e-ISSN 1607-3274 Радіоелектроніка, інформатика, управління. 2022. № 1
p-ISSN 2313-688X Radio Electronics, Computer Science, Control. 2022. № 1

UDC 004.94

DEVELOPING A FUZZY RISK ASSESSMENT MODEL FOR ERP-SYSTEMS

Kozhukhivskyi A. D. – Dr. Sc., Professor, Professor Department of Information and Cybernetic security of State University of Telecommunications, Kyiv, Ukraine.

Kozhukhivska O. A. – Dr. Sc., Associate Professor Department of Information and Cybernetic security of State University of Telecommunications, Kyiv, Ukraine.

ABSTRACT

Context. Because assessing information security risks is a complex and complete uncertainty process, and uncer-tainties are a major factor influencing valuation performance, it is advisable to use fuzzy methods and models that are adaptive to non-calculated data. The formation of vague assessments of risk factors is subjective, and risk assessment depends on the practical results obtained in the process of processing the risks of threats that have already arisen during the functioning of the organization and experience of information security professionals. Therefore, it will be advisable to use models that can adequately assess fuzzy factors and have the ability to adjust their impact on risk assessment. The greatest performance indicators for solving such problems are neuro-fuzzy models that combine methods of fuzzy logic and artificial neural networks and systems, i.e. "human-like" style of considerations of fuzzy systems with training and simulation of mental phenomena of neural networks. To build a model for calculating the risk assessment of information security, it is proposed to use a fuzzy product model. Fuzzy product models (Rule-Based Fuzzy Models/Systems) this is a common type of fuzzy models used to describe, analyze and simulate complex systems and processes that are poorly formalized.

Objective. Development of the structure of a fuzzy model of quality of information security risk assessment and protection of ERP systems through the use of fuzzy neural models.

Method. To build a model for calculating the risk assessment of information security, it is proposed to use a fuzzy product model. Fuzzy product models are a common kind of fuzzy models used to describe, analyze and model complex systems and processes that are poorly formalized.

Results. Identified factors influencing risk assessment suggest the use of linguistic variables to describe them and use fuzzy variables to assess their qualities, as well as a system of qualitative assessments. The choice of parameters is substantiated and the structure of the fuzzy product model of risk assessment and the basis of the rules of fuzzy logical conclusion is developed. The use of fuzzy models for solving problems of information security risk assessment, as well as the concept and construction of ERP systems and analyzed problems of their security and vulnerabilities are considered.

Conclusions. A fuzzy model has been developed risk assessment of the ERP system. Selected a list of factors affecting the risk of information security. Methods of risk assessment of information resources and ERP-systems in general, assessment of financial losses from the implementation of threats, determination of the type of risk according to its assessment for the formation of recommendations on their processing in order to maintain the level of protection of the ERP-system are proposed. The list of linguistic variables of the model is defined. The structure of the database of fuzzy product rules – MISO-structure is chosen. The structure of the fuzzy model was built. Fuzzy variable models have been identified.

KEYWORDS: information security, fuzzy logic, risk assessment, security, ERP-system.

ABBREVIATIONS

ANFIS is an Adaptive Network-based Fuzzy Inference System;

DB is a Database;

DSTU is a State standard of Ukraine;

ERP is a Enterprise Resources Planning;

ERP-System is an Enterprise Recourses Planning System;

MISO is a Structure (Multi Inputs – Single Output);

FIS is a Fuzzy Inference System;

ARL is an acceptable risk level;

MRL is a middle risk level;

HRL is a high-risk level;

VLR is a very low risk;

LR is a low risk;

AR is an average risk;

HR is a High risk;

VHR is a Very high risk;

CVSS is a Common Vulnerability Scoring System;

NVD is a National Vulnerability Database;

CVE is a Common Vulnerabilities and Exposures.

NOMENCLATURE

R_{ij} is a Risk of the *i*-th resource in the implementation of the *j*-th threat;

A_{ij} is a Expected loss from the onetime implementation of the *j*-th threat to for the *i*-th resource;

P_j^t is a probability of occurrence of *j*-th threat;

P_{ij}^v is a Vulnerability of the *i*-th resource to the *j*-th threat;

IR is a Resource set of system;

Th is a A set of threats to the system.

A_i^V is a Value of the ist resource;

F_{ij}^e is a Impact consequences in the implementation of the *j*-th threat on the *i*-th resource, or the propensity of the *i*-th resource to the *j*-th threat;

R_i is a Risk of the *i*-th resource in the implementation of threats;

R_{ik} is a Risk of the *i*-th resource in the implementation of the *k*-th threat;

DOI 10.15588/1607-3274-2022-1-12

Th_i is a set of risks for the *i*-th resource;

R_g is a General system risk;

R_{ig} is a risk of the *i*-th resource at general system risk;

FL_i is a financial loss of the *i*-th resource;

R_i is a risk of the *i*-th resource;

Co_i is a cost of the *i*-th resource;

FL is a Total financial loss;

RL is a Risk level type;

$\min_R$ is a Minimum value of risk assessment;

$\max_R$ is a Maximum value of risk assessment;

$\Pr_1$ is a parameter, maximum value of risk assessment of acceptable type;

$\Pr_2$ is a parameter, the maximum value of the risk assessment of the average type;

$x_j (j=1,\cdots,m)$ is an Incoming Variables (can be either clear or fuzzy);

$x_j \in X_j$, X_j is an The definition area appropriate prerequisites;

y is a Fuzzy output variable;

$y \in Y, Y$ is a the definition area the conclusion;

A_{ij}, B_i is a fuzzy sets defined that are defined by X_j and Y with affiliation functions $\mu_{A_{ij}}(x_j) \in [0;1]$ and $\mu_{B_i}(y) \in [0;1]$ respectively;

p_i, q_i, r_i is a Affiliation functions options;

$k=1,\cdots,K$ is a an example from many examples of training sampling;

$x_1^{(k)}, x_2^{(k)}, \cdots, x_m^{(k)}$ are Input variable values $x_1, x_2, \cdots, x_m$;

$y^{(k)}$ is a reference value of the source variable *y* in the *k*-th example;

K is a he total number of examples, size of Training sample;

$E^{(k)}$ is a error *k*-th example from many examples of educational sample;

E is a Error;

$y^{1(k)}$ is a Installed the value of the source variable y in the *k*-th example;

ε is a installed threshold;

C is a Assessment of the criticality of information;

$C_{CC} = \max(CC_I, CC_p, CC_A, CC_O)$ are Assessment of the consequences of violations of integrity, confidentiallity, accessibility and observation for the commercial interests of the organization;

$C_{MC} = \max(MC_I, MC_p, MC_A, MC_O)$ are Assessment of the consequences of violations of integrity, confidentiality, accessibility and observation for the operational activities of the organization;

$C_R = \max(R_I, R_p, R_A, R_O)$ are Assessment of the consequences of violations of integrity, confidentiality, accessibility and observation for the organization's relationship with customers and partners.

INTRODUCTION

The basis of activity of any organization is business processes, which are determined by the goals and objectives of the entity. The business process broadly understands the structured sequence of actions to perform a certain type of activity at all stages of the life cycle of the subject of activity. Each business process has a start (login), output, and sequence of procedures that ensure that operations are grouped by the appropriate types. In general, the calculation of the risks of information security of ERP-systems should be carried out in relation to each critical business process and only on those vulnerabilities that are relevant to a particular business process, and it should be borne in mind that a number of vulnerabilities may be the same for all business processes.

Each vulnerability in the current list of vulnerabilities is correlated by a threat, the terms of which could be this vulnerability, and for each specified pair, an assessment of the probability of its occurrence and assessment of the impact of the implementation of this pair on the integrity, confidentiality, accessibility and observability is carried out.

We will use the following definitions. Probability is a conditional number that determines the likely frequency of steam threat/vulnerability. Privacy is a property of information that is that information cannot be obtained by an unauthorized user and/or process. Integrity is a property of information, which is that information cannot be modified by an unauthorized user and/or process. System integrity – system property, which is that none of its components can be eliminated, modified or added in violation of security policy. Accessibility – the property of the system resource, which is that the user and/or process, which has the appropriate powers, can use the resource in accordance with the rules established by the security policy, without waiting longer for a specified (small) period of time, that is, when it is in the form required by the user, in the place required by the user, and at the time when it is necessary. Observation – system property, which allows to record the activities of users and processes, the use of passive objects, as well as to unequivocally establish identifiers of users involved in certain events and processes in order to prevent violations of security policies and/or to ensure liability actions.

