УПРАВЛІННЯ У ТЕХНІЧНИХ СИСТЕМАХ

CONTROL IN TECHNICAL SYSTEMS

УПРАВЛЕНИЕ В ТЕХНИЧЕСКИХ СИСТЕМАХ

UDC 004.94

RISK ASSESSMENT MODELING OF 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 security risks is a complex and complete uncertainty process, and uncertainties are a major factor influencing valuation performance, it is advisable to use fuzzy methods and models that are adaptive to noncomputed 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 security professionals. Therefore, it will be advisable to use models that can ade-quately 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 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 a fuzzy model of quality of 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 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 was substantiated and a fuzzy product model of risk assessment and a database of rules of fuzzy logical conclusion using the MATLAB application package and the Fuzzy Logic Toolbox extension package was implemented, as well as improved by introducing the adaptability of the model to experimental data by introducing neuro-fuzzy components into the model. The use of fuzzy models to solve the problems of security risk assessment, as well as the concept and construction of ERP systems and the 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 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: Security, fuzzy logic, fuzzy product model, risk assessment, security, ERP-system.

ABBREVIATIONS

ANFIS is a Adaptive Network-based Fuzzy Inference System;

DB is a Database;

DSTU is a State standard of Ukraine;

ERP is an 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;

DOI 10.15588/1607-3274-2022-4-12

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 an expected loss from the one-time 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*-resource to the *j*-th threat;

IR is a resource set of system;

Th is a set of threats to the system.

A_i^V is a value of the *i*-st resource;

F_{ij}^e is an 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;

Th_i is a set of risks for the *i*-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*-st 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_I is an incoming Variables (can be either clear or fuzzy);

X_I is a definition area appropriate prerequisites;

y is a fuzzy output variable;

Y is a definition area the conclusion;

A_{ij}, B_i are 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 are affiliation functions options;

k is an example from many examples of training sampling;

$x_m^{(k)}$ are input variable values x_m;

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

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

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

E is an error;

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

ε is an installed threshold;

$\mu(x, \sigma, c)$ is a bell function – Gauss distribution function;

x is a degree of belonging to the term;

σ is a standard deviation, function steepness;

c is a shift peak bell Curve from Zero;

l_m are number of functions belonging to specify variables X_1, X_2, X_3, X_4;

l_y is a number of affiliation functions for the source variable Y.

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 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 with the threat that this vulnerability may be, and for each pair, the probability of its occurrence is assessed and the impact of the pair's implementation on integrity, confidentiality, accessibility, and observability is assessed.

We will use the following definitions. Probability is a conditional number that determines the frequency of such a threat / vulnerability of a pair. 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,

DOI 10.15588/1607-3274-2022-4-12

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 modeling 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.

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

1 PROBLEM STATEMENT

Security risk modeling is an important element of the overall security risk management process, which is the process of ensuring that the organization's position is wit-hin acceptable limits defined by senior management and consists of four main stages: security risk assessment, testing and supervision, mitigation, 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. Modeling of information security risks is a process of identifying vulnerable situations, threats, the likelihood of their occurrence, the level of risks and consequences associated with the assets of organization, as well as control, which can mitigate threats and their consequences. Modeling 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.

The full process of risk assessment modeling should also include recommendations for control and evaluation of results.

Information risk assessment can be carried out by modeling. The methodology for modeling information security risk assessment understands the systematized sequence of actions (step-by-step instructions) that need to be implemented 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. At present, the following standards apply on the territory of Ukraine: ISO 27001, ISO 27002, ISO 27003, ISO 27004 and ISO 27005 [2–6].

Recently, methods of analysis and risk assessment, based on elements of fuzzy logic, have been intensively developed. Such methods allow you to change the test table of methods of rough risk assessment to the mathematical method, as well as significantly expand the possibilities of risk modeling [7–11].

To build a risk assessment model, we will use the ratio of risk factors, according to the formulas [11]:

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

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

The general ratio of risks assessment factors (1) and (2) is represented by the expression:

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

As for each information resource many risks (from one to all) can be defined, the estimation of the general risk on an information resource will be defined as the maximum estimation among risks:

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

In turn, the system-wide risk assessment will be defined as the maximum assessment among resource risk assessments:

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

Total financial loss is defined as the sum of financial losses on all resources:

$$FL = \sum_i FL_i,\ i \in IR. \quad (6)$$

Thus, the overall risk assessment of the ERP system can be expressed as follows:

$$Y = f_Y(X_1, X_2, X_3, X_4). \quad (7)$$

Based on the analysis and the formed ratio of risk factors (3), a fuzzy model with four input parameters (X1, X2, X3, X4) and one output Y (MISO structure [11]) is proposed to assess each of the risks. The number of input parameters is selected according to the number of factors influencing the degree of risk (3).

Important processes are the implementation of the model using the MATLAB application package and the Fuzzy Logic Toolbox extension package, as well as improvements by introducing the adaptability of the model to experimental data by introducing neuro-fuzzy components into the model.

As a result of modeling the process of obtaining risk assessments of the ERP system and analyzing the results, a fairly high accuracy and low error of the developed model were established.

The proposed model and approach to assessing the security risks of the ERP system may be further developed and underlie the development of an information risk management system.

