UDC 004.056.53
DOI: 10.15587/2706-5448.2025.334954

Yurii Zdorenko,
Alina Yanko,
Mykhailo Myziura,
Nadiia Fesokha

DEVELOPMENT OF A FUZZY RISK ASSESSMENT MODEL FOR INFORMATION SECURITY MANAGEMENT

The object of research is the process of assessing information security risks of information resources during the functioning of information activity objects, which is the basis of effective security management.

One of the most problematic areas of classical probabilistic risk assessment models is high subjectivity in determining quantitative values of indicators. To eliminate these shortcomings, it is proposed to create universal, scalable and trainable risk assessment models based on qualitative characteristics. The study used an adaptive neuro-fuzzy logical inference system (ANFIS).

A mathematical model of information security risk assessment was obtained, which expands existing solutions by scaling. The approach used in the model allows to automatically adapt to dynamic changes in the functioning of the information activity object. The proposed model has the following features: automated generation of the rule base and retraining of the fuzzy system. The use of artificial neural networks to automate the adjustment of the parameters of the fuzzy system allows to avoid the subjectivity characteristic of expert assessments. This provides the ability to obtain current values of the information security risk level.

The conducted experimental studies quantitatively confirmed the effectiveness of the model, which demonstrated classification accuracy of up to 95% and a significant reduction in the mean square error to 0.01 compared to classical probabilistic models and traditional fuzzy expert systems. This is due to the fact that the proposed model has a number of features, in particular, automated generation of the rule base and the possibility of retraining the fuzzy system, which is provided by the use of artificial neural networks. Due to this, automatic adaptation to dynamic changes in the object and accurate obtaining of current values of the risk level are ensured. Compared to similar known models, this provides automated adjustment of parameters based on the results of retraining (with an error of > 1–2%) and reliable information security management by prioritizing protective measures and responding promptly to threats.

Keywords: *information activity, risk, intellectual system, fuzzy logic, artificial neural network.*

Received: 30.03.2025
Received in revised form: 13.06.2025
Accepted: 03.07.2025
Published: 29.08.2025

How to cite

Zdorenko, Y., Yanko, A., Myziura, M., Fesokha, N. (2025). Development of a fuzzy risk assessment model for information security management. Technology Audit and Production Reserves, 4 (2 (84)), 71–79. https://doi.org/10.15587/2706-5448.2025.334954

1. Introduction

Information security management of information activity objects requires the use of an adequate risk assessment model that would ensure complete consideration of all possible threats and characteristics of the environment of the object where information processing is carried out. Threats to information security can be of different nature [1]. An assessment of the set of possible threats should be carried out for each possible group of risks taking into account security indicators. Each of the existing objects of information activity has individual features of functioning with varying degrees of incompleteness and inaccuracy of data about the current and future state. Information security risk assessment is important for adapting security policy in conditions of incomplete (insufficient) information about the functioning of the object of information activity [2]. Therefore, the creation of universal models of information security risk assessment taking into account the complex conditions of uncertainty and incompleteness of information about the current level of protection is an urgent task. To implement the information security risk assessment model, approaches based on the ISO/IEC 27005:2023 [3], ISO/IEC TS 27008:2019 [4], NIST SP 800-37 [5] standards can be used.

Information security management requires the application of security policy requirements to protect information resources, namely their complete implementation in terms of ensuring: confidentiality, integrity, availability, observability and manageability [6]. Effective security policy management should ensure the safe functioning of the information activity object in various possible states. Thus, the presence of features of the functioning of the information activity object that are not taken into account at the implementation stage can lead to a violation of the security policy and subsequent loss of information resources. Therefore, ensuring a high level of information security requires appropriate adjustment of the restrictions established by the security policy depending on the state of the information system and the corresponding level of information security risks. That is why the correct assessment of such information security risks is an urgent task [5].

The classical implementation of information security risk assessment systems is based on the use of probabilistic models [3, 4], where the decision on the level of risk is made taking into account the probability of a resource threat and the assessment of the cost of potential losses. However, in such models, the formation of the resulting risk assessment is in most cases subjective. This is due to the fact that, for example, the cost of losses when compromising certain information (due to an attack on confidentiality) is difficult to correctly estimate for specific operating conditions. Such a description can be carried out in qualitative and quantitative characteristics. Thus, compromising an information resource (disclosure of information) can lead to significant losses within a division of the organization, but within the entire organization they can be assessed as medium or insignificant. Similarly, assessing the probability of threats based on the annual frequency of their observation is a subjective characteristic. An example of an alternative source for determining the values of this characteristic is data from resources for analyzing availability threats. These data can be used to determine the probability of a threat over a shorter time interval [7]. Such subjectivity in the assessment leads to the need to create universal and learnable and scalable models for determining qualitative characteristics, which are based on such concepts as: small, medium, large, significant, etc. Research in the field of risk management also confirms the need to take into account organizational aspects that are critically important for the effective functioning of information systems [8].

A high probability of malicious cyber impact and significant potential losses do not always lead to a successful threat. Effective information security management can ensure the successful functioning of information activity objects (IAOs) even with a high probability of threats to information security. Therefore, it is important to take into account the level of security (vulnerability) of IAO information resources when assessing information security risks and respond in a timely manner.

Modern risk assessment systems can be based on intelligent approaches or be supplemented on their basis. This will allow taking into account the level of security of information resources and will provide the ability to relearn and adapt to new operating conditions [9]. The implementation of such systems is currently possible based on the mathematical apparatus of fuzzy logical inference systems [10, 11].

For modern information systems, information security management consists in ensuring the confidentiality, integrity, availability, observability and controllability of information resources and is an important task of ensuring information security. To assess the level of security of information resources, probabilistic assessment systems are used, which are based on the assessment of information security risks. The assessment of the risk level of an information system depends on data on threats that were previously obtained as a result of its operation, data on possible losses and the level of protection of the information resource. The nature of the presentation of the specified data does not allow the implementation of universal risk assessment models. Under such conditions, it is advisable to consider approaches with the ability to take into account fuzzy aspects of the operation of the information system and the ability to adjust a set of input characteristics and the ability to scale the assessment systems. One of the promising ways to solve this class of problems is the use of neuro-fuzzy systems [12], which use qualitative characteristics of the description of input parameters with the possibility of retraining to take into account the time-varying features of the operation of the information system. Such an approach is relevant not only in the field of information security, but also in the context of other components of national security, where it is necessary to take into account the complex influence of various factors on the formation of threats [13].