The object of the study is the development of the structure of a fuzzy model of the ERP system.

The subject of the study is neuro-fuzzy models that combine methods of fuzzy logic and artificial neural networks and systems.

DOI 10. 15588/1607-3274-2022-1-12

The purpose of the work is to improve the quality of assessment of information security risks and protection of ERP systems through the use of fuzzy neural models.

1 PROBLEM STATEMENT

Security risk assessment is an important element in the overall security risk management process, which is the process of ensuring that the organization's risk position is within acceptable limits defined by senior management and consists of four main stages: security risk assessment, testing and supervision, mitigation effects and operational security [1].

Risk managers and organizers use risk assessment to determine which risks to reduce through control and which to accept or transfer. Information security risk assessment is a process of identifying vulnerable situations, threats, the likelihood of their occurrence, the level of risks and consequences associated with organing assets, as well as control that can mitigate threats and their consequences. This process includes: assessing the likelihood of threats and vulnerabilities that are possible; calculation of the impact that can be a threat to each asset; determination of quantitative (measurable) or qualitative (described) cost of risk.

Table 1 describes the classification of technologies according to the approach used in risk assessment.

Assessment of information security risks can be divided into three stages (see Table 2): identification of risk; risk analysis; evaluation of results.

Risk assessment includes seven steps: identification of system protection facilities; identification of the threat; identification of vulnerability; control analysis; determination of probability; analysis of consequences; identification of risk.

The full risk assessment process should also include two more steps: recommendations for controlling and documenting the results.

Information risk assessment can be performed using a variety of technologies, documents or software tools. The methodology for assessing information security risks understands the systematized sequence of actions (step-by-step instructions) to be done and the tool (software product) for risk assessment at the enterprise.

Also, to assess security risks, manager documents containing theoretical descriptions can be used and provide guidelines on the risk assessment process, but no specific technologies for their implementation are provided [2–6]. At present, the following standards apply on the territory of Ukraine: ISO 27001, ISO 27002, ISO 27003, ISO 27004 and ISO 2700.

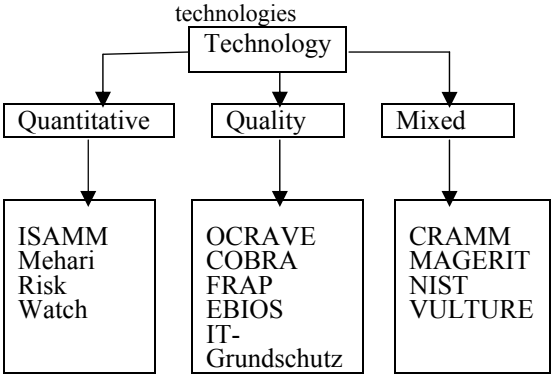
Recently, quite intensively developing methods of analysis and risk assessment, which are based on elements of fuzzy logic. Such methods allow to change the approximate table methods of rough assessment of risks to mathematical method, as well as significantly expand the possibilities of mathematical methods of risk analysis [7–11].

The mechanism of risk assessment with the help of fuzzy logic in general represents the expert system. The knowledge base of such a system complies with the rules that reflect the logic of the relationship between the input values of risk factors and the level of risk. In the simplest case, this logic is described in the table. In general, much more complex logic is used, which is designed to more accurately reflect the real relationship of factors and consequences. Such connections are formalized and described by the production rules of the "if-something" type. In addition, the mechanism of fuzzy logic involves forming levels of factor assessments and presenting them in the form of fuzzy variables. The process of forming this type of assessments in general is quite complex, because it requires a large number of sources of information, taking into account their quality and use of expert experience.

2 REVIEW OF THE LITERATURE

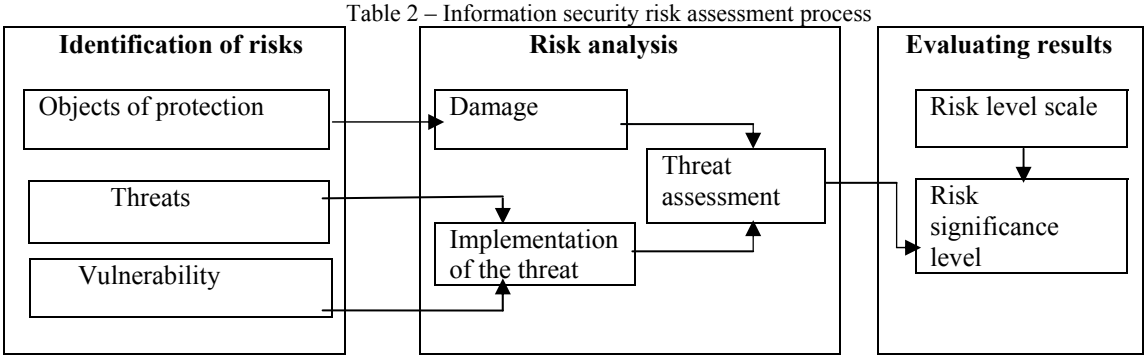
The security risk analysis study begins in the mid-1980s, and in the early 90s R. Baskerville identified risk analysis checklists for tools used to design information system security measures [11]. Over time, complex tools are developed to analyze risks, such as: Facilitated Risk Assessment Process [12]; The Operationally Critical Threat, Asset, and Vulnerability Evaluation) [13]; CORAS [14]; Is Risk Analysis Based on Business Model [15]; Information Security Risk Analysis Method [16]; Risk Watch method [17]; Consultative Objective and Bifunctional Risk Analysis [18]; CRAMM [19].

Table 1 – Information security risk assessment technologies



DOI 10. 15588/1607-3274-2022-1-12

Table 2 – Information security risk assessment process



Also, since the early 2000s, some other methods of modeling security risks, which have provided good indicators and have been commonly titled "soft computing models", including the grey relactional approach, have also been used in the research industry, Fuzzy number arihmetic, Information entropy, Fuzzy weighted average aproach, Fuzzy measure and Evidence theory, fuzzy Analysis of Hierarchy Process method.

The development and application of soft computing and hybrid models are considered to be modern areas of research to assess information security risks.

Soft computing components include: Neural networks – computational systems that assess the risks of information security through similar functioning of biological neural networks and learning tasks (gradually improving their performance of these networks), considering examples, in general, without special programming for the task; Rough sets – an effective mathematical analysis tool to address uncertainty in the field of solution analysis; Grey sets; Fuzzy systems – based on the algorithm for obtaining fuzzy conclusions based on fuzzy preconditions; Generic algorithms belong to the largest class Evolutionary algorithms and generate solutions to optimization problems using methods borrowed from the theory of evolution, such as inheritance, mutation, selection and crossover; Support vector machine – the data analysis method for classification and regression analysis using managed learning models is used when input is either not defined or when only some data is determined by their preprocessing; Bayesian network – used to identify cause and effect relationships of risk factors and predict the likelihood of security risk.

Hybrid models represent a combination of two or more technologies to develop robust risk assessment and information systems. The most common hybrid model is the neuro-fuzzy network.

To determine the level of risk, it is advisable to use the apparatus of the theory of fuzzy sets, which allows you to describe vague concepts and knowledge, operate them and draw vague conclusions. The theory of fuzzy sets is used precisely to solve problems in which inputs are unreliable and poorly formalized, as in the case of the problem solved in this work. To assess the risk, it is appropriate to use the mechanism of a vague logical conclusion – obtaining a conclusion in the form of a fuzzy set corrtsponding to the current values of input variables, using a fuzzy knowledge base and fuzzy operations.

There are developed models of fuzzy conclusion of Mamdani, Sugeno, Larsen, Tsukamoto [20]. Most often, Mamdani and Sugeno algorithms are used in practice. The main difference between them is the way to set the values of the source variable in the rules that constitute the knowledge base. In systems like Mamdani, the values of input variables are set by fuzzy terms, in systems like Sugeno – as a linear combination of input variables. For tasks in which identification is more important, it is ad.

3 MATERIALS AND METHODS

To build a structure a model for calculating information security risk assessment, it is proposed to use Rule-Based Fuzzy Models/Systems.