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 [12]. Over time, complex tools

DOI 10.15588/1607-3274-2022-4-12

are developed to analyze risks, such as: Facilitated Risk Assessment Process [13]; The Operationally Critical Threat, Asset, and Vulnerability Evaluation [14]; CORAS [15]; Method of Risk analysis of business model [16]; Security Risk Analysis Method [17]; Risk Watch method [18]; Consultative Objective and Bifunctional Risk Analysis [19]; CRAMM [20].

In addition, since the early 2000s, some other security risk modeling techniques have also been used in the risk forecasting industry, which have provided good performance and are commonly referred to as "soft computing models", including gray relational approach, fuzzy number arithmetic, information entropy, fuzzy weighted average approach, fuzzy measure and theory of evidence, method of fuzzy analysis of the hierarchical process.

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

Soft computing components include: Neural networks – computational systems that assess the risks of security through similar functioning of biological neural networks and learning tasks (gradually improving performance of these networks), considering examples, in general, without special programming for the task; Rough setsan 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; Method of reference vectors – 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 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 corresponding to the current values of input variables, using a fuzzy knowledge base and fuzzy operations.

Most often, Mamdani and Sugeno algorithms are used in practice. The main difference between them is the method of create the value of the source variable in the rules that make up 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 important, models of fuzzy conclusion Mamdani, Sugeno, Larsen, Tsukamoto [20] have been developed. Most often, Mamdani and Sugeno algorithms are used in practice. The main difference between them is the method of applying the value of the source variable in the rules that make up 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 advisable to use the Sugeno algorithm, and for tasks in which the explanation and justification of the decision is more important, Mamdani's algorithm will have an advan-tage.

3 MATERIALS AND METHODS

To build a structure a model for calculating 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 should take into account: the method of fuzzy inference; fuzzy product rules database; the order of introduction of fuzzy cations; the procedure for aggregating the degree of truth of the preconditions for each of the rules of fuzzy product; activation procedure for each of the rules of the odd product; the procedure for eliminating activated inclusions of all fuzzy product rules for each source variable; diffusion procedure for clarity of each aggregate output variable; procedure for optimizing the parameters 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 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.

DOI 10.15588/1607-3274-2022-4-12

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 compo-sition of the rules in the base and the parameters of the fu-nctions of belonging, as well as to implement various co-mponents of this model on the basis of neuronet techno-logy.

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 formula (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 (see (2)).

Taking into account (1) and (2), we obtain the general ratio of factors for risk assessment (see (3)).

Since many risks can be identified for each informati-on 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 (see (4)).

In turn, the assessment of system risk will be defineed as the maximum assessment among resource risk assess-ments (see 5)).

In turn, the total financial loss will be determined as the amount of financial losses on all resources (see 6)).

We will apply a linguistic approach to the description of security risk factors. Suppose as the values of factors and characteristics of relations between them not only qu-antitative 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 co-nsequence of, the likelihood of a threat, the vulnerabili ty, of resource protection and ways to avoid negative impact from the implementation of risk.

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

Thus, information security risk assessment can be expressed as (see 7)).

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).

To maintain the level of security of the ERP system, it is necessary to determine what risks, according to the le-vel of their assessment – risk level (RL), require proces-sing 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:

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

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

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]:

$$\begin{aligned} P_i: \text{If } x_1 \text{ is } A_{i1} \text{ and } \dots \text{ and } x_j \text{ is } A_{ij} \text{ and } \dots \text{ and} \\ x_m \text{ is } A_{im}, \text{ then } y \text{ is } B_i. \end{aligned} \quad (9)$$

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

In the first case, if there is no need to agree on the opinions of experts, it is assumed that the tasks of ensu-ring completeness and inconsistency of the database of fuzzy rules are solved in advance. If only experimentals 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 network [23].

Since the fuzzy ANFIS network is presented multilay-er 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 network of anfis type, which implements the algorithm of fuzzy output of Takagi-Sugeno [24].

Let the rules of this form be given:

$$\begin{aligned} P_1: \text{If } x_1 \text{ is } A_{11} \text{ and } x_2 \text{ is } A_{12} \text{ then} \\ y_1 = a_1 x_1 + b_1 x_2; \\ P_2: \text{If } x_1 \text{ is } A_{21} \text{ and } x_2 \text{ is } A_{22} \text{ then} \\ y_2 = a_2 x_1 + b_2 x_2. \end{aligned} \quad (10)$$

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 therms: $T(Y)$={«Very low risk (VLR); «Low risk (LR)»; «Medium risk (MR)»; «High risk (HR)»; «Very high

DOI 10.15588/1607-3274-2022-4-12

risk (VHR)»}. Definition Areas of E_Y of the linguistic variable Y will be set at the interval [0; 100] [25].

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 1.

The criticality of the information will be determined, taking into account the assessment of the consequences of violation of the properties of information. To evaluate the linguistic variable X_1 "Resource price", we will use the term set $T(X_1)$ of three high – quality therms: Basis of the development of information risk management systems. $T(X_1)$= {Low Price (LP); Average Price (AP);

Table 1 – 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
Confiden tial (3 points)	4–6	7–12	13–18
Strictly Confidential (4 points)	5–7	8–13	14–19

High Price (HP)}. The Definition Area of E_{X_1} of the linguistic variable X_1 be set at the interval [4;19] [26].