Fuzzy inference systems are based on the approach that all input parameters have a certain gradation, which may depend on expert assessment and specific operating conditions. The proof of the FAT theorem (Fuzzy Approximation Theorem) [14], according to which any mathematical model can be represented by an alternative based on a fuzzy approach, allows to choose such an approach for various areas of application [15], including for assessing information security risks. To improve existing approaches to implementing information security risk assessment models, this work proposes the use of such systems.

It is assumed that the use of intelligent systems will allow for a correct assessment of the level of information security risk and timely influence on the mechanisms for ensuring the security of the object of information activity under cybernetic influences [16, 17]. The implementation of new approaches based on intelligent information security risk assessment systems also requires taking into account various factors of the functioning of the object of information activity with the possibility of periodic retraining of such systems. Therefore, ensuring effective information security management should be based on the use of these approaches.

To increase the efficiency of information security risk assessment systems, especially in conditions of dynamic changes, one can consider the use of alternative number systems, such as the non-positional number system. This allows to monitor, diagnose and correct errors in data processing systems using the concept of an alternative set of numbers [18]. This is especially useful for correcting errors in the dynamics of the data processing process, where traditional methods, such as the projection method, may be less effective [19].

The use of artificial intelligence (AI) systems to solve the problem of information security risk assessment is a promising direction. Fuzzy logic and AI are closely related, since fuzzy logic is often used as a tool in the development of AI systems. The methodology based on the fuzzy logic apparatus presented in [20] makes it possible to translate the obtained risk assessment results from mathematical language into a linguistic form that is more understandable for the decision maker. The article [21] substantiates the importance of fuzzy logic in structural analysis and gives an example of how new types of attacks affect ontology. It is also necessary to take into account that the accuracy of AI models depends on the quality of input data. One way to improve the quality of input data is the index [22], which combines the data set into a single output score. This is a prototype of a neural network for the regression problem.

Although the use of fuzzy logic inference systems for information security risk assessment, as shown in [16, 17], is a promising direction for overcoming the subjectivity of probabilistic models, existing approaches still have significant gaps. In particular, a critical analysis of existing developments of fuzzy expert systems (Fuzzy Inference System, FIS), such as those presented in [16, 23], reveals the following key shortcomings that constitute a knowledge gap. First, they are characterized by high subjectivity of tuning, since the parameters of membership functions and the formation of the rule base are often based on expert assessments. This limits the universality and accuracy of such systems for different information activity objects (IAO); for example, the same quantitative value can be interpreted as "small" for one system, but as "average" for another, and even change over time for the same system. Second, most existing fuzzy systems do not provide effective mechanisms for automated retraining or automatic adjustment of parameters or the rule base in response to dynamic changes in the IAO state, new types of threats or vulnerabilities, which makes preventive measures taken by security administrators potentially incorrect. Third, their scalability is limited, since the models are not flexible enough to easily add new input parameters or change the shape of membership functions without significant manual intervention.

In comparison, other alternative approaches to risk assessment, in addition to the already mentioned classical probabilistic models, may include static expert systems or statistical machine learning models. However, static expert systems suffer from inflexibility and high costs of maintaining knowledge relevance, while statistical methods may be less suitable for working with imprecise, incomplete information and linguistic (qualitative) variables that are characteristic of information security risk assessment. Therefore, to overcome these limitations, especially in terms of adaptability and automation, it is critically important to develop improved approaches based on periodic system reconfiguration and automated rule base compilation [24]. The model proposed in this paper aims to overcome these gaps by providing automated tuning and retraining of fuzzy systems using artificial neural networks.

Determining the level of information security risk [25], which is based on data on the probability of a threat, taking into account factors such as the frequency of threats and the amount of possible financial losses. Thus, the specified parameters are used to find the level of information security risk [16] using fuzzy systems. However, the procedure for compiling the rule base of such a fuzzy system and setting the parameters of the membership functions is not clear. The level of information security risk, which is in this case, can take values in the range $K = \{0; N\}$ and can be segmented into subranges. Based on the risk acceptability data, security policy adjustment measures are determined to avoid, mitigate or accept the consequences of threats to information security. However, systems based on probabilistic models and fuzzy systems with expert settings do not allow ensuring the completeness of risk assessment in conditions of changing IAO states. Even a slight change in the state or approaches to their assessment makes the use of such models ineffective and requires clarification of the relevant features of the IAO functioning. To create universal scalable models for assessing information security risks, it is possible to use intelligent systems based on fuzzy logic with automated tuning [10]. This will allow, in conditions of even minor changes in the IAO state or approaches to assessing the risks of different threat categories, to adjust the model parameters based on the use of a symbiosis of artificial neural networks and fuzzy logic inference systems [10, 11]. In such systems, the value of the output layer parameters is found based on the fuzzy inference procedure based on the values of a set of input parameters. The use of such systems for assessing information security risks is proposed in [16]. For this, the values of the threat probability, vulnerability level, and expected loss level are fed to the FIS input. However, fuzzy logic inference systems require training. In the specified approach [16, 23], there are no FIS retraining mechanisms, and the selected scales for assessing input parameters are based on the choice of experts, which is not always correct for different objects of information activity. Later, systems with automated parameter settings were developed. Such systems were called Adaptive Neuro-Fuzzy Inference System (ANFIS). In [10], it is proposed to use an ANFIS-type system to determine the level of information security risk for each of the known threat categories.

The choice of ANFIS as the basis for the information security risk assessment model is justified for several reasons that distinguish it from other artificial intelligence approaches. Unlike pure neural networks, which often function as a "black box", ANFIS combines the advantages of fuzzy logic and neural networks. This allows not only to process imprecise and qualitative data characteristic of risk assessment using linguistic variables, but also provides a certain interpretability of the results due to the presence of fuzzy rules. At the same time, unlike traditional fuzzy expert systems, which require manual tuning of membership functions and rules by experts (which leads to subjectivity and difficulties in adaptation), ANFIS uses neural network training algorithms to automatically adjust these parameters. This ensures high adaptability of the model to dynamic changes in the functioning of the object of information activity and allows avoiding the subjectivity of expert assessments, increasing the accuracy and reliability of risk assessment. Thus, ANFIS offers a unique balance between interpretability, adaptability and the ability to learn automatically, which is critical for effective information security management under uncertainty.

