
22. Kozhukhivskyi A., Kozhukhivska O. (2022), "RISK ASSESSMENT MODELING OF ERP-SYSTEMS", *Radio Electronics, Computer Science, Control*. No. 4, P. 149-161. DOI: https://doi.org/10.15588/1607-3274-2022-4-12.

Received (Надійшла) 15.11.2025
Accepted for publication (Прийнята до друку) 30.11.2025
Publication date (Дата публікації) 28.12.2025

About the Authors / Відомості про авторів

Petrenko Oleksii – PhD (Engineering Sciences), Ivan Kozhedub Kharkiv National Air Force University, Senior Research Scientist, Professor at the Department of Combat Use of GBAD Systems with Open Architecture, Kharkiv, Ukraine; e-mail: alexwgs78@gmail.com;
ORCID ID: https://orcid.org/0000-0001-9903-7388

Petrenko Olha – PhD (Engineering Sciences), Associate Professor, Kharkiv National University of Radio Electronics, Associate Professor at the Department of Information Technology Security, Kharkiv, Ukraine; e-mail: olha.petrenko@nure.ua; ORCID ID: https://orcid.org/0000-0002-7862-5399

Bidun Andrii – Ivan Kozhedub Kharkiv National Air Force University, Teacher at the Department of Combat Use of GBAD Systems with Open Architecture, Kharkiv, Ukraine; e-mail: andriybidun2@gmail.com; ORCID ID: https://orcid.org/0000-0002-4789-9397

Ostrovskyi Zakhar – Ivan Kozhedub Kharkiv National Air Force University, Full-time attendee of the Faculty of Anti-aircraft Missile Forces, Kharkiv, Ukraine; e-mail: ostrovskiyzakhar1@gmail.com; ORCID ID: https://orcid.org/0000-0002-5215-0620

Петренко Олексій Сергійович – кандидат технічних наук, Харківський національний університет Повітряних Сил ім. І. Кожедуба, старший науковий співробітник, професор кафедри бойового застосування зенітного ракетного озброєння з відкритою архітектурою, Харків, Україна.

Петренко Ольга Євгенівна – кандидат технічних наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри безпеки інформаційних технологій, Харків, Україна.

Бідун Андрій Костянтинович – Харківський національний університет Повітряних Сил ім. І. Кожедуба, викладач кафедри бойового застосування зенітного ракетного озброєння з відкритою архітектурою, Харків, Україна.

Островський Захар Назарович – Харківський національний університет Повітряних Сил ім. І. Кожедуба, слухач факультету зенітних ракетних військ, Харків, Україна.

ОЦІНЮВАННЯ РІВНЯ ТА ПРІОРИТИЗАЦІЇ БАГАТОПАРАМЕТРИЧНИХ ЗАГРОЗ ІЗ ВИКОРИСТАННЯМ АЛГОРИТМУ НЕЧІТКОЇ ЛОГІКИ МАМДАНІ ПЕРШОГО ТИПУ

Предметом дослідження є модель оцінювання загроз і визначення їх пріоритетів на основі методів нечіткої логіки. Для побудови моделі використано алгоритм Мамдані першого типу. Розроблену модель оцінювання загроз протестовано на статичному сценарії, а також на динамічних сценаріях атак у реальному часі. Поставлене питання розв'язано із застосуванням методів нечіткої логіки. Для моделювання системи використано *Fuzzy Logic Toolbox* (розширення MATLAB), що містить інструменти для проєктування систем на основі нечіткої логіки. Блок-схеми статичної та динамічної нечіткої моделі оцінювання загроз подано в застосунку *Simulink*. **Мета дослідження** – розроблення й аналіз нечіткої моделі оцінювання загроз і визначення їх пріоритетів для прийняття рішення щодо послідовності заходів з протидії цим загрозам. **Завдання роботи** передбачають обґрунтування

доцільності та ефективності застосування нечітких логічних виразів і операцій нечіткої логіки для формалізованого опису експертних вимог до визначення пріоритетів загроз. Методи нечіткої логіки широко впроваджуються в різноманітних системах управління, зокрема в таких сферах: управління нелінійними процесами, системи із самонавчанням, аналіз ризикових і критичних ситуацій, розпізнавання образів; фінансовий аналіз, дослідження інформації із корпоративних сховищ, оптимізація стратегій управління та координації дій. **Методи, використані в дослідженні:** теорія ймовірності, теорія нечіткої логіки, моделювання. **Досягнуті результати.** Розглянуто можливість застосування нечітких логічних виразів і операцій нечіткої логіки для формалізованого опису експертних критеріїв щодо визначення пріоритетності загроз. Такий підхід забезпечує отримання числових оцінок загроз на основі заданих параметрів, що сприяє точності та гнучкості в процесі їх аналізу. Обґрунтовано можливість застосування нечітких логічних виразів і операцій нечіткої логіки для формалізованого опису експертних вимог до визначення пріоритетів загроз. Це дає змогу отримати числові оцінки загроз на основі заданих вхідних параметрів, забезпечуючи точність і адаптивність у процесі аналізу. У статті запропоновано алгоритм рейтингової оцінки загроз за шкалою від 0 до 1 за допомогою системи нечіткої логіки, що сприяє точним результатам. **Висновки.** Розроблена процедура пріоритизації загроз, побудована на моделі нечітких множин, значно розширює функціональні можливості й дає змогу визначати рівні загроз. Це зі свого боку створює підґрунтя для ухвалення ефективних рішень щодо впровадження заходів із протидії цим загрозам і є основним результатом дослідження.

Ключові слова: модель; нечітка логіка; функція належності; оцінка рівня загроз; визначення пріоритетів загроз; підтримка прийняття рішень; невизначеність; лінгвістичні змінні; нечіткий висновок.

Bibliographic descriptions / Бібліографічні описи

Petrenko, O., Petrenko, O., Bidun, A., Ostrovskyi, Z. (2025), "Model for assessing the level and prioritizing multi-parameter threats using the Mamdani fuzzy logic algorithm of the first type", *Management Information Systems and Devises*, No. 4 (187), P. 220–233. DOI: https://doi.org/10.30837/0135-1710.2025.187.220

Петренко О. С., Петренко О. Є., Бідун А. К., Островський З. Н. Оцінювання рівня та пріоритизації багатопараметричних загроз із використанням алгоритму нечіткої логіки Мамдані першого типу. *Автоматизовані системи управління та прилади автоматики*. 2025. № 4 (187). С. 220–233. DOI: https://doi.org/10.30837/0135-1710.2025.187.220