The value level assessment scale for each linguistic variable is determined by values 4, 11 and 19, respectively.

To evaluate the linguistic variable X_3 "Threat probability level", we will use the 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 Areas E_{X_3} of the linguistic variable X_3 beset at the interval [0, 05; 365].

The VLT term corresponds to a situation where the threat is almost never realized or implemented no more than 2–3 times in five years (frequency in the range [0, 0,6]). The term LT corresponds to the situation when the threat occus 1–2 times a year (frequency in the range [1, 2]). The term MT corresponds to the situation when the threat occurs once every 2–3 months (frequency in the range [4, 6]). The HT term corresponds to the situation when the threat occurs 1–2 times a month (frequency in the range [12, 24]). The VHT term corresponds to a situ-ation where a threat occurs from 1 time per week to 1 ti-me per day (frequency in the range [52, 365]).

When evaluating the linguistic variable X_4 "Resour-ces 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 indicators 26]: basic metric – reflects the main qualities and characteristics of the vulnerability; time indicators – reflects the following characteristics of the vulnerability, which change over time, develop over the vulnerable period; context metrics – displays vulnerability characteristics that are unique to the user environment. Each group of indicators has a certain numerical score in the range from 0 to 10 and a dot representing the value of all indicators in the form of a block of text.

To obtain vulnerability indicators, we will use the Natioal Vulnerability Assessment System (NVD) [28]. NVD is an information database of the U.S. National Standardization Authority, the National Institute of Standards and Technology, supported by the U.S. Government. In the NVD database, the security level values of the vulnerabi-lity are calculated by values from 0 to 10 (according to CVSS) and are described linguistically by the term None, Low, Medium, High, and Critical [28].

According to the linguistic therms of the NVD data-base, we will use the $T(X_4)$ term set of four quality the-rms 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 variables X_4 set at the interval [0, 10].

Table 2 describes NVD vulnerability scores by points and linguistically [29], description of the impact of exploitation, and corresponding levels of resource vulnerability according to the term sets $T(X_4)$.

Table 2 – Resource Vulnerability Rating Scalt

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
Higt	7.0–8.9	A vulnerability that has a significant impact on the resource, possible access to confidential information, changes in informations 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

DOI 10.15588/1607-3274-2022-4-12

4 EXPERIMENTS

To develop a fuzzy model, we will use the Fuzzy Logic Toolbox tool from the MATLAB package version R2020a.

Fuzzy Logic Toolbox is a MATLAB extension package that contains tools for designing fuzzy logic systems. The package allows you to create expert systems based on fuzzy logic, develop clustering with fuzzy algorithms, as well design fuzzy neural networks. The package includes a graphical interface for interactive step-by-step design of fuzzy systems, command line functions for software development, as well as special blocks for building fuzzy logic systems. All functions of the package are implemented in the open language MATLAB, which allows you to control ol the execution of algorithms, change the source code, as well as create your own functions and procedure [30].

In accordance with the developed structure of the fuzzy model (see (7)) using the Fuzzy Logic Designer GUI of the Fuzzy Logic Toolbox package, a fuzzy product model was developed, the structure of which is shown in Fig. 1.

The developed fuzzy model has a MISO structure: four inputs (risk assessment factors) and one output (risk assessment).

Among the fuzzy Logic Toolbox models available, using Mamdani or Sugeno fuzzy conclusion algorithms, the Sugeno model was chosen as the only one that has the ability to use fuzzy natural production networks based on it, namely the ANFIS network.

For each input of the model according to the developed structure (7), the ranges of the areas for determining the numerical value of the parameter, quantity, type, name and parameters of the membership functions were adjusted:

– the range of the input parameter definition area corresponds to the ranges of estimates of the corresponding risk factor;

– number of affiliation functions corresponds to the number of therms of the linguistic variable of the parameter;

– the names of the functions of the affiliation correspond of the abbreviated names of the term;

– the type of the function of belonging is a kolokoloobrazna curve – the function of the Gauss distribution:

$$\mu(x,\sigma,c) = e^{\frac{-(x-c)^2}{2a^2}}. \qquad (11)$$

– parameters of affiliation functions were selected in accordance with the center of values of parameter evaluations by term, parameters σ are selected so that functions of the affiliation overlap at the level of 0.5.

The results of configuring the source and input data using the Membership Function Editor are shown in Figures 2 and 3, respective.

The list of selected parameters for model data and affiliation functions is shown in Table 3.