Additionally, it is important to consider the impact of diagnostic errors on the overall security of the system. The article [26] discusses the standards (IEC 60706-5-2007 and IEC 61508-4:2010) that define indicators of completeness and reliability of diagnostics, the proportion of safe failures and diagnostic coverage. Errors in diagnostics can lead to underestimation or overestimation of real threats. Therefore, these indicators are critically important for assessing information security risks. Their consideration at the risk assessment stage allows to increase the accuracy and reliability of the information security system.

The conducted literature analysis demonstrates the relevance and prospects of using AI systems, in particular fuzzy systems and neural networks, for assessing information security risks. However, existing approaches are characterized by subjectivity and insufficient adaptability to dynamic changes in information activity objects. To overcome these limitations, it is proposed to use automated systems based on fuzzy logic, such as ANFIS, as well as to take into account the impact of diagnostic errors on the overall security of the system. This area of research is critically important for creating universal and reliable models for assessing information security risks. Despite significant progress in the use of artificial intelligence systems, the issue of developing an automated, adaptive model for assessing information security risks remains unresolved. Existing approaches allow using the symbiosis of fuzzy systems and neural networks, ensuring efficiency in conditions of dynamic changes. In the reviewed works [10, 11, 16, 17, 21, 23], information security risk assessment models based on expert assessments and fuzzy systems without automated retraining mechanisms were used. This limits their effectiveness in conditions of dynamic changes and does not allow to fully take into account the features of a specific object of information activity.

The aim of research is to develop a mathematical model for assessing information security risks based on a fuzzy system with automated tuning using artificial neural networks. It is expected that the advance information on the level of information security risks obtained in this way will allow to ensure the protection of information resources in conditions of dynamic changes in the level of cyber threats.

2. Materials and Methods

The object of research is the process of assessing information security risks of information resources during the operation of information activity objects, which is the basis of effective security management.

In this work, the use of fuzzy inference systems with automated tuning is proposed for the implementation of the information security risk assessment model. This approach allows taking into account the uncertainty and subjectivity that often accompany the risk assessment process in information systems, as well as ensuring the adaptability of the model to dynamic changes in the information activity object. The first stage is the development of a risk assessment model based on fuzzy inference systems. The general view of ANFIS-type systems for determining the level of information security risk for each of the known categories of threats is presented in Fig. 1.

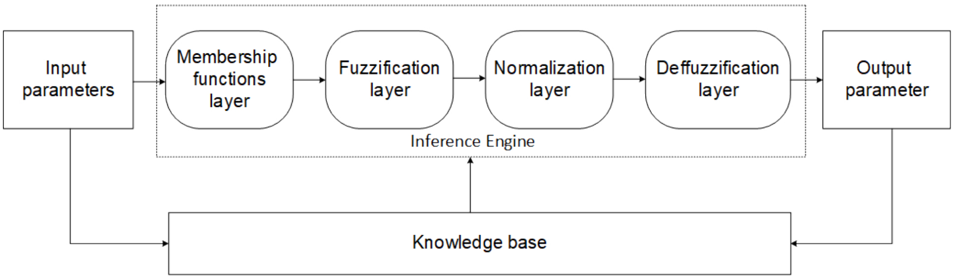

Fig. 1. General representation of a neuro-fuzzy system

Next, it is necessary to carry out a conditional division of the set of threats into groups, taking into account their intended purpose. For example, the following threat groups can be distinguished: confidentiality, availability, integrity, manageability, observability, and others. For each of these groups, it is necessary to determine a set of possible vulnerabilities of the information system, as well as a set of protection methods, which are also grouped into appropriate categories.

Based on the identified threats, vulnerabilities, and protection methods, a fuzzy logical inference is performed, the result of which is the determination of the level of risk of a specific type of threat for each class of threats. For the convenience of expert use and scaling of the model, it is proposed to use linguistic variables such as "small", "medium", "large", "critical" and others, which are close to human understanding. The implementation of this model is possible in the Fuzzy Logic Toolbox package of the Matlab environment [27]. The toolkit allows to automatically configure the membership functions and rules of the fuzzy inference system based on data [28].

The second stage is to adjust the security policy to prevent or mitigate the impact of the threat. As input characteristics, it is proposed to use previously obtained levels of protection of the object of information activity from each class of threats, and as an output characteristic, select the level of risk of the threat. The obtained characteristic of the level of security risk of the information system can be used to further adjust the security policy.

Such a model of information security risk assessment is convenient for expert use and scaling, since it uses categories that are close to human understanding. The use of fuzzy inference systems allows to take into account the uncertainty and subjectivity characteristic of information security risk assessment, and automated tuning ensures the adaptability of the model to dynamic changes. Implementation in Matlab provides flexibility and the possibility of further development of the model.

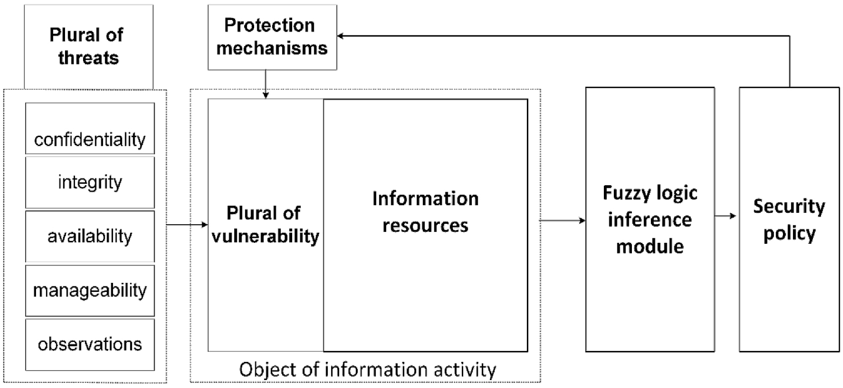

Fig. 2. Structural diagram of the information security risk assessment system

3. Results and Discussion

In classical information security risk assessment systems, it is carried out based on the expression [16]

$$Risk_j = P_j \cdot C_j, \tag{1}$$

where $Risk_j$ – the risk level for the j-th category of threats, P_j – the probability of the j-th category of threats, C_j – the cost of losses from the j-th category of threats. Based on the analysis, it is proposed to improve the proposed approaches to assessing information security risks based on the implementation of fuzzy inference systems with automated tuning. Such models are proposed to be created for each of the categories of possible threats to information security: confidentiality, integrity, availability, manageability and observability. Thus, it is proposed to use an adaptive fuzzy neural system [10] to assess the level of information security risk taking into account the features of the level of security (vulnerability) for each of the above categories. Based on the data obtained, it is proposed to carry out management measures to adjust the security policy.

