UDC 004.94

ERP-SYSTEM RISK ASSESSMENT METHODS AND MODELS

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 non-appearance is a major factor influencing the effectiveness of the assessment, is advisable use vague methods and models that are adaptive to non-computed 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.

Objective. The object of the study are neural models that combine methods of fuzzy logic and artificial neural net-works and systems, that is, human-like style considerations of fuzzy systems with training and simulation of mental phi novena of neural networks.

Method. The paper analyzes modern areas of research in the field of information protection in information systems, methods and technologies of information security risk Assessments, use of vague models to solve problems of information security risk assessment, as well as concept and con-struction of ERP systems and analyze problems of their security and vulnerability.

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 for the development of the structure of a fuzzy product model of risk assessment and the basis of the rules of fuzzy logical conclusion justified.

Conclusions. A vague risk assessment model of ERP systems is considered. You have selected a list of factors that affect information security risk. The methods of assessment of risks 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 for their processing in order to maintain the level of protection of the ERP-system are considered. The list of linguistic variable models is considered. The structure of the database of fuzzy product rules – MISO-structure is selected. Fuzzy variable models are considered.

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

ABBREVIATIONS

ALE – Annualized Loss Expectancy;

ARO – Annualized Rate of Occurrence;

ANFIS – Adaptive Network-based Fuzzy Inference System;

DB – Database;

DSTU – State standard of Ukraine;

CVE – Common Vulnerabilities and Exposures;

CVSS – Common Vulnerability Scoring System;

ERP – Enterprise Resources Planning;

ERP – System-Enterprise Recourses Planning System;

FIS– Fuzzy Inference System;

IES – International Electro-technical Commission;

ISO – International Organization for Standardization;

MIMO – Structure (Multi Inputs – Multi Outputs);

MISO – Structure (Multi Inputs – Single Output)**;**

SISO – Structure (Single Input – Single Output);

NVD – National Vulnerability Database;

RDBMS – relational database management system;

SUN TZY – Normative document on technical protection of information.

NOMENCLATURE

A – financial loss from the single threat implementations;

P_e – the probability of an event;

R – risk of threat implementation;

P_t – probability of threat;

V – vulnerability level;

$<\alpha, X, C(\alpha)>$ fuzzy variable: α – name of the variable, $\alpha \in A$; X – universal set (α definition area);

$C(\alpha)=\{\mu_\alpha(x): x \in X\}$ – indistinct set on X, describing the limit on the possible values of fuzzy variable α; μ– accessory function;

$< X, T(X), E, G, M >$ linguistic variable;

X – the name of the linguistic variable;

$T(X)$ – a set of values of linguistic variable (termplural), which imagines the name of fuzzy variables, the area of definition of each of which is a lot of E;

E – area definition variable (all range of its values);

G – a syntactic procedure that generates the names of a fuzzy variable, allows you to operate elements of the term set T(X), in particular, to generate new terms;

M – a semantic rule, which in accordance with each fuzzy variable X its value $\mu(x)$.

R – set of actual numbers;

$\mu_{A_{ij}}(x_j^1)$ – feature affiliations.

$M=\{\mu_i(x_j^1): i=\overline{1,n}\}$ –a set of functions of belongings;

$\mu_i(x_j^1)$ – the function of the i-th belonging to the Variable x_j^1 the i-th segment of the variable Value area;

i – number of segments area of the variable value.

DOI 10. 15588/1607-3274-2020-4-15

INTRODUCTION

Risk implies a combination of the probability of damage by overcoming the system of protection using vulnerabilities and the severity of such damage. Minimizing the risks is done by developing a "security policy" (behavioral scheme) and managing it. Thus, the concept of "risk of information breach" is based on an analysis of "causes of information security Brea chess "and" consequences of information security breaches".

Risk assessment is carried out in the simplest case by two factors: the probability of accident and the severity of possible consequences.

Object of research in this paper is the information security of ERP-systems.

Subject of research – models and methods for assessing information security risks.

The purpose of this work is to improve the quality of information security and ERP systems risk assessment with fuzzy neural models.

1 PROBLEM STATEMENT

As part of the business risk of an enterprise, the risk of information security is defined as a product of loss (financial) from breach of confidentiality, integrity, authenticity or availability of information resources (the severity of consequences) for the likelihood of such infringement (probability of event):

$$R=A\cdot P_e, \tag{1}$$

Vulnerability:

$$P_e=P_t\cdot V. \tag{2}$$

The level of systemic risk is calculated as the sum of risks for all assets and each threat, taking into account the vulnerabilities and the effect of the taken countermeasures as the difference between the amount of planned costs for countermeasures and the total loss assessment at the determined system risk level.

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 was within the acceptable limit of the senior management, and consists of four main steps: Assessment of security risks, testing and oversight, risk mitigation and operational security.

Risk managers and decision-making organizers use risk assessments to determine which risks are reduced through control and which to take or transmit.

The assessment of information security risks is the process of identifying the vulnerable situations, threats, the probability of their occurrence, the level of risks and consequences related to organizational assets, as well as the control that can mitigate these threats and their consequences. It offers readers:

1) Assess the probability of threats and vulnerabilities that are possible; 2) Calculation of an impact that may that are possible; 3) Calculation of an impact that may have a threat to each asset; 4) Determination of quantitative (measurable) or qualitative (described) cost of risk.

Information security risk assessment is divided into three general stages:

1).Risk identification; 2).Riskanalysis;3).Risk Assessment.

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.

Complete risk assessment process should also include two more steps: Recommendations for monitoring and documentation of results.

According to the results of the risk assessment, it is decided that the choice of means to influence the risk in order to minimize the damage from the implementation of threats in the future. The following methods of exposure to risk are used.

The following methods of exposure to risk are used. Risk reduction – reduction of possible damage or probability of adverse events. This can be achieved as this: exclusion of risk; reducing the likelihood of risk; reduction of possible losses.

Preservation of risk (acceptance) – provides for the refusal of actions aimed at compensation (without Financing), compensation of it from the sources of the Organization (Risk fund, self-insurance Fund), or with the involvement of external sources (subsidies, loans etc.). The most commonly refers to threats with low damage and low probability of occurrence.

Risk transfer – transfer of responsibility for it to third parties (most often for remuneration) while maintaining the existing level of risk.

2 REVIEW OF THE LITERATURE

There are two main approaches to assessing risk: qualitative and quantitative approaches. The third approach, called mixed or hybrid, combines elements of qualitative and quantitative approaches.