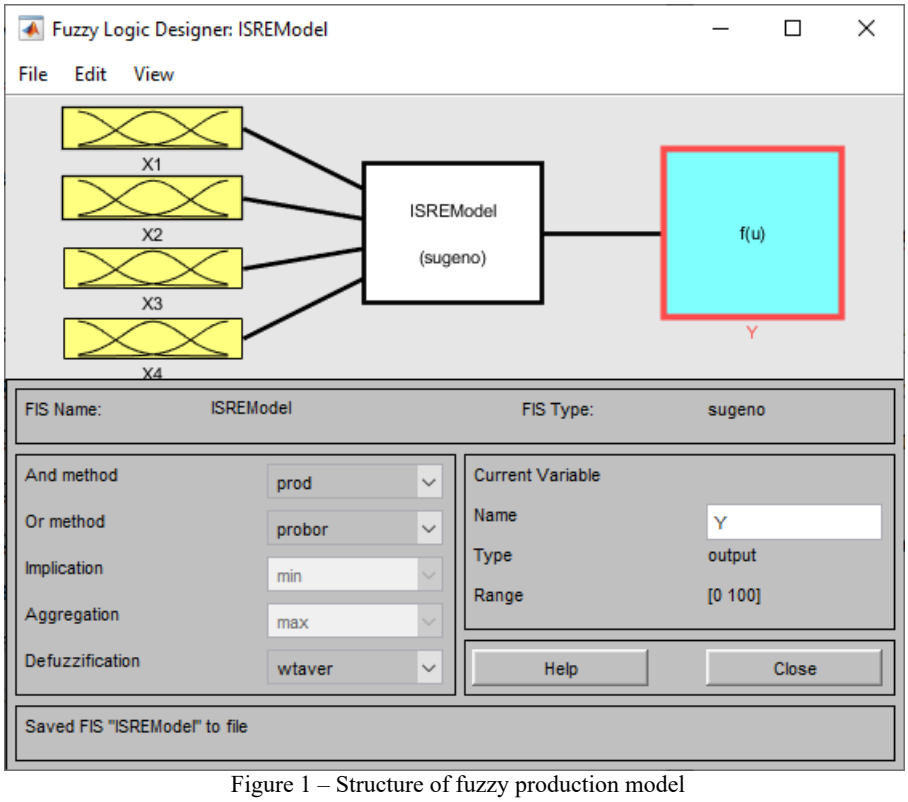

Figure 1 – Structure of fuzzy production model

DOI 10.15588/1607-3274-2022-4-12

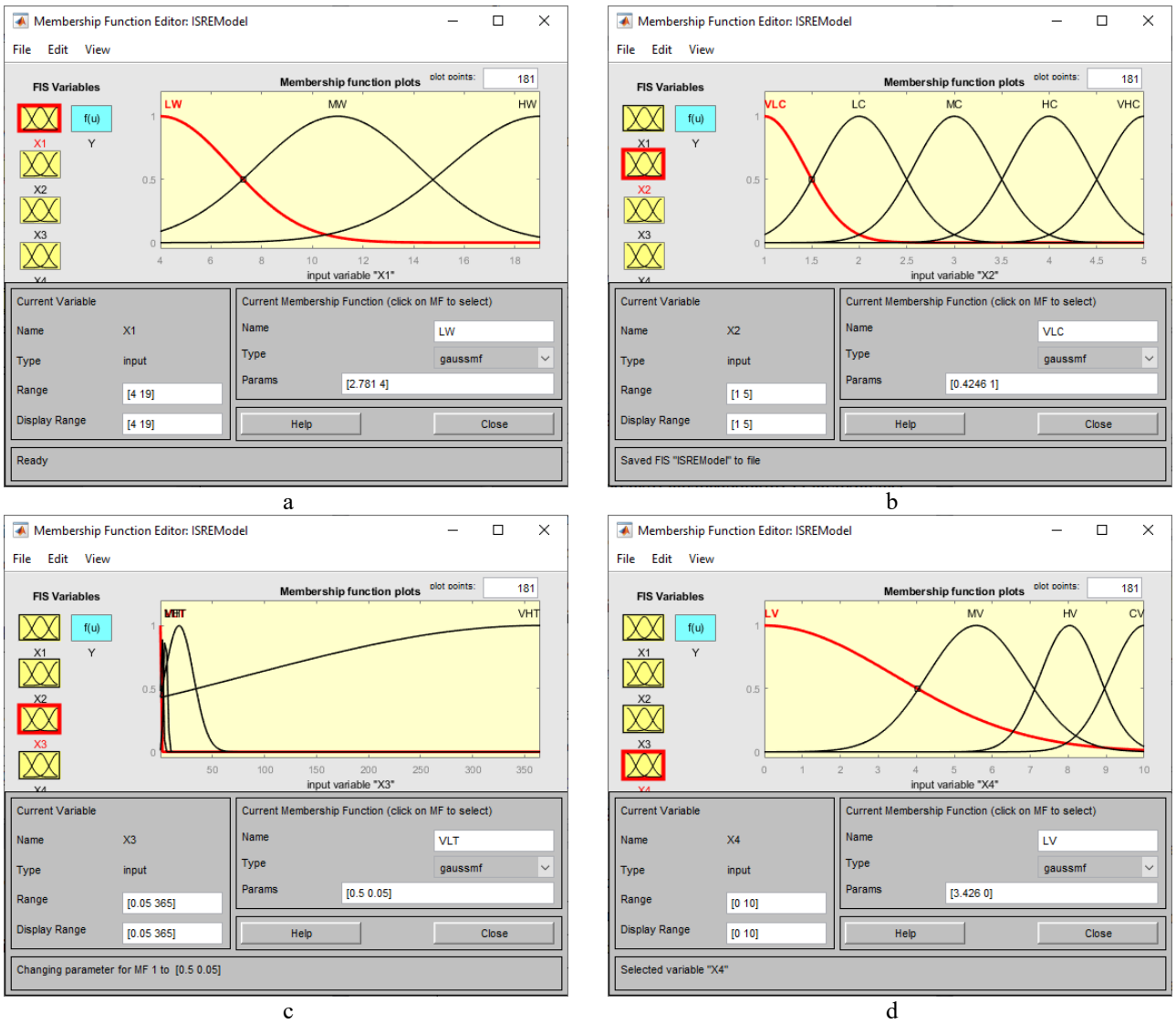

Figure 2 – Model input data configuration results:
a – Input parameter X_1 "Resource Value", b – Input parameter X_2 "Impact the consequence", c – Input parameter X_3 "Probability the emergence of threat", d – Input parameter X_4 "Resource Vulnerability"

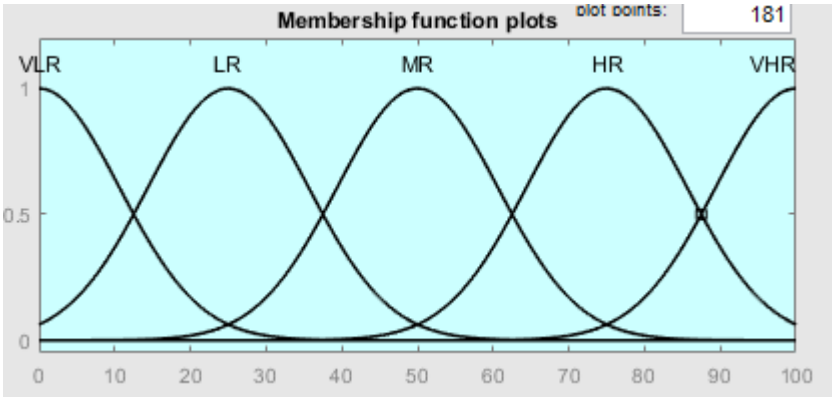

Figure 3 – The results of configuring the original model parameter

DOI 10.15588/1607-3274-2022-4-12

Table 3 – Model Data Options

Imput Parameter Definition Driver Ratings)	**Affiliation function**	**Therm**	**Deviation (σ)**	**Center (peak) (*s*)**
$X_1 \in [4;19]$				
	$\mu_1(X_1)$	LW	2.781	4
	$\mu_2(X_1)$	MV	3.184	11
	$\mu_3(X_1)$	HV	3.589	19
$X_2 \in [1;5]$				
	$\mu_1(X_2)$	VLC	0.4246	1
	$\mu_2(X_2)$	LC	0.4246	2
	$\mu_3(X_2)$	MC	0.4246	3
	$\mu_4(X_2)$	HC	0.4246	4
	$\mu_5(X_2)$	VHC	0.4246	5
$X_3 \in [0.05;365]$				
	$\mu_1(X_3)$	VLT	0.5	0.05
	$\mu_2(X_3)$	LT	1	1.5
	$\mu_3(X_3)$	MT	1.8	5
	$\mu_4(X_3)$	HT	13.86	18
	$\mu_5(X_3)$	VHT	280.8	365
$X_4 \in [0;10]$				
	$\mu_1(X_4)$	LV	3.426	0
	$\mu_2(X_4)$	MV	1.29	5.579
	$\mu_3(X_4)$	HV	0.78	8.037
	$\mu_4(X_4)$	CV	0.8875	10