Under the Rule-Based Fuzzy Models/Systems understand the agreed a lot of individual fuzzy product rules of the type "if A, then B" where A is the prerequisite (parcel, antecendent) of a certain rule, and B – the conclusion (action, consecvent) of the rule in the form of fuzzy statements. The model is designed to determine the degree of truthfulness of the conclusions of fuzzy product rules. The degree of truth is determined on the basis of preconditions with a certain degree of truthfulness of the relevant rules.

When building a fuzzy product model, the following components are determined: method of fuzzy withdrawal of conclusions; database of fuzzy product rules; fuzzyfication input procedure; procedure aggregation of the degree of truthfulness of preconditions for each of the fuzzy product rules; activation procedure for each of the fuzzy product rules; the procedure of liquidation of activated conclusions of all fuzzy product rules according to each output variable; defuzzyfication procedure to clarity on each consiluled output variable; the procedure for parameters optimization of the final base of fuzzy rules.

At present, many different types of fuzzy product models are offered on the basis of different combinations of these components.

Rule-Based Fuzzy Models/Systems are used in solving a number of problems in which information about the system, its parameters, as well as the inputs, outputs and states of the system is unreliable and poorly formalized. Together with the advantages of describing the model in a language close to natural, in the versatility and efficiency of the model, Rule-Based Fuzzy Models / Systems are characterized by certain disadvantages: the wording of the original set of fuzzy rules is carried out with

DOI 10. 15588/1607-3274-2022-1-12

the help of an expert, so it may be incomplete or contradictory; the choice of the type and parameters of the functions of belonging in fuzzy statements of the rules is subjective; automatic acquisition of knowledge cannot be performed.

To eliminate these shortcomings, it is proposed to use an adaptive fuzzy production model, which in the process and on the results of functioning corrects both the composition of the rules in the base and the parameters of the functions of belonging, as well as to implement various components of this model on the basis of neuronet technology.

Determine the incoming and outgoing parameters of the model.

To build a risk assessment calculation model, we will use the risk factor ratio according to the formulas (1, 2) [10].

$$R_{ij} = A_{ij} \cdot P_j^t \cdot P_{ij}^v,\ i \in IR,\ j \in Th. \quad (1)$$

Under the expected damage from a one-time implementation of the threat we understand the cost (or value) of the asset, which is mathematically expressed as follows:

$$A_{ij} = A_i^V \cdot F_{ij}^e, i \in IR,\ j \in Th. \quad (2)$$

Taking into account (1) and (2), we obtain the general ratio of factors for risk assessment:

$$R_{ij} = A_i^V \cdot F_{ij}^e \cdot P_j^t \cdot P_{ij}^V, i \in IR,\ j \in Th. \quad (3)$$

Since many risks can be identified for each information resource (one to all), the assessment of the total risk by the information resource will be defined as the maximum risk assessment of the resource:

$$R_i = \max(R_{ik}),\ k \in Th_i. \quad (4)$$

In turn, the assessment of system risk will be defineed as the maximum assessment among resource risk assessments:

$$R = \max(R_i),\ i \in IR. \quad (5)$$

The amount of financial damage for the information resource will be determine as the product of the risk of the information resource on the cost of the resource:

$$FL_i = R_i \cdot Co_i,\ i \in IR. \quad (6)$$

In turn, the total financial loss will be determined as the amount of financial losses on all resources:

$$FL = \sum_i FL_i,\ i \in IR. \quad (7)$$

We will apply a linguistic approach to the description of information security risk factors. Suppose as the values of factors and characteristics of relations between them not only quantitative assessment, but also qualitative, sentences of natural language. Then this approach will provide a quantitative description of the elements of the model in the conditions of vague information about the value of the risk level, the cost of the resource, the impact of the consequence of, the likelihood of a threat, the vulnerability of resource protection and ways to avoid negative impact from the implementation of risks.

Each risk factor of information security and the risk itself will be described by linguistic variables $X \in \overline{X}$, Wheel the set of linguistic variables of the model $\overline{X}$ is: $\overline{X}$ = {“Resource Price”, “Impact of the consequence”, “Probability the emergence of Threat”, “Resource Vulnerability”, “Risk”}.

The list of linguistic variables of the model corresponding to the risk factors is shown in Table 3.

Thus, information security risk assessment can be expressed as:

$$Y = f_Y(X_1, X_2, X_3, X_4).$$

Based on the analysis [21] and the formed ratio of risk factors (3) for the assessment of each of the risks, a fuzzy model with four input parameters (X_1, X_2, X_3, X_4) and one Y output (MISO structure [22]) is proposed. The number of input parameters is selected according to the number of factors influencing the degree of risk (3). Table 3 shows the structure of the system of fuzzy conclusions for the selected model.

Table 3 – The list of linguistic variables of the model

List	Name of linguistic variable
X_1	Resource Price
X_2	Impact of the consequence
X_3	Probability the emergence of Threat
X_4	Resource Vulnerability
Y	Risk

To maintain the level of security of the ERP system, it is necessary to determine what risks, according to the level of their assessment – risk level (RL), require processing according to certain recommendations. To do this, we will introduce 3 types of risk levels:

– acceptable risk – ARL – will be considered insignificant, the processing of such a risk is not required;

– medium risk – MRL – recommended for processing in order to minimize it;

– high risk-HRL – we will consider it essential and its processing is mandatory.

Determination of the type of risk will be carried out as follows:

DOI 10. 15588/1607-3274-2022-1-12

$$RL=\begin{cases} ARL, R_{ij}\in(\min_R;\Pr_1); \\ MRL, R_{ig}\in(\Pr_1;\Pr_2); \quad i\in IR, j\in Th, \\ HRL, R_{ij}\in(\Pr_2;\max_R). \end{cases} \tag{8}$$

Parameters – the maximum value of the assessment of acceptable and medium risk – $[\Pr_1]$ and $[\Pr_2]$ respectively – are set by experts.

The scheme for processing the result of risk assessment is shown in Table 4.

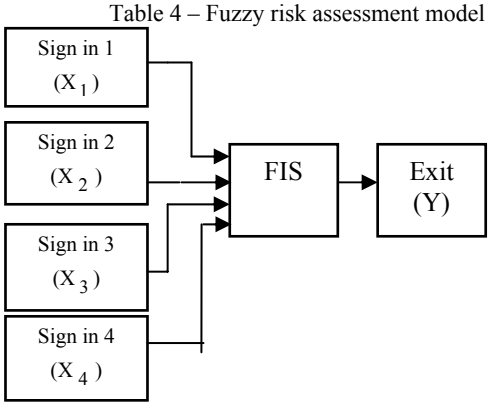
We will create a structure and build bases of fuzzy product rules.

The structure of the rules should correspond to the structure of the model, namely the number of fuzzy statements in the prerequisites and conclusions. The database of rules that has the structure of MISO, in general, has the following rule structure [22].

$$\text{P}_i: \text{If } x_1 \text{ is } A_{i1} \text{ and } \ldots \text{ and } x_j \text{ is } A_{ij} \text{ and } \ldots \text{ and } x_m \text{ is } A_{im}, \text{ then } y \text{ is } B_i. \tag{9}$$

When creating a fuzzy product model, both a priori data coming from experts and data obtained as result of measurements can be used.

Table 4 – Fuzzy risk assessment model



In the first case, if there is no need to agree on the opinions of experts, it is assumed that the tasks of ensuring completeness and inconsistency of the database of fuzzy rules are solved in advance. If only experimental data are known, these tasks can be attributed to the tasks of system identification. In practice, there may also be a mixed case when the initial database of fuzzy rules is built on the basis of heuristic assumptions, and its clarification is carried out using experimental data.

ANFIS, the adaptive network fuzzy output system proposed by Chang in 1992, will be used to represent the fuzzy production model and algorithm of fuzzy output in the form of a fuzzy product network [23].

Since the fuzzy ANFIS product network is presented as multilayer structure with a direct signal propagation, and the value of the source variable can be changed by adjusting the parameters of layer elements, then to teach this network you can use an algorithm for reverse spread ing the error, which belongs to the class of classic gradient algorithms.

Consider the problem of fuzzy neural production network of anfis type, which implements the algorithm of fuzzy output of Takagi-Sugeno [24] (see Figure 1).