Quantitative assessments of the risk of information security use mathematical formulas for determining the exposure factor and the expected loss of one or every threat, as well as the probability of a threat implementation, called the annual rate of ARO. These figures are used to estimate the amount of resources (money) that will be lost annually to vulnerabilities used, called the annual duration of ALE loss. By using the received figures, the organization can plan to monitor this risk if the countermeasure is available and cost effective. These numbers allow for the analysis of costs and benefits for each countermeasure and the threat to the asset. Countermeasures that reduce the annual duration of damages more than their annual costs should be applied if there is sufficient resource to use the countermeasure.

The advantages of using this approach are the ability to quantify the consequences of incidents, analyze costs and benefits when choosing remedies and get a more accurate definition of risk.

DOI 10. 15588/1607-3274-2020-4-15

The disadvantages include the dependence of quantitative indicators on their volume and accuracy of the measurement scale, inaccuracy of results, the need to enrich quality description, a large cost of the analysis, which requires more experience and modern tools.

Qualitative risk assessments of information security use experience, judgment and intuition, not mathematical formulas. Qualitative risk assessment may use surveys or questionnaires, interviews and group sessions to determine the level of threat and the annual loss duration. This type of risk assessment is very useful when it is too difficult to attribute values to a particular risk. Qualitative assessments of information security risks tend to be well perceived because they involve many people at different levels of the organization; they do not require a large number of mathematical computing, but the results tend to be less accurate than the results achieved by quantitative evaluation.

The disadvantages of approach are the inability to determine the probability and results, using numerical measures and approximate overall nature of the results.

It is possible to use a mixed approach to information security risk assessments. This approach combines some elements of both quantitative and qualitative assessments.

This approach is to assess greater credibility through presenting difficult facts, but it also engages people inside the organization to obtain an individual understanding. The disadvantage of this approach is that its implementation may take longer. However, a mixed approach can lead to better data than what these two methods can get separately.

Information risk assessment involves the use of various technologies, documents or software tools.

The methodology for assessing information security risks involves a sequence of actions that are necessary, as well as a tool (software product) to assess the risks at the enterprise.

Information risk assessment is carried out using various technologies, documents or software. The methodology for assessing information security risks is understood by a systematized sequence of actions (step-by-step instructions) that need to be done and a tool (software product) for risk assessment at the enterprise.

Currently, the following standards are operating in Ukraine: ISO 27001, ISO 27002, ISO 27003, ISO 27004 and ISO 27005 [1–5].

Based on the differences in risk analysis approaches, ways to review risk elements, functionality and other assessment methods, all risks vary as follows:

1. Graphical – methods that involve visualization of objects of analysis and processes of interaction between them, while graphs, trees or diagrams are built, allowing different ways to display information about the objects studied. In most cases, these methods only allow identification of risk elements and methods of interaction between them.

2. Mathematical methods, which define the properties of objects and their interaction with the help of some formal languages describing the laws of functioning, changes of properties, etc. These methods allow not only identifying elements, but also to analyze their behavior, changing their properties and influencing on other elements.

3. Linguistic – Methods that do not involve any tools and programs, and require only a team of person is responsible for risk analysis. At the same time, all the stages of risk assessment, as possible, assume only oral communication between groups of persons, during which the elements of risk are identified, the assumptions about their behavior are made and an approximate assessment of opportunities and losses is carried out. This class of methods is most popular and easy to use, but is not always able to lead to an adequate assessment of the situation.

In recent years, highly intensively developed methods of analysis and risk assessment, which are based on the elements of Fuzzy logic. Such methods allow to change the close tabular methods of rough assessment of risks on a mathematical method, as well as to significantly expand the possibilities of mathematical risk analysis methods [6–8].

The mechanism of risk assessment through fuzzy logic in general is imagines with itself the expert system. The knowledge base of such system will make rules that reflect the logic of the relationship of input values of risk factors and risk level. In the simplest case, a table describs this logic in general, which more accurately reflects the real relationships of factors and consequences. Such connections are formalized and described by the production rules of the “if-something” type. In addition, the fuzzy logic mechanism provides for the formation of factor ratings levels and their representation in the form of fuzzy variables. The process of shaping this type of assessments in general is quite complex, because it requires a large number of sources of information, consideration of their quality and the use of experts experience.

To determine the level of risk, it is advisable to use the theory of fuzzy sets, which allows you to describe vague concepts and knowledge, operate them and draw vague conclusions. The theory of fuzzy models used 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.

There are developed models of fuzzy conclusion of Mamdani, Sugeno, Larsen and Tsukamoto [9]. The most commonly used in practice are Mamdani and Sugeno algorithms. The main difference between them is the method of specifying the values of the output variable in the rules constituting the knowledge base. In systems such as Mamdani, values of input variables are given in fuzzy volumes, in Sunio-type systems – as linear coexistence of input variables. For tasks, which are identifications that are more important, it is advisable to use the algorithm Sugeno, and for tasks in which more important is the explanation and justification of the decision, the Mamdani algorithm will have an advantage.

DOI 10. 15588/1607-3274-2020-4-15

3 MATERIALS AND METHODS

A fuzzy plural (fuzzy set) is a set of arbitrary elements that cannot be accurately stated whether these elements have some distinctive properties used for fuzzy values.

Therefore, the fuzzy set A is defined as many ordered pairs consisting of elements of X universal set X and relevant degrees of belonging to the

$$\mu_A : A=\{(x,\mu_A(x))\vdots x\in X\},$$

μ_A – is the indicator affiliation feature (or just a feature of belonging) that takes value in the ordered plural M = [0; 1] and indicates the degree (or level) of the element x subset of A.

The degree of belonging μ_A is a subjective measure of , as the $x\in X$; element, corresponds to the notion whose meaning is formalized by A [10] fuzzy set.

Classical logic cannot work with vague concepts because all statements in formal logical systems can have only two mutually exclusive rules: "True" with the meaning of Truth "1" and "not true" with the meaning of truth "0".

One of the attempts to escape from the double-digit binary logic to describe uncertainty was the introduction of Lukasevich [11] three-digit logic with a third State "may" with the value Truth "0.5". By typing fuzzy sets in the review, Zade [12] suggested summarizing the classical binary logic based on the consideration of the infinite number of truth-values.

In the suggested version of vague logic, the meanings of true statements are summarized to the interval [0; 1], that is, include both individual cases of classical binary logic and Lukasevich's trivial logic. This approach allows us to consider statements with different values of truth and to perform reasoning with uncertainty.

"Perhaps true", "perhaps wrongly", etc. The higher the confidence in the truth expression, the closer the value of the degree of truth to "1". In the boundary cases "0", if there is absolute certainty in the false statement, and "1", if there is an absolute sure of the truth statement. The fuzzy reflection of T: $\Omega \rightarrow$ [0, 1] acts on a multitude of fuzzy statements $\Omega = A, B, C$. In this case, the value of the $\Omega A\in$ [0, 1] and is an estimate of uncertainty [10].