$Y \in [0;100]$				
	$\mu_1(Y)$	VLR	10.62	0
	$\mu_2(Y)$	LR	10.62	25
	$\mu_3(Y)$	MR	10.62	50
	$\mu_4(Y)$	HR	10.62	75
	$\mu_5(Y)$	VHR	10.62	100

To form the initial base of rules, we will use an approach based on the generation of many rules, based on possible combinations of vague statements in the prerequisites and conclusions of the rules, according to which the maximum number of rules in the database is determined [27]:

$$I = I_1 \cdot \cdots \cdot I_m \cdot I_y . \tag{12}$$

Thus, for the model being developed, the number of rules in the initial base will be $3 \cdot 5 \cdot 5 \cdot 4 = 300$ rules.

According to the structure of the rules (10), which for the developed model have a general look of:

$$P_i : \text{It } X_1 \text{ is } T_i(X_1) \text{ and } X_2 \text{ is } T_i(X_2) \text{ and } X_3 \text{ is } T_i(X_3) \text{ and } X_4 \text{ is } T_i(X_4), \text{ then } Y \text{ is } T_i(Y) , \tag{14}$$

the initial database of rules was formed, consisting of 300 rules, fragment of which of the 10 rules is shown in Figure 4.

Tools are allowed when creating a rule to indicate weight, that is, the significance of the rule, which has a definition area [0;1]. In the built database, all rules, by default, have the same weight of 1.