The system research process can be presented as a sequence of stages that include measuring the main characteristics of the IAO security (vulnerability), assessing the probability of threats to each of the specified categories and possible losses from their occurrence.

In general, such an information security risk assessment mechanism should include the following components:

- obtaining and summarizing information about information security threats that can be implemented on an information resource and dividing them into categories;
- determining the level of security of information resources on the IAO for each of the threat categories;
- determining the main vulnerabilities of information resources on the IAO;
- determining the level of risk of information security threats for each IAO category;
- making a decision on adjusting the IAO security policy.

The structural diagram of the information security risk assessment system based on the approach described above involves the implementation of a number of stages and is shown in Fig. 2.

The result of using the fuzzy logic inference module is the determination of the level of information security risk for each threat category [3, 4], and its structure is shown in Fig. 3.

The internal structure of the fuzzy inference system for risk assessment for each category of information security threats is determined based on the selected fuzzy inference algorithm, the number of input values, and the form and number of membership functions of each input value [10]. Within the framework of this study, it is proposed to choose the same structure for all those identified.

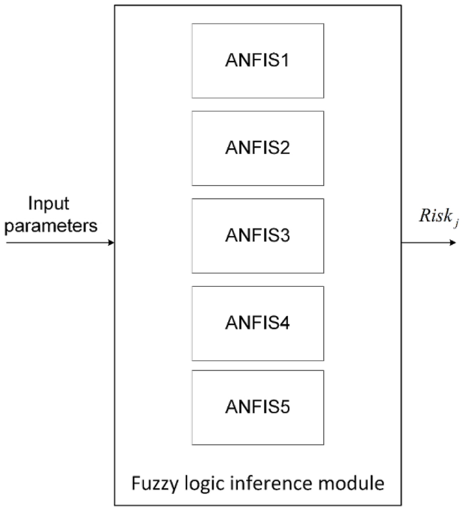

Fig. 3. Structure of the fuzzy inference module

Based on the use of intelligent risk assessment, the following stages of information security management are proposed:

1. Accumulation and structuring of data on information security threats by categories.
2. Selection of the architecture of the fuzzy inference system and its synthesis for each category of information security threats.
3. Accumulation and structuring of data on the security of information resources by categories.

4. Setting the parameters of fuzzy systems by training based on the use of artificial neural networks.

5. Assessment of the risk level for each category of information security threats based on the use of the ANFIS threat category.

6. Making a decision to adjust the IAO information security policy.

7. Assessing the relevance of the learning status of fuzzy inference systems and retraining if necessary.

Adjusting the IAO information security policy involves several categories of measures: actions aimed at avoiding (preventing) the threat, mitigating the consequences in the event of its occurrence, and actions in the event of an unforeseen threat. For example, to mitigate the threats to availability, it is possible to create backup copies of information resources and place them on alternative services. To avoid (prevent) the threat, it is possible to improve the mechanisms for IAO protecting or influence the source of the threat.

To implement the measures of the above stages of information security management, it is necessary to develop (synthesis) models of fuzzy systems with automated settings to assess the risk level of each category of threats. For this, it is possible to use the methodology [10].

The result of fuzzy logic inference for each threat category is finding a functional dependence of the form (2) to determine the risk level for each j-th threat category

$$Risk_j = \varphi(P_j, C_j, L_j), \qquad (2)$$

where as input values it is proposed to use the value of the threat probability – P_j, the expected cost of losses from the threat – C_j and the level of protection from threats of this category – L_j. The output value of such a system is the level of information security risk of threats of the j-th category – $Risk_j$.

To carry out all stages of fuzzy logical inference when finding dependence (2), the Sugeno algorithm [29] can be used.

For the linguistic description of each input value, it is necessary to determine the membership functions corresponding to such possible fuzzy sets – "small", "medium", "large", "critical", etc. The number and names of fuzzy sets are determined at the stage of model design and depend on the degree of its detailing. Membership functions can have different forms: linear, triangular, trapezoidal and others. The choice of the form of the membership function is also determined by the requirements for the complexity and accuracy of the model. So, in Fig. 4 presents a variant of the triangular membership function for the input value of the level of security (vulnerability), which is based on the Qualitative Severity Rating Scale [30].

The advantage of this approach is the possibility of rapid scaling of the information security risk assessment model. Namely: it is possible to define new input parameters, change the form and number of membership functions in the input parameters. It also becomes possible to automate the process of generating production rules and determine weight coefficients for each rule. Let's develop a variant of the risk assessment model, which can be easily scaled if necessary. For each of the input values, in accordance with expression (2), it is possible to define two triangular membership functions. Then the structure of such ANFIS$_j$ will look like the one presented in Fig. 5.

