UDC 004.008
DOI: 10.15587/1729-4061.2020.218158

DEVELOPMENT OF A METHOD FOR ASSESSING CYBERNETIC SECURITY IN SPECIAL-PURPOSE INFORMATION SYSTEMS

S. Drozdov
PhD, Commander
Air Force of Armed Forces of Ukraine
Striletska str., 105, Vinnytsia, Ukraine, 21001
E-mail: red.hnups@gmail.com

Yu. Zhuravskyi
Doctor of Technical Sciences, Senior Researcher
Scientific Center
Zhytomyr Military Institute named after S. P. Koroliov
Myru ave., 22, Zhytomyr, Ukraine, 10004

O. Salnikova
Doctor of Public Administration Sciences, Senior Researcher,
Head of Educational and Research Center
Educational and Research Center of Strategic Communications
in the sphere of National Security and Defense*

R. Zhyvotovskyi
PhD, Senior Researcher, Head of Research Department
Research Department of the Development of Anti-Aircraft Missile Systems and Complexes**

E. Odarushchenko
PhD, Associate Professor
Department of Information Systems and Technologies
Poltava State Agrarian Academy
Skovorody str., 1/3, Poltava, Ukraine, 36003

O. Shcheptsov
PhD, Head of Department
Department of Weapon
Institute of Naval Forces of the National University “Odessa Maritime Academy”
Hradonachalnytska str., 20, Odessa, Ukraine, 65029

O. Alekseienko
PhD, Associate Professor, Head of Laboratory
Scientific and Innovative Laboratory*

R. Lazuta
Senior Researcher
Scientific Center
Military Institute of Telecommunications and Information Technologies named after Heroiv Krut
Moskovsky str., 45/1, Kyiv, Ukraine, 01011

O. Nalapko
Adjunct**

O. Pikul
Institute of Information Technology*
*Ivan Chernyakhovsky National Defense University of Ukraine
Povitrofloski ave., 28, Kyiv, Ukraine, 03049
**Central Scientifically-Research Institute of Arming and Military Equipment
of the Armed Forces of Ukraine
Povitrofloski ave., 28, Kyiv, Ukraine, 03049

A method for assessing cybersecurity in special-purpose information systems was developed. Cybersecurity assessment was performed using decision trees, implemented using “IF-THEN” fuzzy rules, which are considered as common building blocks of the decision tree. This approach allows processing large amounts of data. The use of the decision tree allows increasing evaluation accuracy, is easy to set up and intuitive. Improvement of the efficiency of cybersecurity assessment (error reduction) was achieved using evolving neuro-fuzzy artificial neural networks. Training of evolving neuro-fuzzy artificial neural networks was carried out by learning not only the synaptic weights of the artificial neural network, type, parameters of the membership function, but also by reducing the dimensionality of the feature space. The efficiency of information processing was also achieved through training the architecture of artificial neural networks; taking into account the type of uncertainty of information to be assessed; working with both clear and fuzzy products, and reducing the feature space. This reduces the computational complexity of decision-making and eliminates the accumulation of learning errors of artificial neural networks. The computational complexity of the method is on average 2 million calculations less compared to the known ones, and after 2 epochs, the learning error decreases. Cybersecurity analysis in general occurs due to an advanced clustering procedure that allows working with both static and dynamic data. Testing of the proposed method was carried out. The increase in the efficiency of cybersecurity assessment of about 20–25 % in terms of information processing efficiency was revealed

Keywords: cybersecurity, artificial intelligence, cyber threats, intelligent systems, information systems

Received date 27.10.2020
Accepted date 09.12.2020
Published date 18.12.2020

1. Introduction

The experience of conducting operations (combat operations) in recent years shows the growing role of special-purpose information systems (IS) in achieving the goal of combat operations.

The specificity of special-purpose IS is that, on the one hand, they solve the problem of transmission and processing of information, and, on the other hand, must meet the requirements of survivability under the influence of enemy means.

In order to disorganize management and achieve an information advantage by the enemy, means of electronic and cybernetic influence on special-purpose IS are widely used [1, 2].

Given this, cyber attacks on IS have become a real threat and are one of the priority issues of national security and risk management.

Cybersecurity encompasses all security measures that can be taken against these attacks. The significant increase in the complexity and intensity of cyber attacks in recent years has forced most developed countries to strengthen their defense and adopt national cybersecurity strategies. Therefore, the problem of improving the cybersecurity of special-purpose information systems in the conditions of destructive influences is relevant.