DOI 10.15588/1607-3274-2022-4-12

1. If (X1 is LW) and (X2 is VLC) and (X3 is VLT) and (X4 is LV) then (Y is VLR) (1)
2. If (X1 is LW) and (X2 is VLC) and (X3 is VLT) and (X4 is MV) then (Y is VLR) (1)
3. If (X1 is LW) and (X2 is VLC) and (X3 is VLT) and (X4 is HV) then (Y is LR) (1)
4. If (X1 is LW) and (X2 is VLC) and (X3 is VLT) and (X4 is CV) then (Y is LR) (1)
5. If (X1 is LW) and (X2 is VLC) and (X3 is LT) and (X4 is LV) then (Y is VLR) (1)
6. If (X1 is LW) and (X2 is VLC) and (X3 is LT) and (X4 is MV) then (Y is VLR) (1)
7. If (X1 is LW) and (X2 is VLC) and (X3 is LT) and (X4 is HV) then (Y is LR) (1)
8. If (X1 is LW) and (X2 is VLC) and (X3 is LT) and (X4 is CV) then (Y is LR) (1)
9. If (X1 is LW) and (X2 is VLC) and (X3 is MT) and (X4 is LV) then (Y is VLR) (1)
10. If (X1 is LW) and (X2 is VLC) and (X3 is MT) and (X4 is MV) then (Y is VLR) (1)

Figure 4 – Fragment of model product rules base

5 RESULTS

The use of a fuzzy model provides a more flexible processing of inaccurate /substandard factors of security risk and allows you to proceed to the numerical representation of any characteristcs. The proposed fuzzy model and methods can be used both to assess specific types of security risks of ERP system resources and to the overall risk of security of the ERP system.

In a real enterprise, the use of a fuzzy model involves the implementation of a certain block of preparatory work such as: identify specific objects of protection of the, ERP-system; make a list of threats and possible vulnerabilities; to make a list of current threat/vulnerability for ERP-systems (taking into account the peculiarities of business processes); assess the probabilities of implementing a threat using the specified vulnerability; to assess the consequences of the threat, the impact of the threat on the integrity, confidentiality, availability and observation of in formation; perform a risk assessement from the implementation of the threat; determine the level of risk and
provide recommendations for the need to process it; assess security risk by asset and business process.

The prospect of developing the proposed model is the use of adaptive neuro-fuzzy product model, which will allow reassessing risk in case of changes in the values of factors, changes in the product base of rules or in case of new risk.

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 about the value of fuzzy 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 security, including noncompliance with regulatory standards, can lead tofinancial 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 organiztion'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 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.

CONCLUSIONS

The developed fuzzy evaluation model of the ERP-system was practically implemented using the Matlab en-

DOI 10.15588/1607-3274-2022-4-12

vironment. The implemented model was improved by using a fuzzy output algorithm in the form of a fuzzy production network, namely the ANFIS system of the Fuzzy Logic Toolbox package of the Matlab environment, which implements the Sugeno fuzzy output algorithm. Model training was conducted on different volumes and content of educational data, as well as for different number of learning epochs. The data obtained as a result of the analysis showed:

1) ANFIS-systems have a much lower estimate of error in obtaining the result of a logical conclusion;

2) increasing the size of the sample and increasing the number of learning epochs both individually and together improve the quality of the conclusion by increasing the accuracy of the result.

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.