Let the rules of this form be set:

P1: If x_1 is A_{11} and x_2 is A_{12} then $y_1 = a_1 x_1 + b_1 x_2$;

P2: If x_1 is A_{21} and x_2 is A_{22} then

$$y_2 = a_2 x_1 + b_2 x_2. \tag{10}$$

The structure of the fuzzy neural production network of ANFIS type, which implements the algorithm of fuzzy output of Takagi-Sugeno (according to the example) is shown in Fig. 2 [23].

Layer 1. The outputs of the elements of this layer are $\mu_{A_{ij}}(x_j)$ the values of the functions of the affiliation at specific (specified) values of input variables. For example, circular functions hare the form of:

$$\mu_{A_{ij}}(x_j) = \exp\left[-\frac{1}{2}\left(\frac{x_j - a_{ij}}{b_{ij}}\right)^2\right]. \tag{11}$$

Layer 2. Elements of the second layer perform aggregation of the truth levels of the prerequisites of each base rule in accordance with the T-norm operation, which uses the operation minimum (4) [20] according to the rules:

$$\begin{aligned} a_1 &= \min\{A_{11}(x_1), A_{12}(x_2)\}, \\ a_2 &= \min\{A_{21}(x_1), A_{22}(x_2)\}. \end{aligned} \tag{12}$$

Layer 3. Elements of this layer normalize and lead these results to a type convenient for calculating the output of a fuzzy network. Calculation β_i -normalized values α_i are performed as follows:

$$\beta_1 = \frac{\alpha_1}{\alpha_1+\alpha_2}, \beta_2 = \frac{\alpha_2}{\alpha_1+\alpha_2}. \tag{13}$$

Layer 4. Elements in this layer calculate function values:

$$\begin{aligned} y_1^{/} &= (p_1 x_1 + q_1 x_2 + r_1), \\ y_2^{/} &= (p_2 x_1 + q_2 x_2 + r_2). \end{aligned} \tag{14}$$

Layer 5. Elements of this layer allow you to form a defaziated value at the output of the network, which is formed as follows:

$$y^{/} = \beta_1 y_1^{/} + \beta_2 y_2^{/}. \tag{15}$$

DOI 10. 15588/1607-3274-2022-1-12

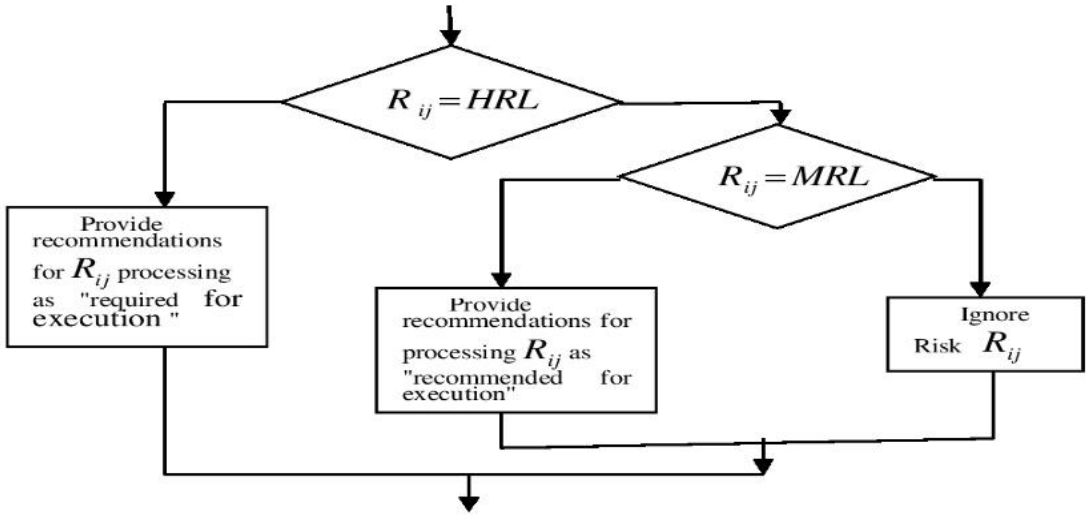


Figure 1 – Scheme for processing the result of risk assessment

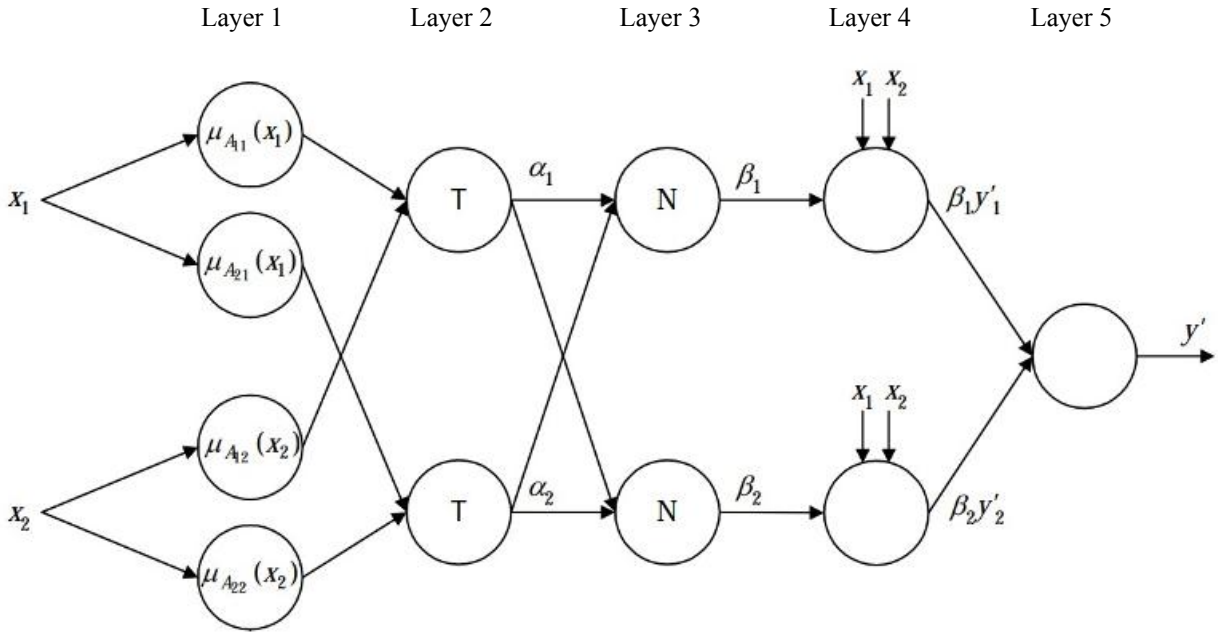


Figure 2 – The structure of the fuzzy ANFIS neural production network, which implements the Sugeno fuzzy output algorithm

Parametric layers fuzzy ANFIS neural production network, that is, the layers, the parameters of the elements in which will be adjusted during the learning process, are the first and fourth, and the parameters configured in the learning process are:

– in the first layer – nonlinear parameters of the affiliation functions $\mu_{A_{ij}}(x_j)$ fuzzy sets of preconditions of the rules;

– in the fourth layer – nonlinear parameters p_i, q_i, r_i affiliation functions $\mu_{B_i}(y)$ fuzzy sets of rule conclusions.

The Picks for learning the network consists of many examples and has the form of:

$$(x_1^{(k)}, x_2^{(k)}, \cdots, x_m^{(k)}, y^{(k)}). \qquad (16)$$

Since the fuzzy ANFIS product network is presented as multilayer structure with a direct signal propagation, and the value of the source variable can be changed by adjusting the parameters of layer elements, then to study this network we use an algorithm for reverse spreading the error, which belongs to the class of gradient algorithms.

Network training continues (iteratively repeats the procedure for adjusting the values of all parameters) as long as [21]:

– or the error function value for each sample example does not exceed some set threshold:

$$E^{(k)} < \varepsilon, k = 1, \cdots, K. \qquad (17)$$

DOI 10. 15588/1607-3274-2022-1-12

– or assessment of the average total error of a fuzzy product model, taking into account all examples of the educational sample does not exceed some established threshold:

$$E = \frac{1}{k}\sum_{k=1}^{K}(y^{/(k)} - y^{(k)})^2 < \varepsilon. \quad (18)$$

4 EXPERIMENTS

Let's define a linguistic variable Y "Risk". To evaluate the linguistic variable Y, we will use the term set T(Y) of five quality thermals: $T(Y)$={"Very level risk (VLR); "Low risk (LR) "; "Average risk (AR)"; "High risk HR)"; "Very high level of risk (VHR)"}.