Like normal logic, fuzzy logic uses operations to construct complex statements.

1. Logical objection – "Not A", "false as A", the value of truth of which: $T\neg A=1-TA$.

2. Logical Conjunction – "A and B", who's meaning is truth:

$$TA\cap B=\min(TA;TB). \quad (3)$$

3. Logical disjunction – "A or B", whose meaning is truth:

$$TA\cup B=\max(TA;TB). \quad (4)$$

4. Fuzzy momentum is "with A should B", " if A, then B", whose truth-values are:

$$TA\supset B=\max(\min(TA;TB);1-TA).$$

5. Indistinct equivalence – "A is equivalent to B", whose truth-values are? $TA\equiv B=\min(\max(T\neg A;TB);\max(TA;T\neg B))$.

In describing objects and phenomena by means of Fuzzy sets, the concept of fuzzy and linguistic variables [10, 13, and 14] is used.

Fuzzy variable characterized by the following expression

$$<\alpha,X,C(\alpha)>.$$

Fuzzy plural on X, which describes the limitations on possible values of a fuzzy variable α, has a drawer:

$$C(\alpha)=\{\mu_\alpha(x)\vdots x\in X\}.$$

Linguistic variable is a subjective assessment of a person, which is expressed as a natural language, regarding a specific value of a numerical variable.

Linguistic variable is called set

$$<X,T(X),E,G,M>. \quad (5)$$

For example, the expert determines the thickness of the manufactured product using the concepts of "low thickness", "average thickness" and "high thickness", with the minimum thickness equal to 10 mm, and the maximum – 80 mm.

Formalization of this description can be carried out with the help of the following linguistic variable (5):

We will present: X – thickness of the product; $T(X)$ – {"Small thickness", "average thickness", "high thickness"}; E – [10, 80]; G –procedure for the formation of new term with the help of connections "i", "or" and modifiers such as "very", "not"", ""slightly"" etc. For example: ""Small or medium thickness", "Very small thickness", etc.; M – Task Procedure X = [10, 80] fuzzy subsets, A_1 = "small thickness", A_2 = "average thickness", A_3 = "large thickness".

4 EXPERIMENTS

The term-many and extended term set in the conditions of an example can be characterized by the functions of belonging (see Fig. 1–2).

Fuzzy numbers are fuzzy variables defined in the metric axis, which is a fuzzy number A defined as fuzzy for a set of real R numbers with function affiliation R with feature affiliations $\mu_{A_x}(x) \in [0,1]$, x is a real number, i.e. $\in A$.

DOI 10. 15588/1607-3274-2020-4-15

The system of Fuzzy logic conclusion is the process of obtaining fuzzy conclusions in the necessary management object based on fuzzy conditions or preconditions, representing information about the current state of the object.

The basis for a fuzzy logical conclusion is the indistinct system, which consists of linguistic rules. Let *x* and *y* are input and output linguistic variable; *A* and *B* are some fuzzy sets (feature affiliations) taken from the term sets of *x* and y variables, respectively.

The linguistic rule of vague conclusion "if any" looks like: R = "$x \in A$, then $y \in B$", where R "$x \in A$" is a vague statement, called the rule

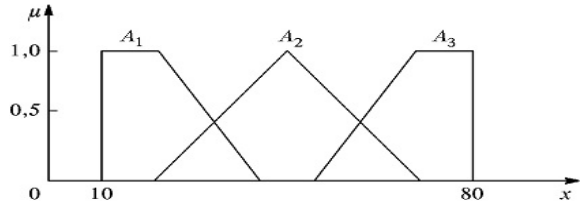

Figure 1 – The accessories of fuzzy sets: "small thickness" = A_1, "average thickness" = A_2, "high thickness" = A_3

Condition, "$y \in B$" is a vague statement called the conclusion rules.

Fuzzy logical conclusion combines all basic concepts of the theory of fuzzy sets: Functions of belonging, Linguistic variables, methods of fuzzy implication, etc.

The fuzzy output system consists of five functional blocks [9, 15 and 16].

1. Block of Phazyfication. Phazyfication (introduction of fuzziness) is the setting of the correspondence between the numerical value of the input variable of the fuzzy Output system and the value of the function of belonging to the corresponding term of the linguistic variable. At the stage of phazyfication the value of all input variables of the system fuzzy output, received externally with respect to the system of fuzzy output method.

In case of a clear value of the input variable x_j^1 the degree truth fuzzy saying "$x_j^1 \in A_{ij}\, x_j^1$" is determined by the.

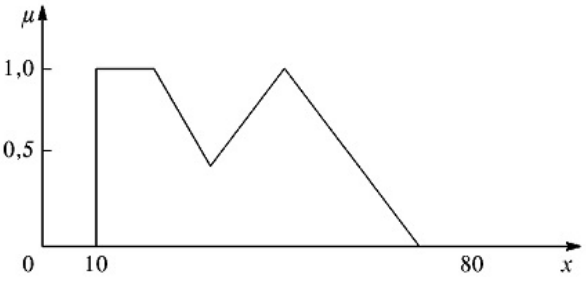

Figure 2 – The function of the fuzzy set "small or average thickness" = $A_1 \cup A_2$

Value of the $\mu_{A_{ij}}(x_j^1)$ function. When the same fuzzy value is specified, the input variable $\tilde{x}_j^1$ the degree of truth of the appropriate fuzzy statement "$\tilde{x}_j^1 \in A_{ij}^1$" in the premise is determined based on one of the fuzzy conjunction operations (3), e.g. operation min – conjunction $\mu_{A_{ij}^1}(x)$ = min $\{\mu_{\tilde{x}_j}(x_j),\ \mu_{A_{ij}}(x_j)\}$, or the operation of algebraic product $\mu_{A_{ij}^1}(x_j) = \{\mu_{x_i}(x_j) * \mu_{A_{ij}}(x_j)\}, \forall x_j \in X_j$.) For an example of fuzziness, see Fig. 3 [16].

2. The base of the system rules of fuzzy output is intended for the formal presentation of empirical knowledge of experts in a particular subject area in the form of fuzzy product rules. Thus, the base of fuzzy product rules of fuzzy output system is a system of fuzzy product rules; reflecting expert's knowledge on methods of management of the object in different situations, nature of its functioning in different conditions, etc. i.e., contains the formalized human knowledge.

Depending on the number of fuzzy statements in the prerequisites and the conclusions database of the fuzzy product model, the structure of one of the following types can be represented [17]:

– SISO-Structure;
– MISO-Structure;
– MIMO Structure.