REFERENCES

1. Leighton J. Security Controls Evaluation, Testing and Assessment Handbook. Syngress, 2016, 678 p.
2. Methody zahysty systemy upravlinnia informaciinoiu Bezpekou [Tekst], DSTU ISO/IES 27001, 2015. Chyn. 2017.01.01. Kyiv, DP “UkrNDNC”, 2016, 22 p.
3. Informaciini tehnolohii. Metody zahystu. Zvid praktyk shchodo zahodiv informaciinoi bezpeky [Tekst], ISO/IES 27002:2015, 2015, Chyn. 2017.01.01. Kyiv, DP “UkrNDNC”, 2016.
4. Informaciini tehnolohii. Metody zahystu. Systemy ke-ruvannia informaciinoiu bezpekoiu. Nastanova [Tekst], DSTU ISO/IES 27003, 2018, Chyn, 2018.01. 01. Kyiv, DP “UkrNDNC”, 2018.
5. Informaciini tehnolohii. Metody zahystu. Systemy ke-ruvannia informaciinoiu bezpekoiu. Monitoring, Vy-miriuvannia, analisuvannia ta ociniuvannia [Tekst], DSTU ISO / IES27004, 2015, 2018, Chyn. 2018.01. 01. Kyiv, DP “UkrNDNC”, 2018.
6. Informaciini tehnolohii. Metody zahystu.Upravlinnia Rysykamy informaciinoi bezpeku [Tekst], DSTU ISO / IES 27001: 2015, Chyn. 2015.01.01. Kyiv, DP “Ukr-NDNC”, 2016.
7. Ehlakov Yu. P. Nechyotkaya model ocenki riskov Prodvizheniya prohramnyh produktov, *Biznes-informatika*, 2014, No. 3 (29), pp. 69–78,
8. Gladysh S. V. Predstavlenie znanii ob upravlenii in-Cyndentami informacionnoj bezopasnosti posredstvom Nechyotkich vremennyh raskrashennyh Setei Petri, *Mizhnarodnyi naukovo-tehnichnyi zhurnal “Informaciini tehnolohii ta kompyuterna inzheneriia”*, 2010, No. 1 (17), 2010, pp. 57–64.
9. Nieto-Morote A. A., RuzVila 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. Kozhukhivskyi A. D., Kozhukhivska O. A. Developing a Fuzzy Risk Assessment Model for ERP-Systems (Tekst) *Radio Electronics, Computer Science, Control*, 2022, No. 1, pp. 106–119. DOI 10. 15588/1607-3274-2022-1-12
12. Baskerville R. An analysis survey of information sy-stem security design methods: Implications for Infor-mation Systems Development, *ACM Computing Survey*, 1993, pp. 375–414.
13. Peltier T. R. Facilitated risk analysis process (FRAP). Auerbach Publication, CRC Press LLC, 2000, 21 p.
14. Alberts C., Dorofee A. Managing Information Security Risks: The Octave Approach. Addison-Wesley Professional, 2002, 512 p.
15. 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
16. Suh B., Han I. The IS risk analysis based on business model, *Information and Management,* 2003, Vol. 41, No. 2, pp. 149–158.
17. Karabacaka B., Songukpinar I. ISRAM: Information security risk analysis method, *Computer & Security, March,* 2005, pp. 147–169.
18. 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
19. 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.
20. Yazar Z. 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
21. Korchenko A. G. Postroenie system zashhity informa-cii na nechetkih mnozhestvah. Teoriya i prakticheskie resheniya. Kyiv, MK-Press, 2006, 320 p.: IL.
22. Karpenko A.C. Lohika Lukasevicha i prostye chisla. Moscow, Nauka, 2000, 319 p.
23. Teoriya algoritmov ta matematychna lohika [Elektronnyi resurs], *Materialy dystanciinogo navchnnya sumskogo derzhavnogo universytetu.* Rezhim dostupu: https://dl. sumdu. edu.ua /textbooks/ 85292/354091/index.html
24. Kruglov V. V., Borisov V. V., Fedulov A. C. Nechitki modeli i seti. Moscow, Goriachaya liniya, Telekom, 2012, 284 p. IL.
25. Kruglov V. V., Borysov V. V. Iskusstvennye neironnye seti. Teoriya i praktika. Moscow, Goriachaya liniya, Telekom, 2002, 382 p.: Il.
26. Zade L. Ponyatie lingvisticheskoi pemennoi i ego Primenenie k ponyatiyu priblizhyonnykh reshenii, Per. s Angl. Moscow, Mir, 1976, 166 p.
27. Jang J.-S. R. ANFIS: Adaptive Network – based Fuzzy Inference System, *IEEE Trans. On System, Man and Cybernetics,* 1993, Vol. 23, No. 3, pp. 665– 685.
28. 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
29. National vulnerability database Release [Elektronnyi resurs], *National Institute of Standards and Technology*. Rezhim dostupu: https://nvd.nist.gov
30. FUZZY LOGIC TOOLBOX [Elektronnyi resurs], *Czentr Inzhenernykh Tekhnolohii i Modelirovaniia Eksponenty*, Rezhim dostupu: https://exponenta.ru/fuzzy-logic-toolbox.

Received 10.08.2022.
Accepted 20.10.2022.

УДК 004.94

МОДЕЛЮВАННЯ ОЦІНКИ РИЗИКІВ ERP-СИСТЕМИ

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

DOI 10.15588/1607-3274-2022-4-12

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

АНОТАЦІЯ

Актуальність. Оскільки оцінка ризиків 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 су-б'єктивним, а оцінка ризиків залежить від практичних результатів, отриманих у процесі обробки ризиків загроз, які вже виникли під час функціонування організації та досвіду фахівців з 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 мо-делі розрахунку оцінки ризику 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 нечіткої моделі оцінки ризиків безпеки та захисту систем ERP шляхом використання нечітких нейронних моделей.

Метод. Для побудови моделі розрахунку оцінки ризику безпеки пропонується використовувати нечітку про-дукційну 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 реалізовано нечітку продукційну модель оцінювання ризиків та бази правил нечіткого логічного висновку з використанням пакету прикладних програм MATLAB та пакету розширення Fuzzy Logic Toolbox, а також покращено за рахунок введення адаптивності моделі до експериментальних даних шляхом впровадження в модель нейро-нечітких компонентів. Розглянуто використання нечітких моделей для вирішення задач оцінки ризиків 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 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: безпека, нечітка логіка, нечітка продукційна модель, оцінка ризиків, захищенність, ERP-система.

УДК 004.94

МОДЕЛИРОВАНИЕ ОЦЕНКИ РИСКОВ 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 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 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. «человекоподобный» стиль соображений нечетких систем с обучением и моделированием психических явлений нейронных сетей. Для построения модели расчета оценки рисков 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 нечеткой модели оценки рисков безопасности и защиты систем ERP с использованием нечетких нейронных моделей.