Definition Area of E_Y of the linguistic variable Y will be set at the interval [0,100]. Table 5 shows the scale for assessing the level of risk.

Taking into account the selected area of determining the risk assessment of information security when determining the type of risk to make recommendations for its reducti-on according to the formula (6), we will use the following values:

Table 5 – Y Risk Assessment Scale

Risk assessment	Risk level
0–20	VLR
20–40	LR
40–60	MR
60–80	HR
80–100	VHR

$\min_R = 0, \max_R = 100.$

Consider the definition identifying threats and assessing the likelihood of threats. The main security threats of ERP systems include deliberate actions of violators, for example, criminals, spies, saboteurs, or offended persons from among the personnel of the organization [25].

1. According to the results of the actions of violators:

– threat of information leakage;

– threat of information modification; – threat of loss of information.

2. Based on the motives of the violators: unintentional; deliberate.

According to the Normative Document in the Field of Technical Information Protection (GNI TZI) 2.5-004-99 [25] in the risk assessment model we will consider threats of the following four types in accordance with the properties of information security:

– threats related to unauthorized acquaintance with information and pose threats to the confidentiality of information;

– threats related to unaut-horized modification of information and pose threats to the integrity of information;

– threats related to violation of the possibility of using the system or information that is processed and poses threats of violation of the availability of information;

– threats related to the violation of the possibility of surveillance, managing and controlling user activity, the possibility of legality of access, capabilities and capabilities to perform the functions of a complex of means of protection and pose a threat of violation of the observation of information.

When analyzing the negative consequences of influencing the ERP system of different types of information th-reats, as a rule, their following categories are considered [26].

Refusals and hardware failures and/or network failures, emergencies and other events occurring without the participation of personnel; unintentional or erroneous actions of administrators, users, system operators or other types of personnel; unauthorized access by violators to the information that is generated, processed and stored in the ERP system, for example, information that:

– perform management and decision making – information of users of the ERP system; provides equipment management of ERP-system; allows you to implement business processes and technologies of information processing in the ERP system.

The "subjective" and "objective" probability of a threat is calculated by expert methods using mathematical methods. The frequency of threats can be determined by quantitative indicator in accordance with the number of cases of threat per year.

To evaluate the linguistic variable X_3 "Threat probability level", we will use the term set $T(X_3)$ of five quality therms: $T(X_3)$={Very low probability of threat (VLT); Low probability of threat (LT); Average threat probability (MT); High probability of threat (HT); Very high probability (VHT).

Definition Area E_{X_3} of the linguistic variable X_3 beset at the interval [0, 05; 365].

Table 6 provides a scale for assessing the level of threat probability in accordance with the frequency of threats per year.

When evaluating the linguistic variable X_4 "Resources Vulnerability", we will rely on the common vulnerability assessment system (CVSS), which makes it possible to fix the basic characteristics of the vulnerability and create a numerical score that reflects its criticality [27]. CVSS is a free and open industry standard for assessing the severity of a computer system security vulnerability, allowing users to prioritive resources according to threat. The CVSS assessment system consists of three metrics [26]: basic metric – reflects the basic qualities and characteristics of the vulnerability; temporary metrics – reflects the following characteristics of the vulnerability, which change over time, develop during a vulnerable period; contextual metric – displays the characteristics of the vulnerability that are unique to the user environment.

DOI 10. 15588/1607-3274-2022-1-12

Each metric group has a specific numerical score (rating) in the range from 0 to 10 and a period representing the value of all metrics in the form of a block of text.

To obtain highquality vulnerability metrics, we will use the National Vulnerability Database (NVD) assessment system. NVD is an information database of the U.S. National Standardization Authority, the U.S. Government supported National Institute of Standards and Technology, that collaborates with the Common Vulnerabilities and Exposures (CVE) database, which represents a dictionary of commonly used names (such as CVE identifiers) for publicly available information security vulnera-bilities. In the NVD database, the security level values of the vulnerability are calculated by values from 0 to 10 (according to CVSS) and are described linguistically by the term None, Low, Medium, High and Critical.

According to the linguistic therms of the NVD database, we will use the $T(X_4)$ term set of four quality therms to evaluate the linguistic variable X_4 "Resource Vulnerability":

$T(X_4)$ = {Low vulnerability (LV); Medium vunerability (MV); High vulnerabilidad (HV); Critical vulnerability (CV).

Definition Area E_{X_4} of the linguistic variable X_4 set at the interval [0,10].

Table 7 describes NVD vulnerability scores by points and linguistically, description of the impact of exploitation, and corresponding levels of resource vulnerability according to the term sets $T(X_4)$.

We will determine the consequences of violation of the integrity, confidentiality, accessibility and observation of information in such important areas of activity of the organization as: – commercial concernment (CC); – management control (MC); relation with clients and partners – relations (R).

The results of the assessment of the consequences of Violation of integrity, confidentiality, accessibility and observation of information in the spheres of activity of the organization are given in Table 8.

Table 6 – Threat probability level assessment scale (X_3)

Frequency	Probability of occurrence a threat for a certain period	Level
0,05	threat is almost never realized	VLT
0,6	approximately 2–3 times in five years	VLT
1	approximately once a year and less (180 <in> 366 (days))	LT
2	approximately 1 time in six months (90 <in > 180 (days))	LT
4	approximately 1 time in 3 months (60 <in > 90 (days))	MT
6	approximately 1 time in 2 months (30 <in > 60 (days))	MT
12	approximately 1 time per month (15 <in > 30 (days))	HT
24	approximately 2 times a month (7 <In > 15 (days))	HT
52	approximately 1 time per week (1 <In > 7 (days))	VHT
365	Daily (1 <In > 7 (Hours))	VHT

Table 7 – Resource Vulnerability Rating Scale

Level by NVD	Score by NVD	Description of the vulnerability level	Vulnerability level
None	**0.0**	Vulnerability has no effect on resource	
Lov	**0.1–3.9**	A vulnerability that has little impact on the resource does not Affect the availability, integrity and confidentiality of information	**LV**
Medium	**4.0–6.9**	A vulnerability that may have some impact on the resource but has a complexity of implementation or does not cause serious consequences. It is possible to access confidential information, change some information, but there is no control over the information, or the scale of losses is small. Resource availability failures occur	**MV**
High	**7.0–8.9**	A vulnerability that has a significant impact on the resource, possible access to confidential information, changes in information and control over information. Significant resource availability failures and performance reductions	**HV**
Critical	**9.0–10.0**	Vulnerability, the consequence of the exploitation of which has a serious impact on the resource: complete loss of availability and integrity of information, full disclosure of confidential information	**CV**

Table 8 – Assessment of the consequences of violation of information properties in the spheres of activity

	Spheres of activity of the organization		
Information Resource Property	**Commercial concernment (CC)**	**Management control (MC)**	**Relationships with clients and partners (R)**
Integrity	CC_I	MC_I	R_I
Confidentiality	CC_I	MC_P	R_P
Accessibility	CC_A	MC_A	R_A
Observability	CC_O	MC_O	R_O

DOI 10. 15588/1607-3274-2022-1-12

To assess the consequences of the threat, we will use a quantitative assessment of the impact on certain properties of information (integrity, confidentiality, accessibility and observation), as proposed by the NBU Methodological Recommendations (National Bank of Ukraine).

The values of assessments of the consequences of violation of integrity, confidentiality, availability and observation of information for commercial interests (CC), management control (MC) and customer-to-partner relationships (R) will be within the range of integer values [1,5].

We will calculate the impact assessment (CA) for each property of the information.