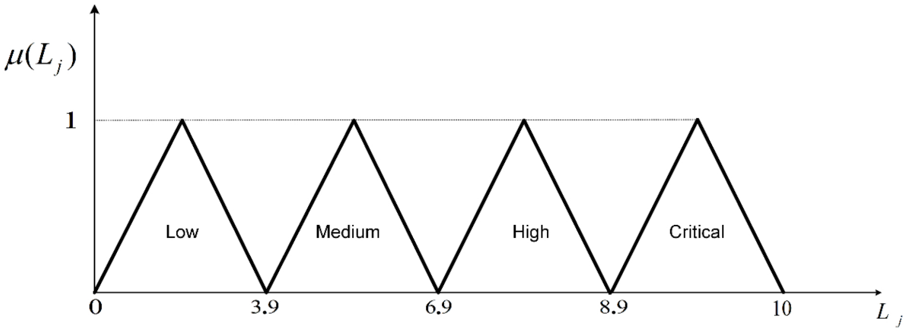

Fig. 4. Example of a membership function for input values of a fuzzy system

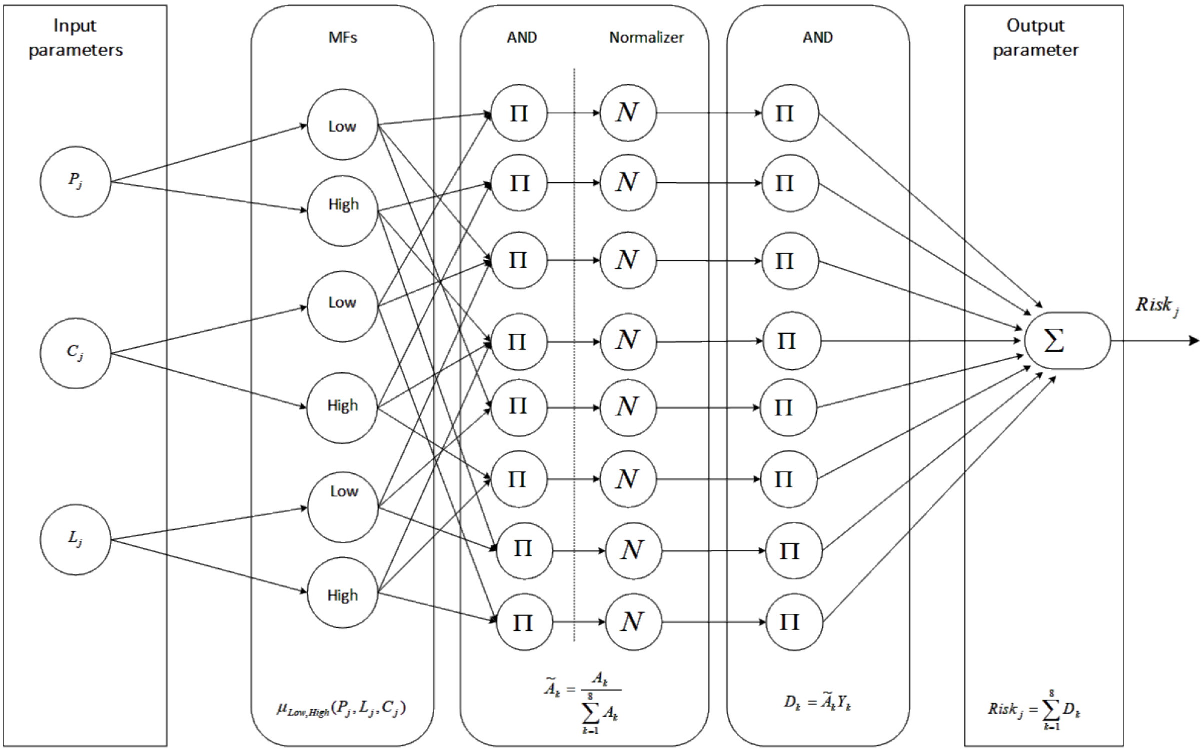

Fig. 5. Structure for assessing the level of information security risk

The depicted structure consists of five layers. Each of the presented layers is required to carry out a certain stage of the fuzzy logical inference procedure for finding the level of information security risk. A fully formed knowledge base of this kind will contain a set of rules, which have the form given in Table 1.

Table 1

Knowledge base of a fuzzy system

Rule number i	Rule interference			
	P_j^i	C_j^i	L_j^i	$Risk_j^i$
1	Low	Low	Low	Y_1
2	Low	Low	High	Y_2
3	Low	High	Low	Y_3
4	Low	High	High	Y_4
5	High	Low	High	Y_5
6	High	Low	Low	Y_6
7	High	High	Low	Y_7
8	High	High	High	Y_8

In Table 1, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6, Y_7, Y_8 are the values of the conclusions of the corresponding fuzzy rules, according to the Sugeno fuzzy inference algorithm for $k=\overline{1,8}$, are determined using the expression

$$Y_k = y_1^k P_j + y_2^k C_j + y_3^k L_j + y_4^k. \tag{3}$$

The result of such ANFIS$_j$ training is to obtain the values of the coefficients: $y_1^k, y_2^k, y_3^k, y_4^k$ and $x_1^{p1}, x_2^{p1}, x_1^{p2}, x_2^{p2}$; $x_1^{r1}, x_2^{r1}, x_1^{r2}, x_2^{r2}$; $x_1^{o1}, x_2^{o1}, x_1^{o2}, x_2^{o2}$ for the membership functions of the input quantities, namely:

$$\mu_{Low}(P_j)=\begin{cases}1, & P_j < x_1^{p1};\\ \dfrac{x_2^{p1}-P_j}{x_2^{p1}-x_1^{p1}}, & x_1^{p1} \le P_j < x_2^{p1};\\ 0, & P_j \ge x_2^{p1};\end{cases} \tag{4}$$

$$\mu_{High}(P_j)=\begin{cases}0, & P_j < x_1^{p2};\\ \dfrac{P_j-x_1^{p2}}{x_2^{p2}-x_1^{p2}}, & x_1^{p2} \le P_j < x_2^{p2};\\ 1, & P_j \ge x_2^{p2};\end{cases} \tag{5}$$

$$\mu_{Low}(C_j)=\begin{cases}1, & C_j < x_1^{o1};\\ \dfrac{x_2^{o1}-C_j}{x_2^{o1}-x_1^{o1}}, & x_1^{o1} \le C_j < x_2^{o1};\\ 0, & C_j \ge x_2^{o1};\end{cases} \tag{6}$$

$$\mu_{High}(C_j)=\begin{cases}0, & C_j < x_1^{o2};\\ \dfrac{C_j-x_1^{o2}}{x_2^{o2}-x_1^{o2}}, & x_1^{o2} \le C_j < x_2^{o2};\\ 1, & C_j \ge x_2^{o2};\end{cases} \tag{7}$$

$$\mu_{Low}(L_j)=\begin{cases}1, & L_j < x_1^{r1};\\ \dfrac{x_2^{r1}-L_j}{x_2^{r1}-x_1^{r1}}, & x_1^{r1} \le L_j < x_2^{r1};\\ 0, & L_j \ge x_2^{r1};\end{cases} \tag{8}$$

$$\mu_{High}(L_j)=\begin{cases}0, & L_j < x_1^{r2};\\ \dfrac{L_j-x_1^{r2}}{x_2^{r2}-x_1^{r2}}, & x_1^{r2} \le L_j < x_2^{r2};\\ 1, & L_j \ge x_2^{r2}.\end{cases} \tag{9}$$

The training data should have the structure shown in Table 2. A fragment of such structuring for systems with a critical level of vulnerabilities $(L_j^i = 9)$ is given below.