Метод. Для построения модели расчета оценки рисков 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 реализованы нечеткая модель оценки рисков и основы правил нечеткого логического заключения с использованием пакета прикладных программ MATLAB и пакета расширения Fuzzy Logic Toolbox, а также улучшено за счет введения адаптивности модели к экспериме-нтальным даным путем внедрения в модель нейро-нечетких

DOI 10.15588/1607-3274-2022-4-12

компонентов. Рассмотрено использование нечетких моделей для решения проблем оценки рисков 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 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 переменных модели. Выбрана структура базы данных нечетких правил продукта – MISO-структура. Построена структура нечеткой модели. Выявлены нечеткие переменные модели.

КЛЮЧЕВЫЕ СЛОВА: безопасность, нечеткая логика, нечеткая продукционная модель, оценка рисков, защищенность, ERP-система.

ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. Leighton J. Security Controls Evaluation, Testing and Assessment Handbook / J. Leighton. – Syngress, 2016. – 678 p.
2. Методи захисту системи управління інформацій-ною безпекою [Текст]: ДСТУ ISO/IEC 27001:2015. – 2016. – Чин. 2017.01.01. – Київ : ДП «УкрНДНЦ», 2016. – 22 с.
3. Інформаційні технології. Методи захисту. Звід пра-ктик щодо заходів інформаційної безпеки [Текст] : ДСТУ ISO/IEC 27002: 2015. – 2015. – Чин. 2017. 01.01. – Київ : ДП «УкрНДНЦ», 2016.
4. Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Настанова [Текст] : ДСТУ ISO/IEC 27003: 2018.–2018. – Чин. 2018.10.01. – Київ : ДП «УкрНДНЦ», 2018.
5. Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Моніторинг, вимірювання, аналізування та оцінювання [Текст]: ДСТУ ISO/IEC 27004: 2018. 2018. – Чин. 2018.10. 01. – Київ : ДП «УкрНДНЦ», 2018.
6. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки [Текст]: ДСТУ ISO/IEC 27005:2015.–2015.–Чин. 2017.10.01. – Київ : ДП «УкрНДНЦ», 2016.
7. Ехлаков Ю. П. Нечеткая модель оценки рисков продвижения программных продуктов / Ю. П. Ехлаков // Бизнес-информатика. – 2014. – №3 (29). – С. 69–78.
8. Гладыш С. В. Представление знаний об управлении инцидентами информационной безопасности посредством нечетких временных раскрашенных сетей Петри / С. В. Гладыш // Міжнародний науково-технічний журнал «Інформаційні технології та комп'ютерна інженерія». – 2010. – № 1(17). – С. 57–64.
9. Nieto-Morote A. A. Fuzzy approach to construction Project risk assessment / A. Nieto-Morote, F. RuzVila // 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.
11. Kozhukhivskyi A. D. Developing a Fuzzy Risk Assessment Model for ERP – Systems (Tekst) /A.D. Kozhukhivskyi, O.A. Kozhukhivska // Radio Electronics, Computer Science, Control. – 2022. – No. 1. – P. 106–119. DOI 10. 15588/1607-3274-2022-1-12
12. Baskerville R. An analysis survey of information sy- stem security design methods: Implications for Information Systems Development / R. Baskerville // ACM Computing Survey. – 1993. – P. 375–414.
13. Peltier T. R. Facilitated risk analysis process (FRAP) / T. R. Peltier. – Auerbach Publication. – CRC Press LLC, 2000. – 21 p.
14. Alberts C. Managing Information Security Risks: The Octave Approach / C. Alberts, A. Dorofee. – Addison-Wesley Professional, 2002. – 512 p.
15. 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
16. 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.
17. Karabacaka B. ISRAM: Information security risk analysis method / B. Karabacaka, I. Songukpinar. – Computer & Security, March. – 2005. – P. 147–169.
18. 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
19. 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.
20. 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
21. Корченко А. Г. Построение систем защиты инфор-мации на нечетких множествах. Теория и практические решения / А. Г. Корченко – К. : МК-ПресС, 2006. – 320 с.: ил.
22. Карпенко А. С. Логика Лукасевича и простые числа / А. С. Карпенко. – М. : Наука, 2000. – 319 с.
23. Теорія алгоритмів та математична логіка [Електронний ресурс] / Матеріали дистанційного навчання Сумського державного університету. – Режим доступу: https://dl. sumdu. edu.ua /textbooks/ 85292/354091/index.html.
24. Круглов В.В. Нечеткие модели сети / В. В. Круглов, В. В. Борисов, А. С. Федулов. – М. : Горячая линия – Телеком, 2012. – 284 с.: ил.
25. Круглов В. В. Искусственные нейронные сети. Теория и практика / В. В. Круглов, В. В. Борисов. – М. : Горячая линия-Телеком, 2002. – 382 с.: ил.
26. Заде Л. Понятие лингвистической переменной и его применение к принятию приближенных решений / Л. Заде. – Пер. с англ. – М. : Мир, 1976. – 166 с.
27. 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, № 3. – P. 665– 685.
28. 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
29. National vulnerability database Release [Elektronnyi resurs] // National Institute of Standards and Technology. – Rezhim dostupu: https://nvd.nist.gov
30. FUZZY LOGIC TOOLBOX [Elektronnyi resurs] // Центр инженерных технологий и моделирования экспоненты – Rezhim dostupa: https:// exponenta.ru/fuzzy-logic-toolbox.

DOI 10.15588/1607-3274-2022-4-12