Assessment of the consequences of integrity violation:

$$CA_I = \max(CC_I, MC_I, R_I).$$

Assessment of the consequences of a privacy violation:

$$CA_P = \max(CC_P, MC_P, R_P).$$

Assessment of the consequences of accessibility violations:

$$CA_A = \max(CC_A, MC_A, R_A).$$

Assessment of the consequences of observational violations:

$$CA_O = \max(CC_O, MC_O, R_O).$$

The implementation of the threat can affect several properties at once, so it is necessary to determine thee general assessment of the consequences of violation of the properties of information:

$$CA = \max(CA_I, CA_P, CA_A, CA_O). \quad (19)$$

To evaluate the linguistic variable X_2 "Impact the consequence of", will use the term set $T(X_2)$ of five quality therms:

$T(X_2)$= {Very low consequences (VLC); Low consequences (LC); Medium consequences (MC); Significant consequences (SC); Very big consequences (VBC)}.

The impact level assessment scale is shown in Table 9.

Table 9 – Impact Level Assessment Scale Consequences

Score	Impact Level Description	Level of impact
1	Very low consequences	VLC
2	Low consequences	LC
3	Medium consequences	MC
4	Significant consequences	SC
5	Very big consequences	VBC

The value of information will be defined as the relationship between the type of confidentiality and criticality – criticality (C) of the information. Value estimation is formed as the sum of points corresponding to each type and level of criticality of information. Estimates of the value of information are given in Table 10.

The criticality of the information will be determined, taking into account the assessment of the consequences of violation of the properties of information (see Table 2) by the formula

$$C = C_{CC} + C_{MC} + C_R. \quad (20)$$

To evaluate the linguistic variable X_1 "Resource price", we will use the term set $T(X_1)$ of three highquality therms:

Basis of the development of information risk management systems.

$T(X_1)$= {Low Price (LP); Average Price (AP); High Price (HP)}.

The Definition Area of E_{X_1} of the linguistic variable X_1 be set at the interval [19]. The scale for assessing the value level of information is presented in Table 11.

Table 11 – Information Value Assessment Scale

Price	Description of Price level	Level of Price
4	Low Price	LP
11	Average Price	AP
19	High Price	HP

Table 10 – Definition of value assessment of information

	Criticality of information (C)		
Type of information	Insignificant (1–3 points)	Significant (4–9 points)	Critical (10–15 points)
Open (1 point)	2–4	5–10	11–16
For internal use (2 points)	3–5	6–11	12–17
Confidential (3 points)	4–6	7–12	13–18
Strictly Confidential (4 points)	5–7	8–13	14–19

DOI 10. 15588/1607-3274-2022-1-12

5 RESULTS

This article developed a fuzzy risk assessment model of the ERP system and performed the following stages of Development: a list of factors influencing information security risk is selected; suggested methods for assessing the risk of information resources and ERP-systems in general, assessing financial losses from the implementation of threats, determining the type of risk according to its assessment to form recommendations for their processing in order to maintain the level of security of the ERP-system; the list of linguistic variables of the model is determined; the structure of the base of fuzzy product rules – MISO-structure was chosen; the structure of the fuzzy model was built; fuzzy model variables are defined; the principles of construction of systems of fuzzy logical conclusion and neuro-fuzzy models, use of fuzzy models to solve problems of risk assessment of information security are considered. The concept, principles of construction, functioning and requirements for information security of ERP systems are considered, problems of their safety and vulnerability are analyzed.

According to the results of the review, the main factors influencing the risk assessment are determined, the choice of parameters of a fuzzy product model for risk assessment and the structure of the rules base of a fuzzy logical conclusion is substantiated. Adaptive neuro-fuzzy product model of risk assessment of information security threats is developed.

It is proposed to use a linguistic approach to describe the main factors influencing the assessment of risks, variables and fuzzy variables to assess their qualities, as well as a system of qualitative assessments. The choice of parameters was substantiated and the structure of a fuzzy product model for risk assessment and the basis of the rules of a fuzzy logical conclusion were developed.

As a result, the developed adaptive neuro-fuzzy product model for risk assessment of information security of ERP systems allows to perform risk assessment on four factors: resource value, impact of impact on resource, probability of threat and vulnerability of the resource.

The obtained risk assessments can be used both to assess the risks of information security of ERP-system resources and to the general risk of information security of the ERP system.

The use of a linguistic approach ensures the possibility of using quantitative description of both all and individual elements of the model, provided that there is only infmation about the value of fuzzy information security risk factors, which provides opportunities, if necessary, to separate and rank risk factors and their consequences. Such actions may be useful in determining ways to avoid and /or reduce the negative impact of risk.

The use of neuro-fuzzy system components gives the model flexibility. Setting up the model by training in accordance with the obtained knowledge base allows you to perform risk reassessment in case of changes in the values of factors, changes in the product base of rules or the emergence of new risks. This provides an opportunity to shape and adapt the model to a specific ERP system.

6 DISCUSSIONS

Violation of information security, including noncompliance with regulatory standards, can lead to financial and reputational consequences that are best avoided for any organization, regardless of size, scope or form of ownership.

The operating procedures and business applications that support them must be strategically managed and monitored to ensure the integrity, availability and confidentiality of the data that the organization owns.

Currently, the vast majority of organizations rely on ERP-Systems to implement business processes and integrate financial data. The ERP system is an application system that implements a strategy of comprehensive resource planning that integrates the company's business processes and financial data into one platform. Integration provides better quality and availability of information, but it also increases the risk of fraud from within the organization by users and malicious attacks from outside. This dependency increases the security value of the ERP system to protect your organization's information assets.

A key aspect of any security strategy is the ability to achieve a level of security that adequately demonstrates the organization's commitment to information security and data security regulations collected from its customers and partners. Too little security increases the risk of violations, while too much can lead to unnecessary costs for information technology, software and hardware, deteriorating system performance, and slowing down business processes. There is no optimal security solution for any ERP-system. Each organization needs to assess risks and set goals related to their environment and the type of information it processes.

The peculiarity of risk assessment tasks is that most of the data on risk factors has signs of imperfection and uncertainty: contradiction, inaccuracy, unreliability or incompleteness, are nonlinear and dynamically variable. For effective assessment in case of uncertainty of input data, fuzzy logic methods and neuro-fuzzy networks are used to use linguistic variables and statements to describe risk factors and be adaptive at the expense of the neuro-network component.

ACKNOWLEDGEMENTS

The work was performed at the Department of Information and cybernetic security of the State University of telecommunications within scientific researches conducted by the department.