3. Database. It contains definition of the belonging to the fuzzy sets function used in fuzzy rules:

$$M = \{\mu_i(x_j^1) : i = \overline{1,n}\}.$$

4. Decision-making unit (block of vague logical conclusion). Performs withdrawal operations based on existing rules: aggregation of conditions – the procedure for determining the level of truthfulness of the rules of the system of fuzzy conclusion. Activation of conclusions – the procedure for determining the level of truthfulness of the conclusions of the product rules. Accumulation – the procedure for finding the function of belonging for each of the original linguistic variables specified by the set of rules [9].

5. Block of Dephazyfication. Dephazyfication in fuzzy output systems is the process of transition from the function of the source linguistic variable to its clear (Numeric) value. The purpose of dephazyfication is to obtain quantitative values for each output variable used by external means in relation to the fuzzy output system using the results of accumulating all outgoing linguistic variables [10].

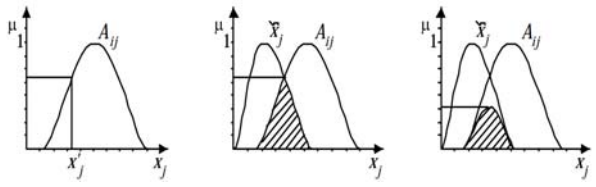

Figure 3 – Examples of entering a fuzzy with the use of clear values of the input variable x_j^1 (A) and fuzzy value of the input variable $\tilde{x}_j^1$ operation min-conjunct (B) and algebraic equal (C)

DOI 10. 15588/1607-3274-2020-4-15

Neural fuzzy networks have fuzzy values in different components of traditional neural networks based on the theory of fuzzy sets and fuzzy logic. Different types of intelligent systems have their own characteristics, for example, regarding the possibilities of learning, generealization and getting results, which makes them the most suitable for solving some classes of problems and less suitable for others.

Neural networks are convenient for the problems of pattern recognition, but are very inconvenient to explain how they perform recognition. They can automatically gain knowledge, but the process of their learning is often slow enough, and the analysis of the trained network is very complex (trained network is usually "black box" for the user). At the same time, some priori information (expert knowledge) to accelerate the learning process in the neural network is difficult to enter.

Systems with fuzzy logic, opposite, are easy to explain obtained with their help of conclusions, but they cannot automatically gain knowledge for their use in mechanisms Vive den. The need to break the universal sets into separate areas, as a rule, limits the number of input variables in such systems a small value.

Hayashi and Imura [18] have shown that a direct-spread neural network can approximated any system based on vague rules, and any direct-spread neural network can be aproximized by a system based on vague rules. In theory, systems with fuzzy logic and artificial neural networks are similar to each other, but in practice, they have their own advantages and shortcomings. This understanding has formed the basis for the creation of the apparatus of fuzzy neural networks, in which the output is made based on fuzzy logic, but the relevant affiliation functions are adjusted using methods of teaching neural networks, for example, method of reverse propagation error. Such systems not only use a priori information, but also can acquire new knowledge, being logically transparent.

Neuro-fuzzy network is the presentation of a fuzzy output system in the form of a neural network convenient for learning, analyzing and using. The structure of the neuro-fuzzy network corresponds to the main blocks of fuzzy output systems [19, 20].

Fuzzy models and algorithms of fuzzy output on their basis can be presented in the form of fuzzy products networks, in the structure of identical multilayered neural networks with direct signal distribution (feed forward), elements of each layer (or combination of layers), implementing a separate stage of fuzzy output in a fuzzy production model:

The first layer of neurons performs the function of introducing fuzziness (phazyfication); Hidden layers display a combination of fuzzy rules and implement the fuzzy output algorithm; The last layer performs the function of bringing to clarity (dephazyfication) of the original variable.

At present, a large number of different architectures of neuro-fuzzy networks are known [21, 22]:

– Fuzzy neural systems (fuzzy neural systems): In neural networks, fuzzy logic principles are applied to speed up the configuration process or improve the parameters;

– Fuzzy logic is only an instrument of neural networks and such a system cannot be interpreted in fuzzy rules, since it represents the "black box";

– Competing neuro-fuzzy systems (concurrent neuro-fuzzy systems): A fuzzy system and a neural network are working on one task without affecting each other's parameters;

– Parallel neuro-Fuzzy systems (cooperative neuro-fuzzy systems): Settings executed are with the help of neural networks, after which the fuzzy system functions in-dependently;

– Integrated (hybrid) neuro-fuzzy systems (Integrated neuro-fuzzy systems) – systems with close interaction of fuzzy logic and neural networks.

ERP is understood to be the concept of a coherent solution for accounting, control, planning and management of industrial and financial resources of the enterprise. Research firm Gartner Group to describe management systems that provide automation of planning, forecasting and financial management processes, production, logistics and marketing, accounting, product design, development of technological processes, etc. introduced the term. ERP is a global management standard proposed by the U.S. Manufacturing and Reserves Management Community.

5 RESULTS

ERP-System is a corporate integrated information system that implements the ERP concept, creating a single information environment for automation of planning, accounting, control, management and analysis of the main business processes of the enterprise.

The purpose of the ERP-system is to integrate all departments and structures of the company into a single information and technological computer network to meet all the needs of individual units.

The most common ERP systems are SAP, Oracle E-Business Suite, and Microsoft Dynamics.

The term ERP-system used in the following two meanings as:

1) information system for identification and planning of all resources of the enterprise, which are necessary for the sale, production, purchase and accounting in the process of fulfillment of client orders;

2) Methodology for effective planning and management of all resources of the enterprise, which are necessary for the sale, production, procurement and accounting when fulfilling customers orders in the spheres of production, distribution and service provision.

The typical ERP-system ensures the following tasks:

– financial management;
– Production management;
– Managing inventory formation and distribution;
– Management implementation and marketing;
– Management of customer retention;
– Supply management;

DOI 10. 15588/1607-3274-2020-4-15

– Project management;
– Personnel management;
– Service management;
– Quality assurance procedures.

In addition, the ERP-systems can support electronic data exchange with other software applications, as well as simulate situations that are related to planning and forecasting.

The use of ERP-Systems has the following advantages for the enterprise:

– Saving business in the long term by optimizing processes;
– Reducing operating expenses due to simplified business processes and best practices;
– Improve user collaboration;
– Reducing risk by increasing data integrity and financial control;
– Reducing management and operation costs through single-form and integrated systems;
– Providing a unified system that reduces IT, workforce and training costs;
– Obtaining real-time information by business;
– Facilitating the reporting and planning process with improved data and analytics;
– Increase accountability and security by controlling user rights.