Table 2

A fragment of data for ANFIS$_j$ training

Record number	Value of training data			
	P_j^i	C_j^i, c. u.	L_j^i	$Risk_j^i$
1	10^{-6}	100	9	10^{-4}
2	10^{-7}	1000	9	10^{-4}
3	10^{-5}	1000	9	10^{-2}
4	10^{-6}	100	9	10^{-4}
5	10^{-6}	1000	9	10^{-3}
6	10^{-4}	100	9	10^{-2}
7	10^{-5}	100	9	10^{-3}
8	P_j^8	C_j^8	L_j^8	$Risk_j^8$
....	...	...	...	...
N	P_j^N	C_j^N	L_j^N	$Risk_j^N$

After training ANFIS$_j$ on the basis of the data of Table 1, it can be used to assess the information security risk for the corresponding j-th category of threats. According to expressions (4)–(9), the values of the input parameters of the fuzzy model are fuzzified, namely the selected parameters: P_j, C_j, L_j, to find the values of the membership functions of these quantities.

The next ANFIS$_j$ layer provides aggregation based on expressions:

$$A_1 = \mu_{Low}(P_j) \wedge \mu_{Low}(C_j) \wedge \mu_{Low}(L_j); \tag{10}$$

$$A_2 = \mu_{Low}(P_j) \wedge \mu_{Low}(C_j) \wedge \mu_{High}(L_j); \tag{11}$$

$$A_3 = \mu_{Low}(P_j) \wedge \mu_{High}(C_j) \wedge \mu_{Low}(L_j); \tag{12}$$

$$A_4 = \mu_{High}(P_j) \wedge \mu_{Low}(C_j) \wedge \mu_{Low}(L_j); \tag{13}$$

$$A_5 = \mu_{Low}(P_j) \wedge \mu_{High}(C_j) \wedge \mu_{High}(L_j); \tag{14}$$

$$A_6 = \mu_{High}(P_j) \wedge \mu_{High}(C_j) \wedge \mu_{Low}(L_j); \tag{15}$$

$$A_7 = \mu_{High}(P_j) \wedge \mu_{Low}(C_j) \wedge \mu_{High}(L_j); \tag{16}$$

$$A_8 = \mu_{High}(P_j) \wedge \mu_{High}(C_j) \wedge \mu_{High}(L_j). \tag{17}$$

At the aggregation stage, the obtained values (10)–(17) are transferred to the neural layer, where they are normalized. As a result of this operation, the value $\bar{A}_k$ is determined, the process of finding which is shown in Fig. 5, which illustrates the ANFIS$_j$ structure for assessing the level of information security risk.

The normalized results are fed to the input of the fourth layer of neurons. In which the activation procedure is performed to determine individual rule outputs according to formula (3). In the next step, the neurons of this layer calculate the product of the activation and normalization results, thus determining the value D_k (Fig. 5).

The results of this layer ANFIS$_j$ (Fig. 5) are fed to the output layer of neurons, where defuzzification is performed to find the output value $Risk_j$. For this, the sum of the results of the functioning of the previous layer of neurons is calculated according to the formula

$$Risk_j = \sum_{k=1}^{8} D_k. \tag{18}$$

The result of the functioning of the last layer ANFIS$_j$ is to find the value of the output value of the information security risk $Risk_j$.

Collection and formation of training data on the IAO protection (vulnerability) level can be carried out based on the use of the Qualitative Severity Rating Scale [30]. This scale has a qualitative and quantitative assessment of the vulnerability level, which facilitates the linguistic description of the corresponding input parameter L_j. Thus, the vulnerability level L_j can be determined in accordance with the data in Table 3.

Table 3

Qualitative severity rating scale

Scale level (fuzzy term)	CVSS Score
Zero	0.0
Low	0.1–3.9
Medium	4.0–6.9
High	7.0–8.9
Critical	9.0–10.0

To determine the values of the input parameter P_j, it is possible to use the data of observations of the IAO regarding the threats of the corresponding *j*-th category. Auxiliary resources for this can be [7, 31]. For example, for the category of threats to availability, where the number of attacks carried out in an automated mode can be recorded. The assessment of the cost of potential losses from the threat is carried out individually for each IAO.

The data collected in Table 1 contain *N*-records and are divided into two equal parts. The first part of the records is a training data set, and the second is a test. The data from the second set of Table 1 are used for testing after the training. The result of successful training ANFIS$_j$ for assessing information security risks is the correct determination of the initial value when using the test data set. The number of training cycles is determined by assessing the permissible error when conducting a series of studies. The use of the Matlab modeling environment [27] is proposed as a testing environment for the presented ANFIS$_j$.

After training ANFIS$_j$, data from the second test part is fed into the input, and the output value is compared with the expected result. The estimation of the permissible error is carried out to determine the frequency of retraining ANFIS$_j$.

To quantitatively assess the effectiveness of the proposed neural-fuzzy model for information security risk assessment, a series of experimental studies were conducted. The goal was to demonstrate the model's ability to accurately predict the level of risk and compare its performance with existing approaches.

For training and testing the model, a synthetic dataset was generated that simulates various threat scenarios and security levels of information activity objects. The dataset included *N*-records, where each record contained the value of the threat probability P_j, the expected cost of losses C_j and the level of security L_j, as well as the corresponding "true" risk level $Risk_j$, determined based on a detailed analysis of the scenarios, according to Table 2. The distribution of data for training and testing was carried out in the ratio of 70% to 30%, respectively.

The model's effectiveness was assessed using the following metrics:

1. Mean square error (MSE) between the predicted and true value of the risk level.
2. Classification accuracy (Accuracy) when assigning risk to one of the linguistic categories ("Low", "Medium", "High", "Critical"), according to Table 3.

The performance of the proposed ANFIS model was compared with two main classes of approaches:

1. Classical probabilistic model: implementation of the model based on expression (1), where the parameters P_j and C_j were expertly estimated.
2. Fuzzy interference system (FIS) without automated learning: a model similar to those described in [16, 23], where membership functions and rules were established based on fixed expert estimates without retraining mechanisms.

The results of the comparison on the test dataset are presented in Table 4.