DOI 10. 15588/1607-3274-2022-1-12

REFERENCES

1. Leighton J. Security Controls Evaluation, Testing and Assessment Handbook. Syngress, 2016, 678 p.
2. Rescher N. «Many-Valued Logic», Mc.Graw-Hill. New York, 1969. DOI:10.2307/2272880
3. Rosser J. B., Turquette A. R. Many-Valued Logics, North Holland. Amsterdam, 1952.
4. Common Vulnerability Scoring System version 3.1: Specification Document. CVSS Version 3.1 Release [Elektronnyi resurs], *Forum of Incident Response and Security Teams*. Rezhim dostupu: https://www.first.org/cvss/ specification-document.
5. Abhishek kumar srivastav, Irman Ali, Shani Fatema. A Quantitative Measurement Methodology for calculating Risk related to Information Security, *IOSR Journal of Computer Engineering (IOSR-JCE),* Volume 16, Issue 1, Ver. IX (Feb. 2014), pp. 17–20.
6. Hayashi Y., Imura A. Fuzzy neural expert system with automated extraction of fuzzy If-Then rules from a trained neural network, *Proceedings. First International Symposium on Uncertainty Modeling and Analysis*, 1990, pp. 489–494. DOI.1109/ISUMA.1990.151303
7. Buckleya J. J., Hayashi Y. Fuzzy neural networks: a survey, *Fuzzy sets and systems,* 1994, Vol. 66, Issue 1, pp. 1–13. https://doi.org/10.1016/0165-0114(94)90297-6
8. Hendrawirawan D. Tanriverdi H., Zetterlund C. ERP Security and Segregation of Duties Audit: A Framework for Building an Automated Solution, *Information systems control journal*, 2007, Vol. 2, 4 p. ISACA. All rights reserved. www.isaca.org
9. Nieto-Morote A., Ruz-Vila A. F. Fuzzy approach to construction Project risk assessment, *International Journal of Project Management*, 2011, Vol. 29, Issue 2, pp. 220–231.
10. Kozhukhivskyi A. D., Kozhukhivska O. A. ERP-System Risk Assessment Methods and Models (Tekst), *Radio Electronics, Computer Science, Control*, 2020, No. 4(55), pp. 151–162. DOI 10.15588/1607-3274-2020-4-15.
11. Baskerville R. An analysis survey of information system security design methods: Implications for Information Systems Development, *ACM Computing Survey*, 1993, pp. 375–414.
12. Peltier T. R. Facilitated risk analysis process (FRAP), *Auerbach Publication,* CRC Press LLC, 2000, 21 p.
13. Alberts C., Dorofee A. Managing Information Security Risks: The Octave Approach. Addison-Wesley Professional, 2002, 512 p.
14. Stolen K., den Braber F., Dirmitrakos T. Model-based risk assessment – the CORAS approach [Elektronnyi resurs], 2002. Rezhim dostupu, http://folk.uio.no/nik/2002/Stolen.pdf
15. Suh B., Han I. The IS risk analysis based on business model, *Information and Management*, 2003, Vol. 41, No. 2, pp. 149–158.
16. Karabacak B., Songukpinar I. ISRAM: Information security risk analysis method, *Computer & Security, March,* 2005, pp. 147–169.
17. Goel S., Chen V. Information security risk analysis – a matrix-based approach [Elektronnyi resurs], *University at Albany*, SUNY, 2005. Rezhim dostupu: https://www.albany.edu /~goel/publications/goelchen2005.pdf
18. Elky S. An introduction to information system risk management [Elektronnyi resurs], *SANS Institute InfoSec Reading Room*, 2006. Rezhim dostupu: https://www.sans.org/reading-room/whitepapers/auditing/introduction-information-system-risk-management-1204.
19. Yazar Z. A. A Qualitative risk analysis and managment tool – CRAMM [Elektronnyi resurs], *SANS Institute InfoSec Reading Room*, 2011, Rezhim dostupu: https://www.sans.org/reading-room/whitepapers/auditing/qualitative-risk-analysis-management-tool-cramm-83
20. Korchenko A. G. Building information protection systems on fuzzy sets. Theory and practical solutions. Kyev, MK-Press, 2006, 320 p.: IL.
21. Security issues in ERP. Security, Audit and Control Features SAP ERP 4th Edition, Audit Program. Isaca, 2015, 574 p.
22. A Complete Guide to the Common Vulnerability Scoring System. Forum of Incident Response and Security Teams (June2007). Rezhim dostupu: http://www.first.org/cvss/cvss-guide.pdf
23. Polyakov A. ERP Security Deserves Our Attention Now More Than Ever [Elektronnyi resurs], Forbes, 2017. Rezhim dostupu: https://www.forbes.com/sites/forbestechcouncil/2017/07/07/erp-security-deserves-our-attention-now-more-than-ever/.
24. "NVD Common Vulnerability Scoring System Support v2". National Vulnerability Database. National Institute of Standards and Technology. Retrieved March 2, 2013.
25. Jang J.-S. R. ANFIS: Adaptive Network – based Fuzzy Inference System, *IEEE Trans. On Syst. Man and Cybernetics*, 1993, Vol. 23, No. 3, pp. 665– 685.
26. National vulnerability database Release [Elektronnyi resurs], *National Institute of Standards and Technology.* Rezhim dostupu: https://nvd.nist.gov
27. National vulnerability database Release. Vulnerability Metrics [Elektronnyi resurs], *National Institute of Standards and Technology.* Rezhim dostupu: https://nvd.nist.gov/vuln-metrics/cvss

Received 08.11.2021.
Accepted 16.12.2021.

УДК 004.94

РОЗРОБКА НЕЧІТКОЇ МОДЕЛІ ОЦІНКИ РИЗИКІВ ДЛЯ ERP-СИСТЕМИ

Кожухівський А. Д. – д-р техн. наук, професор, професор кафедри інформаційної та кібернетичної безпеки Державного університету телекомунікацій, Київ, Україна.

Кожухівська О. А. – д-р техн. наук, доцент кафедри інформаційної та кібернетичної безпеки Державного університету телекомунікацій, Київ, Україна.

АНОТАЦІЯ

Актуальність. Оскільки оцінка ризиків інформаційної безпеки є складним і повним процесом невизначеності, а невизначеність є основним фактором, що впливає на ефективність оцінки, доцільно використовувати нечіткі методи та моделі, які є адаптивними до необчислюваних даних. Формування розпливчастих оцінок факторів ризику є суб'єктивним, а оцінка

DOI 10. 15588/1607-3274-2022-1-12

ризиків залежить від практичних результатів, отриманих у процесі обробки ризиків загроз, які вже виникли під час функціонування організації та досвіду фахівців з інформаційної безпеки. Тому доцільним буде використання моделей, що здатні адекватно оцінювати нечіткі фактори та мають можливість корегування їх впливу на оцінку ризику. Найбільші показники ефективності для вирішення таких задач мають нейро-нечіткі моделі, що комбінують методи нечіткої логіки та штучних нейронних мереж і систем, тобто «людиноподібного» стилю міркувань нечітких систем з навчанням та моделюванням розумових явищ нейронних мереж. Для побудови моделі розрахунку оцінки ризику інформаційної безпеки пропонується використовувати нечітку продукційну модель. Нечіткі продукційні моделі (нечіткі моделі/системи на основі правил) це поширений тип нечітких моделей, які використовуються для опису, аналізу та моделювання складних систем і процесів, що слабо формалізуються.

Мета роботи – розробка структури нечіткої моделі оцінки ризиків інформаційної безпеки та захисту систем ERP шляхом використання нечітких нейронних моделей.

Метод. Для побудови структури моделі розрахунку оцінки ризику інформаційної безпеки пропонується використовувати нечітку продукційну модель. Нечіткі продукційні моделі це загальний вид нечітких моделей, які використовуються для опису, аналізу та моделювання складних систем і процесів, що слабо формалізуються.

Результати. Визначено фактори, що впливають на оцінку ризиків, запропоновано використання лінгвістичних змінних для їх опису та використання нечітких змінних для оцінки їх якостей, а також системи якісних оцінок. Обґрунтовано вибір параметрів та розроблено структуру нечіткої продукційної моделі оцінювання ризиків та бази правил нечіткого логічного висновку. Розглянуто використання нечітких моделей для вирішення задач оцінки ризиків інформаційної безпеки, а також концепцію та побудову ERP-систем та проаналізовано проблеми їх безпеки та вразливості.

Висновки. Розроблено нечітку модель оцінки ризиків ERP-системи. Обрано перелік факторів, що впливають на ризик інформаційної безпеки. Запропоновано методи оцінки ризику інформаційних ресурсів та ERP-систем взагалі, оцінки фінансових збитків від реалізації загроз, визначення типу ризику за його оцінкою для формування рекомендацій відносно їх обробки з метою підтримки рівня захищеності ERP-системи. Визначено перелік лінгвістичних змінних моделі. Обрано структуру бази нечітких продукційних правил – MISO-структуру. Побудовано структуру нечіткої моделі. Визначено нечіткі змінні моделі.

КЛЮЧОВІ СЛОВА: інформаційна безпека, нечітка логіка, оцінка ризиків, захищенність, ERB-система.

УДК 004.94

РАЗРАБОТКА НЕЧЕТКОЙ МОДЕЛИ ОЦЕНКИ РИСКОВ ДЛЯ ERP-СИСТЕМЫ

Кожуховский А. Д. – д-р техн. наук, профессор, профессор кафедры информационной та кибернетической безопасности Государственного университета телекоммуникаций, Киев, Украина.

Кожуховская О. А. – д-р техн. наук, доцент кафедры информационной та кибернетической безопасности Государственного университета телекоммуникаций, Киев, Украина.

АННОТАЦИЯ

Актуальность. Поскольку оценка рисков информационной безопасности является сложным и полным процессом неопределенности, а неопределенность является одним из основных факторов, влияющих на эффективность оценки, целесообразно использовать нечеткие методы и модели, которые являются адаптивными к неучтенных данных. Формирование расплывчатых оценок факторов риска субъективно, а оценка рисков зависит от практических результатов, полученных в процессе обработки рисков угроз, которые уже возникли в ходе функционирования организации, и опыта специалистов по информационной безопасности. Поэтому целесообразно использовать модели, которые могут адекватно оценивать нечеткие факторы и иметь возможность корректировать их влияние на оценку рисков. Наибольшими показателями эффективности для решения таких проблем являются нейро-нечеткие модели, сочетающими методы нечеткой логики и искусственные нейронные сети и системы, т.е. «человеко-подобный» стиль соображений нечетких систем с обучением и моделированием психических явлений нейронных сетей. Для построения модели расчета оценки рисков информационной безопасности предлагается использовать нечеткую модель продукта. Нечеткие модели продуктов (нечеткие модели /системы на основе правил) являются обычным типом нечетких моделей, используемых для описания, анализа и моделирования сложных систем и процессов, которые плохо формализованы.