In addition to advantages, the use of ERP-Systems has its drawbacks:

– deploying and maintaining the ERP-system can be very expensive;
– System deployment is a long and complicated process;
– Deploying a system of significant changes in management;
– ERP-systems are often less complex than specialized software and may not be used or replaced.

The objectives and tasks of information security in ERP-systems are as follows:

– mitigation of the risks of loss/disclosure;
– Compliance with state and intra corpo-rate standards of information protection;
– Data integrity protection;
– Guarantee of confidentiality of company's internal information.

ERP-systems have a complex architecture that combines various technologies, such as application servers, databases, inter-platform software, Web server, operating systems, ID management systems, etc. This complexity creates additional threats in terms of information security, which can occur in the design and development stages of the ERP-system, and during the implementation and operation stages [24].

The typical ERP-system consists of three components, connected through the client-server architecture (see Fig. 4):

– DB level;
– Application level;
– View level ((assigned to the user).

Data storage is carried out in the database (level DB), their processing is done on the server application (application level), and user interaction occurs through the client application (presentation layer). The environment, which unites all the components that are on different architectural levels of the ERP, is the network infrastructure.

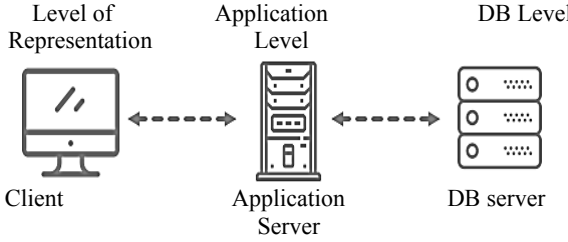

Figure 4 – Three level environment of ERP-systems

The three tiered client-server architecture can be deployed to a multilevel system.

Thus, the main aspects of security to consider when using the ERP-system, are:

– network security;
– Operating system security;
– DB security;
– application-level security;
– Protection of information on the client computer.

Ensuring security of information is necessary at each of the selected levels of the ERP-system, with the choice of information security mechanisms at the above levels depends on the specifics of a particular project and the risk level of each threat.

ERP systems are generally developed as large, complex, homo geneous, critical applications, and are usually developed and marketed as commercial extraordinary software by large software vendors such as SAP, Oracle, and Microsoft. ERP application development is theoretically based on the best industry practices, and they are designed to meet the broad business requirements covering a wide range of industries.

The functionality provided by commercial ERP-systems is designed in such a way that it can be configured to enable customers to incorporate their own business rules to meet specific business or industrial requirements. However, even after the configuration is completed, gaps often remain between the standard functions provided and specific requirements of the organization. Aiming to improve user adoption, most ERP systems customers complete the development of extensions and settings to make sure the app better supports business processes.

As ERP systems handle and store confidential personal and commercial information relating to employees, customers, suppliers, prospects and projects, further development beyond the original scheme exposes the application to increased risk of data breaches and non-compliance with the rules.

Custom development tends to constitute a very small portion of the entire application, but since they are accessing and processing the same sensitive data as the un-derlying program, they pose a significant security risk, which can potentially cost an organization's loss from a

DOI 10. 15588/1607-3274-2020-4-15

security breach. Extension and configuration of ERP applications is a specialized technical effort that requires, apart from the necessary development skills, to understand the architectural, functional and security model of the program, including proposed by the manufacturer best practices for product expansion. Here are some key aspects of security that enterprise developers must take into account when using ERP-applications:

1) Access Management. ERP application access control refers to the identification and management of authorized users, including giving them the appropriate roles needed to access processes and data. Access control is crucial for protecting data against unauthorized disclosure and change at the same time, maintaining appropriate availability levels for authorized users for operational purposes.

2) Database level security. At the heart of the ERP-system is RDBMS, which manages data entry/output and storage on the database server. The ability to customize data objects for different users is the key to any application and the basis for the security architecture to control access to data. Different database platforms provide tools for creating logical data objects that allow various users to view and handle common business objects differently.

3) Data encryption/ Data masking. In addition to functional access and data access controls, ERP data can be encrypted to mitigate exposure risks. Encryption is the most important tool for protecting sensitive information, more commonly used to transmit data, ensuring privacy and data integrity. For static data, encryption is not required for all security scenarios, but for sensitive personal data such as credit card numbers or passwords, this is an important tool. Data masking is a technique that is used to protect further data when encryption is not necessary. This allows you to move sensitive information in a way that will not prevent ordinary operations with a database such as maintaining reference integrity and limiting data types. Data values change but meet the schema requirements, allowing extracts from a database that usually contain sensitive data used for development purposes and testing. Data masking can be done using scripts, or special tools from developers of ERP systems.

Among the most common security problems, ERP-system can specify the following threats:

– The delay of updates that are necessary mainly to eliminate the vulnerabilities found in the software, and the installation of which is vital to prevent the possibility of using these vulnerabilities;

– Insufficient control of access rights, which, in the wrong setting, become potential internal risks to the system and threaten the integrity and confidentiality of information;

– Insufficient training of personnel working with the system, especially for new employees, who do not have deep knowledge of internal processes and errors, which may violate the principles of business processes execution;

– Insufficient checking of personnel having unimpeded access to system processes and ability to change the functionality of the ERP-system software;

– Use of unlicensed programs that can be used together with the ERP-system to achieve a single goal (for example, support for sales data in the ERP system, but run reports using Excel);

– Errors in implementation and configuration of the platform (customization, incorrect credentials, open ports, etc.) ERP system, which has many configuration files, can also potentially compromise the functioning of the process and data;

– Failure to comply with the regulatory norms and regulations intended to protect confidential information entails financial and reputational consequences.

Here is a list of common vulnerabilities of ERP-systems:

1) Complexity. ERP systems handle transactions and implement procedures to ensure that users have different access privileges. For example, in SAP R/3 system, there are actually automated object objects that allow to perform various actions on systems. In an organization of medium size can be created about one hundred types of transactions, each transaction usually requires that the smallest, two-object authorization. On the example of the SAP system, if the company has 200 users, there are approximately 800 000 (100 * 2 * 20 * 200) methods for configuring the security parameters of ERP-systems [25].

As complexity increases, the possibility of errors and conflicts of authority also increases [26].

2) Specificity of the software. Software vendors regularly correct the vulnerabilities because hackers track business applications to find and use security issues: SAP Monthly releases a hot fix, Oracle issues security fixes to quarterly, moreover, business applications become increasingly exposed to Internet or migrate to the cloud [27].

Internal business applications close to prying eyes, and this leads to the illusion of “safe as classified”, but in specific business applications find trivial and extremely dangerous security vulnerabilities that are rare in popular products.