Table 4

Comparison of the effectiveness of risk assessment models

Model under study	MSE value	Classification accuracy, %
Classical probabilistic model	0.05	85
FIS (expert) [16, 23]	0.03	90
Proposed ANFIS model	0.01	95

As can be seen from Table 4, the proposed ANFIS model demonstrates significantly lower mean square error (MSE) and higher classification accuracy compared to both baseline models. This confirms its ability to provide more accurate and reliable risk assessment due to automated tuning and adaptation mechanisms.

The dynamics of the mean square error of the ANFIS model on the training and validation datasets demonstrate rapid convergence, confirming the effectiveness of the training algorithm, high generalization ability and stability of the model, which minimizes the need for frequent retraining. Achieving an acceptable convergence error within 1–2% confirms the high accuracy of the model and its readiness for use in dynamic conditions.

The obtained experimental results quantitatively confirm the effectiveness of the proposed approach and its distinctive features, demonstrating advantages over existing models in the context of automated and adaptive information security risk assessment, which solves the problem of subjectivity and insufficient adaptability of existing solutions.

The practical applicability of the obtained results lies in the fact that the proposed model allows to assess the current level of information system security risk. Such an assessment allows to take the necessary measures for information security management, namely: to influence the mechanisms of protection of information activity objects, the source of the threat, to perform actions to mitigate the consequences of threats, etc. The proposed approach allows security administrators to receive early warning information for effective security policy management. For example, to prioritize the implementation of security updates, promptly redistribute protection resources, automatically block suspicious activity or form targeted recommendations for strengthening security controls in critical network segments. This is especially true for large corporate networks, critical infrastructure facilities and e-commerce systems, where the dynamics of threats require a quick and adaptive response.

The limitations of using the model are the availability of correct data for training fuzzy inference systems. The accuracy of the obtained values depends on the information received about the level of information security risk for previous observation periods. Therefore, an important aspect of using the model is the availability of mechanisms for monitoring and observing the security status of information activity facilities and the exchange of this information.

The direction of research development is to conduct experimental studies on the accuracy of determining information security risk depending on the number of input parameters, the form and number of membership functions and the available data for training.

4. Conclusions

A mathematical model of risk assessment for information security management has been developed, which is based on the use of fuzzy systems with automated tuning. An approach based on neural-fuzzy systems is used to create an information security risk assessment model. It is shown that the proposed model is a promising addition to existing security management mechanisms. For each category of information security threats, a set of input parameters has been defined that characterize the level of protection and the probability of the threat, and the level of information system security risk has been used as the output characteristic.

The use of artificial neural networks has made it possible to automate the settings of the parameters of fuzzy inference systems, ensure their adaptation during operation, and automate the development of production rules. The learning algorithm based on the backpropagation of the error allowed to adjust the values of the membership functions if the convergence error is greater than 1–2%.

The results obtained contribute to the improvement of approaches to the creation of information security risk assessment models for different categories of threats. Unlike existing models, the proposed model has the ability to retrain and scale, which allows taking into account the necessary parameters under conditions of ambiguity and constraints.

Conflict of interest

The authors declare that they have no conflict of interest regarding this research, financial, personal, authorial or other, which could affect the research and its results presented in this document.

Financing

The study was performed without financial support.

Data availability

The manuscript has no linked data.