Цель работы – разработка структуры нечеткой модели оценки рисков информационной безопасности и защиты систем ERP с использованием нечетких нейронных моделей.

Метод. Для построения модели расчета оценки рисков информационной безопасности предлагается использовать нечеткую модель продукта. Нечеткие модели продуктов являются обычным видом нечетких моделей, используемых для описания, анализа и моделирования сложных систем и процессов, которые плохо формализованы.

Результаты. Выявленные факторы, влияющие на оценку риска, свидетельствуют об использовании лингвистических переменных для их описания и использования нечетких переменных для оценки их качеств, а также системы качественных оценок. Обоснован выбор параметров и разработана структура нечеткой модели оценки рисков и основы правил нечеткого логического заключения. Рассматривается использование нечетких моделей для решения проблем оценки рисков информационной безопасности, а также концепция и строительство систем ERP и проанализированы проблемы их безопасности и уязвимости.

Выводы. Разработана нечеткая модель оценки рисков системы ERP. Выбран перечень факторов, влияющих на риск информационной безопасности. Предлагаются методы оценки рисков информационных ресурсов и ERP-систем в целом, оценка финансовых потерь от реализации угроз, определение вида риска в соответствии с его оценкой для формирования рекомендаций по их обработке в целях поддержания уровня защиты системы ERP. Определен список лингвистических перемен-

DOI 10. 15588/1607-3274-2022-1-12

ных модели. Выбрана структура базы данных нечетких правил продукта – MISO-структура. Построена структура нечеткой модели. Выявлены нечеткие переменные модели.

КЛЮЧЕВЫЕ СЛОВА: информационная безопасность, нечеткая логика, оценка рисков, защищенность, ERB-система.

ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. Leighton J. Security Controls Evaluation, Testing and Assessment Handbook / J. Leighton. – Syngress, 2016. – 678 p.
2. Rescher N. Many-Valued Logic / N. Rescher. – Mc.Graw-Hill, New York, 1969. DOI:10.2307/2272880
3. Rosser J. B. Many-Valued Logics / J. B. Rosser, A. R. Turquette. – North Holland, Amsterdam, 1952.
4. Common Vulnerability Scoring System version 3.1: Specification Document. CVSS Version 3.1 Release [Електронний ресурс] // Forum of Incident Response and Security Teams. – Режим доступу: https://www.first.org/cvss/ specification-document.
5. Abhishek Kumar Srivastav A Quantitative Measurement Methodology for calculating Risk related to Information Security / Abhishek Kumar Srivastav, Irman Ali, Shani Fatema // IOSR Journal of Computer Engineering (IOSR-JCE). – (Feb. 2014). – Volume 16, Issue 1, Ver. IX. – P. 17–20.
6. Hayashi Y. Fuzzy neural expert system with automated extraction of fuzzy If-Then rules from a trained neural network / Y. Hayashi, A. Imura // Proceedings. First International Symposium on Uncertainty Modeling and Analysis. – 1990. – P. 489–494. DOI.1109/ISUMA.1990.151303
7. Buckleya J. J. Fuzzy neural networks: a survey / J. J. Buckleya, Y. Hayashi // Fuzzy sets and systems. – 1994. – Vol. 66, Issue 1. – P. 1–13. https://doi.org/10.1016/0165-0114(94)90297-6
8. Hendrawirawan D. ERP Security and Segregation of Duties Audit: A Framework for Building an Automated Solution / D. Hendrawirawan, H. Tanriverdi, C. Zetterlund // information systems control journal. – 2007. – Vol. 2. – 4 p. ISACA. All rights reserved. www.isaca.org
9. Nieto-Morote A. A. Fuzzy approach to construction Project risk assessment / A. Nieto-Morote, F. Ruz-Vila // International Journal of Project Management. – 2011. – Vol. 29, Issue 2. – P. 220–231.
10. Kozhukhivskyi A. D. ERP-System Risk Assessment Methods and Models (Tekst) / A. D. Kozhukhivskyi, O. A. Kozhukhivska // Radio Electronics, Computer Science, Control. – 2020. – No. 4(55). – P. 151–162. DOI 10.15588/1607-3274-2020-4-15.
11. Baskerville R. An analysis survey of information system security design methods: Implications for Information Systems Development / R. Baskerville // ACM Computing Survey. – 1993. – P. 375–414.
12. Peltier T. R. Facilitated risk analysis process (FRAP) / T. R. Peltier. – Auerbach Publication, CRC Press LLC, 2000. – 21 p.
13. Alberts C. Managing Information Security Risks: The Octave Approach / C. Alberts, A. Dorofee, Addison-Wesley Professional. – 2002. – 512 p.
14. Stolen K. Model-based risk assessment – the CORAS approach [Elektronnyi resurs] / K Stolen, F. den Braber, T. Dirmitrakos. – 2002. – Rezhim dostupu: http://folk.uio.no/nik/2002/Stolen.pdf
15. Suh B. The IS risk analysis based on business model / B. Suh, I. Han // Information and Management. – 2003. – Vol. 41, No. 2. – P. 149–158.
16. Karabacaka B. ISRAM: Information security risk analysis method / B. Karabacaka, I. Songukpinar. – Computer & Security, March. – 2005. – P. 147–169.
17. Goel S. Information security risk analysis – a matrix-based approach [Elektronnyi resurs] / S. Goel, V. Chen. – University at Albany. – SUNY. – 2005. – Rezhim dostupu: https://www.albany.edu /~goel/publications/goelchen2005.pdf
18. Elky S. An introduction to information system risk management [Elektronnyi resurs] / S. Elky. – SANS Institute InfoSec Reading Room. – 2006. – Rezhim dostupu: https://www.sans.org/reading-room/whitepapers/auditing/introduction-information-system-risk-management-1204.
19. Yazar Z. A. Qualitative risk analysis and management tool – CRAMM [Elektronnyi resurs] / Z. A. Yazar. – SANS Institute InfoSec Reading Room. – 2011. – Rezhim dostupu: https://www.sans.org/reading-room/whitepapers/auditing/qualitative-risk-analysis-management-tool-cramm-83
20. Yurchenko A. G. Building information protection systems on fuzzy sets.Theory and practical solutions / A. G. Yurchenko, A. G. Korchenko. – K. : MK-Press. – 2006. – 320 p.: IL.
21. Security issues in ERP. Security, Audit and Control Features SAP ERP 4th Edition, Audit Program. – Isaca. – 2015. – 574 p.
22. A Complete Guide to the Common Vulnerability Scoring System. Forum of Incident Response and Security Teams (June 2007). Rezhim dostupu: http://www.first.org/cvss/cvss-guide.pdf
23. Polyakov A. ERP Security Deserves Our Attention Now More Than Ever [Elektronnyi resurs] / A. Polyakov // Forbes. – 2017. – Rezhim dostupu: https://www.forbes.com/sites/forbestechcouncil/2017/07/07/erp-security-deserves-our-attention-now-more-than-ever/.
24. NVD Common Vulnerability Scoring System Support v2. National Vulnerability Database. – National Institute of Standards and Technology. Retrieved March 2, 2013.
25. Jang J.-S. R. ANFIS: Adaptive Network – based Fuzzy Inference System / J.-S.R. Jang // IEEE Trans. On Syst. Man and Cybernetics. – 1993. – Vol. 23, No. 3. – P. 665–685.
26. National vulnerability database Release [Elektronnyi resurs] // National Institute of Standards and Technology. – Rezhim dostupu: https://nvd.nist.gov
27. National vulnerability database Release. Vulnerability Metrics [Elektronnyi resurs] // National Institute of Standards and Technology. – Rezhim dostupu: https://nvd.nist.gov/vuln-metrics/cvss.

DOI 10. 15588/1607-3274-2022-1-12