3) Lack of competent specialists. Most ERP system training programs are designed to teach how to use system capabilities and pay little attention to ERP security and auditing [25]. The majority of companies understand the threats of ERP systems by the security service at best superficially [28]. Many companies do not pay proper attention to the security of the ERP system. The implementation consultants tend to be concerned only by having to deploy the system in time and invest in a pre-determined budget. Safety issues are considered secondary. Because of this, the security of the system turns out to be weak, and to identify and fix safety problemsa difficult and costly measure.

4) Lack of security auditing tools. ERP security Audit is done manually, as various tools with ERP, packages do not provide system security auditing tools. Manual audit

DOI 10. 15588/1607-3274-2020-4-15

is a complex and laborious process that increases the possibility of error [26].

5) A large number of settings. In the default, system settings there are many parameters and subtle settings that include the differentiation of rights for different Objects, such as transactions and tables. In all these mass settings, the task of securing is not easy even for a system. In addition, the customer somehow sharpens a large part of the ERP system settings, so that there are no two identical ERP systems. In addition, they develop their programs, safety of which should also be taken into account in the comprehensive assessment of the [29]. For this reason, it is difficult to develop a consistent approach or methodology for security audits.

We provide a list of vulnerabilities of ERP systems, according to the level of architecture [30].

Network layer:

1. Ability to intercept and modify traffic:

– lack of data encryption – data transfer between the client and the server client-server requests containing critical information can be intercepted or modified;

– password transfer in the open form.

2. Vulnerabilities in the encryption or authentication protocol:

– ash authentication;

– XOR password encryption;

– Introduction of the use of old authentication protocols;

– Non correct authentication algorithms.

3. Using a network protocol vulnerability would cause legitimate users to be denied access so that an attack could be carried out:

– Error in RFC the YSTEM_-CREATE_INSTANCE function (exploit the vulnerability allows arbitrary code);

– Error in RFC RFC_START_GUI function (exploiting the vulnerability also allows arbitrary code);

– Error in RFC the RFC_START_PROGRAM function (exploit the vulnerability could allow arbitrary code or learn about the RFC server configuration);

– Error in RFC the TRUSTED_SYSTEM_SECURITY function (exploit the vulnerabilities allows information about existing users and groups on the RFC server).

Operating system level:

1) OS software vulnerabilities: Any vulnerability in the OS used to access applications.

2) Weak OPERATING OS passwords:

– possibility of remote selection of passwords;

– Empty passwords for remote control tools such as RAdmin and VNC.

3) Unsafe OS settings:

– NFS and SMB (data can be accessed by an anonymous user via NFS or SMB);

– File permissions;

– The unsafe settings of the hosts (trusted hosts can be set by servers that can easily be captured by an attacker.

Application vulnerabilities.

– All possible vulnerabilities in web applications;

– Buffer overflow and format string in web servers and application servers;

– Dangerous access rights.

6 DISCUSSIONS

Modern scientific directions in the field of information protection in information systems, methods and technologies of information security risk assessment, use of fuzzi models to solve problems of information security risk assessment, as well as concepts and developments of ERP systems and problems of their security and vulnerability.

According to the results of the survey, the proposed factors influencing risk assessment use linguistic variables to qualities, and determine the system of qualitative assessments describe them and use fuzzy variables to assess their.

CONCLUSIONS

The approach to information security risk assessment of ERP systems may be further developed and lie the basis of the development of information risk management systems.

Ensuring security of information is necessary at each of the selected levels of the ERP-system, with the choice of information security mechanisms at the above levels depends on the specifics of a particular project and the risk level of each threat. Assessment of information security risks when using the ERP-system is necessary to develop recommendations for reducing the level of risks, as well as taking effective measures to ensure the information security of the entire enterprise.

ACKNOWLEDGEMENTS

The work was carried out at the Department of Information and Cybersecurity of the State University of Telecommunications within the framework of scientific researches.

REFERENCES

1. Methody zahysty systemy upravlinnia informaciinoiu Bezpekoiu [Tekst], DSTU ISO/IES 27001, 2015. Chyn. 2017.01.01. Kyiv, DP “UkrNDNC”, 2016, 22 p.
2. Informaciini tehnolohii. Metody zahystu. Zvid praktyk shchodo zahodiv informaciinoi bezpeky [Tekst], ISO/IES 27002:2015. 2015. Chyn. 2017.01.01. Kyiv, DP “UkrNDNC”, 2016.
3. Informaciini tehnolohii. Metody zahystu. Systemy keruvannia informaciinoiu bezpekoiu. Nastanova [Tekst]: DSTU ISO/IES 27003: 2018. Chyn. 2018.01. 01. Kyiv, DP “UkrNDNC”, 2018.
4. Informaciini tehnolohii. Metody zahystu. Systemy кeruvannia informaciinoiu bezpekoiu. Monitoring, Vymiriuvannia, analisuvannia ta ociniuvannia [Tekst]: DSTU ISO/IES 27004: 2015.–2018. Chyn. 2018.01.01. Kyiv: DP “UkrNDNC”, 2018.
5. Informaciini tehnolohii. Metody zahystu. Upravlinnia Rysykamy informaciinoi bezpeku [Tekst]: DSTU ISO / IES 27001: 2015 Chyn. 2015.01.01. Kyiv, DP “Ukr-NDNC”, 2016.