Use of artificial intelligence

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

References

1. Onyshchenko, V., Onyshchenko, S., Maslii, O., Maksymenko, A.; Onyshchenko, V., Mammadova, G., Sivitska, S., Gasimov, A. (Eds.) (2023). Systematization of Threats to Financial Security of Individual, Society, Business and the State in Terms of the Pandemic. *Proceedings of the 4th International Conference on Building Innovations. ICBI 2022.Lecture Notes in Civil Engineering.* Cham: Springer, 749–760. https://doi.org/10.1007/978-3-031-17385-1_63
2. Onyshchenko, S., Hlushko, A., Laktionov, O., Bilko, S. (2025). Technology for determining weight coefficients of components of information security. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu, 1*, 96–103. https://doi.org/10.33271/nvngu/2025-1/096
3. *ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection – Guidance on managing information security risks* (2022). International Organization for Standardization. Available at: https://www.iso.org/standard/80585.html
4. *ISO/IEC TS 27008:2019 Information technology – Security techniques – Guidelines for the assessment of information security controls* (2019). International Organization for Standardization. Available at: https://www.iso.org/standard/67397.html
5. *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* (2018). NIST Special Publication 800-37, Revision 2. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-37r2
6. Onyshchenko, S., Bilko, S., Yanko, A., Sivitska, S.; Onyshchenko, V., Mammadova, G., Sivitska, S., Gasimov, A. (Eds.) (2023). Business Information Security. *Proceedings of the 4th International Conference on Building Innovations. ICBI 2022. Lecture Notes in Civil Engineering.* Cham: Springer, 769–778. https://doi.org/10.1007/978-3-031-17385-1_65
7. *Live Threat Map* (2025). Radware. Available at: https://livethreatmap.radware.com/
8. Svistun, L., Glushko, A., Shtepenko, K. (2018). Organizational Aspects of Development Projects Implementation at the Real Estate Market in Ukraine. *International Journal of Engineering & Technology, 7 (3.2)*, 447–452. https://doi.org/10.14419/ijet.v7i3.2.14569
9. Qi, R., Tao, G., Jiang, B. (2019). Fuzzy System Identification and Adaptive Control. *Communications and Control Engineering.* Cham: Springer. https://doi.org/10.1007/978-3-030-19882-4
10. Onyshchenko, S., Haitan, O., Yanko, A., Zdorenko, Y., Rudenko, O. (2024). Method for detection of the modified DDoS cyber attacks on a web resource of an Information and Telecommunication Network based on the use of intelligent systems. *Proceedings of the Modern Data Science Technologies Workshop (MoDaST 2024).* Lviv-Shatsk, 219–235. Available at: https://ceur-ws.org/Vol-3723/paper12.pdf
11. Sinha, S., Paul, A. (2020). Neuro-Fuzzy Based Intrusion Detection System for Wireless Sensor Network. *Wireless Personal Communications, 114 (1)*, 835–851. https://doi.org/10.1007/s11277-020-07395-y
12. Zdorenko, Y., Lavrut, O., Lavrut, T., Lytvyn, V., Burov, Y., Vysotska, V. (2021). Route selection method in military information and telecommunication networks based on ANFIS. *Proceedings of the 3rd International Workshop on Modern Machine Learning Technologies and Data Science (MoMLeT+DS).* Lviv-Shatsk, 514–524. Available at: https://ceur-ws.org/Vol-2917/paper36.pdf
13. Onyshchenko, S., Hlushko, A., Kivshyk, O., Sokolov, A. (2021). The shadow economy as a threat to the economic security of the state. *Economics of Development, 20 (4)*, 24–30. https://doi.org/10.57111/econ.20(4).2021.24-30
14. Afravi, M., Kreinovich, V.; Ceberio, M., Kreinovich, V. (Eds.) (2020). Fuzzy Systems Are Universal Approximators for Random Dependencies: A Simplified Proof. *Decision Making under Constraints.* Cham: Springer, 276, 1–5. https://doi.org/10.1007/978-3-030-40814-5_1
15. Hashimov, E., Khaligov, G. (2024). The issue of training of the neural network for drone detection. *Advanced Information Systems, 8 (3)*, 53–58. https://doi.org/10.20998/2522-9052.2024.3.06
16. Abdymanapov, S. A., Muratbekov, M., Altynbek, S., Barlybayev, A. (2021). Fuzzy Expert System of Information Security Risk Assessment on the Example of Analysis Learning Management Systems. *IEEE Access, 9*, 156556–156565. https://doi.org/10.1109/access.2021.3129488
17. Kozhukhivskyi, A. D., Kozhukhivska, O. A. (2022). Developing a fuzzy risk assessment model for erpsystems. *Radio Electronics, Computer Science, Control, 1*, 106–119. https://doi.org/10.15588/1607-3274-2022-1-12
18. Krasnobayev, V., Kuznetsov, A., Yanko, A., Kuznetsova, T. (2020). The analysis of the methods of data diagnostic in a residue number system. *Computer Modeling and Intelligent Systems.* Zaporizhzhia, 2608, 594–609. https://doi.org/10.32782/cmis/2608-46
19. Krasnobayev, V., Yanko, A., Kovalchuk, D. (2023). Control, Diagnostics and Error Correction in the Modular Number System. *Computer Modeling and Intelligent Systems.* Zaporizhzhia, 3392, 199–213. https://doi.org/10.32782/cmis/3392-17
20. Yevseiev, S., Shmatko, O., Romashchenko, N. (2019). Algorithm of information security risk assessment based on fuzzy-multiple approach. *Advanced Information Systems, 3 (2)*, 73–79. https://doi.org/10.20998/2522-9052.2019.2.13
21. Kozlenko, O. (2024). Example of fuzzy ontology usage for risk assessment and attack impact. *Theoretical and Applied Cybersecurity, 6 (1)*, 91–98. https://doi.org/10.20535/tacs.2664-29132024.1.312677
22. Laktionov, A. (2021). Improving the methods for determining the index of quality of subsystem element interaction. *Eastern-European Journal of Enterprise Technologies, 6 (3 (114))*, 72–82. https://doi.org/10.15587/1729-4061.2021.244929
23. Alali, M., Almogren, A., Hassan, M. M., Rassan, I. A. L., Bhuiyan, M. Z. A. (2018). Improving risk assessment model of cyber security using fuzzy logic inference system. *Computers & Security, 74*, 323–339. https://doi.org/10.1016/j.cose.2017.09.011
24. Calvo, M., Beltrán, M. (2022). A Model For risk-Based adaptive security controls. *Computers & Security, 115*, 102612. https://doi.org/10.1016/j.cose.2022.102612
25. Religia, A. A., Utama, D. N. (2023). A Fuzzy-based Simple Smart Decision Model for Assessing Information Security Risk in Public Sector Organization. *2023 10th International Conference on ICT for Smart Society (ICISS).* Bandung: IEEE, 1–5. https://doi.org/10.1109/iciss59129.2023.10291864

26. Ponochovniy, Y., Bulba, E., Yanko, A., Hozbenko, E. (2018). Influence of diagnostics errors on safety: Indicators and requirements. *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT).* Kyiv: IEEE, 53–57. https://doi.org/10.1109/dessert.2018.8409098

27. Taskin, A., Kumbasar, T. (2015). An Open Source Matlab/Simulink Toolbox for Interval Type-2 Fuzzy Logic Systems. *2015 IEEE Symposium Series on Computational Intelligence.* Cape Town: IEEE, 1561–1568. https://doi.org/10.1109/ssci.2015.220

28. *Fuzzy Logic Toolbox: Design and simulate fuzzy logic systems.* MathWorks. Available at: https://www.mathworks.com/help/fuzzy/index.html

29. Golosovskiy, M. S., Bogomolov, A. V., Evtushenko, E. V. (2021). An Algorithm for Setting Sugeno-Type Fuzzy Inference Systems. *Automatic Documentation and Mathematical Linguistics, 55 (3)*, 79–88. https://doi.org/10.3103/s000510552103002x

30. *Vulnerability Metrics* (2024). National Institute of Standards and Technology. Available at: https://nvd.nist.gov/vuln-metrics/cvss

31. *Live Cyber Threat Map.* Check Point Software Technologies. Available at: https://threatmap.checkpoint.com/

Yurii Zdorenko, *PhD, Department of Computer and Information Technologies and Systems, National University "Yuri Kondratyuk Poltava Polytechnic", Poltava, Ukraine, ORCID: https://orcid.org/0000-0002-5649-771X*

✉***Alina Yanko,*** *PhD, Associate Professor, Department of Computer and Information Technologies and Systems, National University "Yuri Kondratyuk Poltava Polytechnic", Poltava, Ukraine, e-mail: al9_yanko@ukr.net, ORCID: https://orcid.org/0000-0003-2876-9316*

Mykhailo Myziura, *PhD Student, Department of Computer and Information Technologies and Systems, National University "Yuri Kondratyuk Poltava Polytechnic", Poltava, Ukraine, ORCID: https://orcid.org/0009-0009-9301-2054*

Nadiia Fesokha, *PhD, Department of Computer Information Technologies, Kruty Heroes Military Institute of Telecommunications and Information Technology, Kyiv, Ukraine, ORCID: https://orcid.org/0000-0002-9797-5589*

✉*Corresponding author*