DOI 10. 15588/1607-3274-2020-4-15

6. Ehlakov Yu. P. Nechyotkaya model ocenki riskov Prodvizheniya prohramnyh produktov, *Biznes-informatika*, 2014, No. 3 (29), pp. 69–78.
7. 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), pp. 57–64.
8. Nieto-Morote A. A., Ruz-Vila F. Fuzzy approach to construction Project risk assessment, *International Journal of Project Management*, 2011, Vol. 29, Issue 2, pp. 220–231.
9. Korchenko A. G. Postroenie system zashchity Infor-macii na nechetkikh mnozhestvakh. Teoriya i Prakticheskiie resheniia. K., MK-Press, 2006, 320 p.
10. Teoriia alhoritmiv ta matematychna lohika [Elektronnyi resurs] / materialy dystanciinnogo Navchannia Sumskogo derzhavnogo universytetu, Rezhim dostupu: https://dl. Sum d u. edu.ua /textbooks/ 85292/354091/index.html.
11. Karpenko A. C. Lohika Lukacevicha i prostye chisla. Moscow, Nauka, 2000, 319 p.
12. Zade L. Ponyatie lingvisticheskoi peremennoi i ego primenenie k ponyatiyu priblizhyonnykh reshenii, Per. s Angl. Moscow, Mir, 1976, 166 p.
13. Nechyotkaya i lingvisticheskaya peremennye [Elektronnyi resurs], *Project Neuronus.com Portal Znanii Ob iskusstvennom intelekte.* Rezhim dostupu: https://neuronus.com/theory/fl/310-chast-3-nechetkaya-i-lingvisticheskaya-eremennye.html.
14. Neiro-nechitki merezhi. Nechitka logika v Matlab [Elektronnyi resurs] Yevropeiskii universitet Finansiv, informaciinykh system, menedzhmentu i Biznesu. *Kurs lekcii "Ekspertni systemy. Intelektualni Informaciini systemy"*, 2016, Rezhim dostupu: https://studfile.net/preview/5474324/page:3/.
15. Shutovskii V. O. Rozrobka adaptyvnogo algoritmu kilkisnoi ocinky ryzykiv z vykorystanniam metodiv nechitkoi logiky, *Teoretychni i Prykladni problemy fizyky, mathematyky ta Informatyky. Zbirka tez dopovidei uchasnyki,* 2008, P. 146.
16. Kruglov V. V., Borisov V. V., Fedulov A. C. Nechitki modeli i seti. Moscow, Goriachaya linia, Telekom, 2012, 284 s. Il.
17. 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 Mode Ling and Analysis,* 1990, pp. 489–494.
18. Kruglov V. V., Borysov V. V. Iskusstvennye neironnye seti. Teoriya i praktika. Moscow, Goriachaya liniya – Telekom, 2002, 382 p.: Il.
19. Zagalna kharakterystyka ta vlastyvosti neiro-nechitkykh merezh [Elektronnyi resurs] //Informaciinyi sait nechitkoi logiky. Rezhym dostupu: https://sites.google.com/site/ne4itkalogika, Nejro-necitki merezhi, zagalna harakteristika ta vlastivosti nejro-necitkih merezh.
20. Subbotin S. O. Podannia i obrobka znan u Systemach Shtuchnogo intelektu ta pidtrymky Pryiniattia Rishen: Navch. Posibnyk. Zaporizhzhia, ZNTU, 2008, 341 p.
21. Buckleya J. J., Hayashi Y. Fuzzy neural networks: asurvey, *Fuzzy sets and systems*, 1994, Vol. 66, Issue 1, pp. 1–13.
22. ERP-sistema (planuvannia resursiv pidpryemstva) [Elektronnyi resurs], Navchalni materialy onlain (pid-ruchniki-website). Rezhym dostupu: https://-pidruchniki.com / 1171062647760 / informatika Pidpriyemstva.
23. Zyryanov Yu. Informacionnaya bezopasnost ERP-sistem. CITforum. Rezhim dostupu: http://citforum.ru/gazeta/49/.
24. Hendrawirawan D., Tanriverdi H., Zetterlund C. ERP Security and Segregation Of duties Audit: A Framework for Building an utomated Solution, *Information systems control journal*, 2007, Vol. 2, 4 p.
25. Security issues in ERP. Security, Audit and Control Features SAP ERP 4th Edition, Audit Program. Isaca, 2015, 574 p.
26. Polyakov A. ERP Security Deserves Our Attention Now More than Ever [Elektronnyi resurs], *Forbes,* 2017. Rezhym dostupu: https://www.forbes.com/ sites / forbestechcouncil /2017/07/07/ erp-security-deserves-our-attention-now-more than-ever/.
27. Polyakov A. Bezopasnost SAP v cyfrakh [Elektronnyi resurs], Blog kompanii Digital Security. Khabrakhabar, 2012, Rezhym dostupu: https://habr.com/ru/company/Dsec/blog/146967/.
28. 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.
29. Goel S., Kiran R., Carg D. Vulnerability Management for an Enterprise Resource Planning System, *International Journal Of Computer Applications*, 2012, Vol. 53,No. 4, pp. 19–22.
30. National vulnerability database Release [Elektronnyi resurs], *National Institute of Standards and Technology*. Rezhym dostupu: https://nvd.nist.gov/vuln-metrics/cvss.

Received 12.10.2020.
Accepted 05.11.2020.

УДК 004.94

МЕТОДИ І МОДЕЛІ ОЦІНКИ РИЗИКІВ 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 невизначеності процесом, а невизначеності є основним фактором, що впливає на ефективність оцінки, доцільно використовувати нечіткі методи та моделі, що є адаптивними до нечислових даних. Формування нечітких оцінок факторів ризиків носять суб'єктивний характер, а оцінка ризику залежить від практичних результатів, отриманих у процесі обробки ризиків загроз, що вже виникали у процесі функціонування організації та досвіду фахівців з інформаційної безпеки.

Мета роботи – дослідження нейронечітких моделей, 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.

DOI 10. 15588/1607-3274-2020-4-15

Метод. У роботі оглянуто сучасні напрямки досліджень в сфері захисту інформації в інформаційних системах, методи та технології оцінювання ризиків інформаційної безпеки, використання нечітких моделей для вирішення задач оцінки ризиків інформаційної безпеки, а також концепцію та побудову ERP-систем та проаналізовано проблеми їх безпеки та вразливості.

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 для розробки структури нечіткої продукційної моделі оцінювання ризиків та бази правил нечіткого логічного висновку.

Висновки. Розглянуто нечітку модель оцінки ризику ERP-систем. Вибрано список факторів, що впливають на ризик інформаційної безпеки. Розглянуто методи оцінки ризиків інформаційних ресурсів та ERP-систем загалом, оцінки фінансових втрат від реалізації загроз, визначення виду ризику за його оцінкою для формування рекомендацій щодо їх обробки з метою підтримання рівня захисту ЕРП-системи. Розглянутий перелік лінгвістичних змінних моделей. Вибрано структуру бази даних нечітких правил продукту – MICO-структура. Розглядаються нечіткі змінні моделі.

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

УДК 004.94

МЕТОДЫ И МОДЕЛИ 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 информационной безопасности есть сложным и полным неопределенности процессом, а неопределенности есть основным фактором, что влияет на эффективность оценки, целесообразно использовать нечеткие методы и модели, что есть адаптивными до нечисловых данных. Формирование нечетких оценок факторов рисков имеют субъективный характер, а оценка рисков зависит от практических результатов, полученных в процессе обработки рисков погроз, что уже возникали у процессе функционирования организации и опыта специалистов с информационной безопасности.

Цель работы – исследования нейронечетких моделей, что комбинируют методы нечеткой логики и искусственных нейронных сетей и систем, то есть человекоподобного стиля мышлений нечетких систем с обучением и моделированием умственных свойств нейронных сетей.

Метод. В работе рассмотрены современные направления исследований в сфере защиты информации в информационных системах, методы и технологии оценивания рисков информационной безопасности, использования нечетких моделей для решения задач оценки рисков информационной безопасности, а также концепцию и построения ERP-систем и проанализировано проблемы их безопасности и уязвимости.

Результаты. Определены факторы, что влияют на оценку рисков, предложено использование лингвистических переменных для их описания и использования нечетких переменных для оценки их качеств, а также системы качественных оценок. Обоснован выбор параметров для разработки структуры нечеткой продукционной модели оценивания рисков и базы правил нечеткого логического заключения.

Выводы. Рассмотрено нечеткую модель оценки рисков ERP-систем. Выбрано список факторов, что влияют на риск информационной безопасности. Рассмотрены методы оценки риску информационных ресурсов и ERP-систем вообще, оценки финансовых втрат от реализаци погроз, определение типа риску за его оценкою для формирования рекомендаций относительно их обработки для поддержания уровня защищенности ERP-системы. Определен список лингвистических переменных модели; выбрано структуру базы нечетких продукционных правил – MISO-структура. Рассмотрено структуру нечеткой модели. Определены нечеткие переменные модели.

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

ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. Методи захисту системи управління інформаційною безпекою [Текст]: ДСТУ ISO/IEC 27001:2015. –2016. – Чин. 2017.01.01. –К. : ДП «УкрНДНЦ», 2016. – 22 с.
2. Інформаційні технології. Методи захисту. Звіт практик щодо заходів інформаційної безпеки [Текст]: ДСТУ ISO/IEC 27002: 2015. – 2015.– Чин. 2017. 01.01. – Київ: ДП «УкрНДНЦ», 2016.
3. Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Настанова [Текст]: ДСТУ ISO/IEC 27003: 2018. – 2018. – Чин. 2018.10.01. – К. : ДП «УкрНДНЦ», 2018.
4. 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.
5. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки [Текст]: ДСТУ ISO/IEC 27005:2015. – 2015. – Чин. 2017.10.01. – К. : ДП «УкрНДНЦ», 2016.
6. Ехлаков Ю. П. Нечеткая модель оценки рисков продвижения программных продуктов / Ю. П. Ехлаков // Бизнес-информатика. – 2014. – №3 (29). – С. 69–78.
7. 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), 2010. – С. 57–64.
8. Nieto-Morote 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.

DOI 10. 15588/1607-3274-2020-4-15

9. Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / А. Г. Корченко. – К. : МК-ПресС, 2006. – 320 с.: ил.
10. 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.
11. Карпенко А. С. Логика Лукасевича и простые числа / А. С. Карпенко. – М. : Наука, 2000. – 319 с.
12. Заде Л. Понятие лингвистической переменной и его применение к принятию приближенных решений / Л. Заде. – Пер. с англ. – М. : Мир, 1976. – 166 с.
13. Нечеткая и лингвистическая переменные [Електронний ресурс] / Проект Neuronus.com Портал знаний об искусственном интеллекте. – Режим доступу: https://neuronus.com/theory/fl/310-chast-3- nechetkaya-i-lingvisticheskaya-peremennye.html
14. Нейро-нечіткі мережі. Нечітка логіка в MatLab [Електронний ресурс] // Європейський університет фінансів, інформаційних систем, менеджменту і бізнесу. Курс лекцій «Експертні системи. Інтелетуальні інформаційні системи».– 2016. – Режим доступу: https://studfile.net/preview/ 5474324/page:3/.
15. Шутовський В. О. Розробка адаптивного алгоритму кількісної оцінки ризиків з використанням методів нечіткої логіки / В. О. Шутовський // Теоретичні і прикладні проблеми фізики, математики та інформатики. Збірка тез доповідей учасників. – 2008. – С. 146.
16. Круглов В. В. Нечеткие модели сети / В. В. Круглов, В. В. Борисов, А. С. Федулов. – М. : Горячая линия-Телеком, 2012. – 284 с.: ил.
17. 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.
18. Круглов В. В. Искусственные нейронные сети. Теория и практика / В. В. Круглов, В. В. Борисов. – М. : Горячая линия-Телеком, 2002. – 382 с.: ил.
19. Загальна характеристика та властивості нейро-нечітких мереж [Електронний ресурс] // Інформаційний сайт нечіткої логіки. – Режим доступу: https://sites.google.com/site/ne4itka logika / nejronecitki-merezi / zagalna harakteristika ta vlastivosti-nejro-necitkih-merez.
20. Субботін С. О. Подання й обробка знань у системах штучного інтелекту та підтримки прийняття рішень: навч. посібник / С. О. Субботін. – Запоріжжя : ЗНТУ, 2008. – 341 с.
21. Buckleya J. J. Fuzzy neural net works: asurvey / J. J. Buckleya, Y. Hayashi // Fuzzy sets and systems. – 1994. – Vol. 66, Issue 1. – P. 1–13.
22. ERP-система (планування ресурсів підприємства) [Електронний ресурс] / Навчальні матеріали онлайн (pidruchniki website). – Режим доступу: https://-pidruchniki. Com / 1171062647760 / informatika Pidpriyemstva.
23. Информационная безопасность ERP-систем [Електронний ресурс] / Ю. Зырянов // CITforum. – 2007. – Режим доступу: http://citforum.ru/gazeta/49/.
24. 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. – V. 2. – 4 p.
25. Security issues in ERP. Security, Audit and Control Features SAP ERP 4th Edition, Audit Program. – Isaca. – 2015. – 574 p.
26. Polyakov A. ERP Security Deserves Our Attention Now More Than Ever [Електронний ресурс] / A. Polyakov Forbes. – 2017. – Режим доступу: https://www.forbes.com/sites/forbestechcouncil/-2017/07/07/erp-security-deserves-our-attention-now-more-than-ever/.
27. Polyakov A. Безопасность SAP в цифрах [Електронный ресурс] / A. Polyakov // Блог компании Digital Security / Хабрахабр.– 2012. – Режим доступу: https://habr.com/ru/company/dsec/blog/146967/.
28. Jang J.-S.R. ANFIS: Adaptive Network – based Fuzzy Inference System / J.-S.R.Jang // IEEE Trans. On Syst., Man and Cybernetics. – 1993.– V. 23. № 3. – P. 665–685.
29. Goel S. Vulnerability Management for an Enterprise Resource Planning System / S. Goel, Kiran, D Garg // International Journal of Computer Applications. – 2012. – Vol. 53, No. 4. – P. 19–22.
30. National vulnerability database Release [Електронний ресурс] // National Institute of Standards and Technology. – Режим доступу: https://nvd.nist.gov.

DOI 10. 15588/1607-3274-2020-4-15