The term "information system" means a set of organizational and technical means for storing and processing information to meet the information needs of users [3]. Examples of special-purpose IS are [4] "Dzvin-AS", "Buh" and "Prostir", which collect, process and store information in the interests of the Armed Forces of Ukraine. Given the above, special-purpose IS are the object of priority cyber attacks, due to the fact that they circulate information with limited access and the interception of control over such systems will lead to the loss of groups control.

However, there are a number of difficulties and problems in the analysis of cyber threats to special-purpose information systems:

1. Assessment of cyber threats occurs against the background of intentional artificial and natural interference.
2. The obtained data do not match the standards due to the influence of different types of interference and incomplete threat databases.
3. Interpretation of the received information depends on the decision-maker's experience and completeness of additional information on a specific task (conditions of uncertainty).
4. High dynamics of changes in system security.
5. Large number of cybersecurity features.
6. Limited time for analysis and decision making in conditions of uncertainty.
7. Large number of different types of objects that simultaneously function in the network and affect each other.

Game theory [5, 6], artificial neural networks [7, 8], fuzzy sets [9], expert evaluation method [10], etc. are actively used to solve the problem of cybersecurity. Game theory allows you to describe the conflict between the security system and the attacker, but has great computational complexity. This happens because it is necessary to build a matrix with a significant dimension for each parameter. This necessiates working with large amounts of data. The expert evaluation method is also actively used to solve cybersecurity problems. It allows working with qualitative and quantitative indicators. However, the expert evaluation method is characterized by great subjectivity, which often leads to errors. Taking into consideration the need to involve experts to formulate the rules and membership function, the methods of fuzzy set theory have the disadvantages of the expert evaluation method.

Artificial neural networks are actively used to ensure cybersecurity in special-purpose information systems [7, 8]. The most important advantage of artificial neural networks in detecting attacks is their ability to study the characteristics of deliberate attacks and identify elements that are not similar to those observed in the network before.

In [5], the classification of problems solved by artificial neural networks is given:

– rapid recognition of threats;

– fight against malicious software, which also has the self-learning ability;

– making certain conclusions in the training process, and building a more powerful security system on their basis.

In applied information security problems, neural networks are used in [8]:

– attack detection systems. The formed image of the normal behavior of a network allows finding and recognizing dangerous anomalies with a high degree of efficiency;

– firewalls. The neural network analyzes traffic and makes assumptions about possible intrusions (performs the functions of an expert system).

That is why the use of artificial neural networks in the interests of special users is a promising way to ensure a given level of cybersecurity in special-purpose IS.

Evolving artificial neural networks (ANN) are a type of artificial neural networks. Evolving artificial neural networks are actively used for pattern recognition, monitoring and prediction of complex systems. A feature of evolving artificial neural networks is the adaptation not only of the parameters of the artificial neural network but also the network architecture itself, namely: the number of network layers, the number of network neurons, the number of connections between network neurons depending on the amount of information to be processed.

Evolving artificial neural networks have both universal approximating properties and fuzzy inference capabilities. Evolving ANNs are widely used to solve various problems of data mining, identification, emulation, forecasting, intelligent control, etc.

Evolving ANNs provide stable operation in conditions of nonlinearity, uncertainty, stochasticity and chaos, various disturbances and interference.

That is why the urgent task is to increase the cybersecurity of special-purpose information systems by increasing the speed (efficiency) of assessing cybersecurity in special-purpose information systems while maintaining the necessary reliability by improving the interpretability of the results and using evolving neuro-fuzzy artificial neural networks.

2. Literature review and problem statement

The paper [7] proposes to use Bayesian hierarchical networks to quantify the level of cybersecurity risks in special-purpose information systems. However, this approach is limited by the statistical distribution that can be used and the extensibility of the model structure. This imposes restrictions on the information system architecture and does not take into account qualitative factors that affect the cybersecurity of the information system.

The paper [8] proposes the security certification methodology developed for information systems to enable various stakeholders to evaluate security solutions for large-scale deployments of information systems automatically. The methodology supports transparency regarding the security level of information systems for consumers, as the methodology provides labeling as one of the main results of the certification process. The disadvantages of the proposed approach include the inability of knowledge bases to learn new threats, the difficulty of generalization and analysis of various types of data circulating in the network.

The paper [9] proposes the model that combines fault tree analysis, decision theory and fuzzy theory to determine the current causes of cyber attack prevention failures. The model was used to assess cybersecurity risks associated with a website attack, e-commerce, and corporate resource planning, as well as to assess the possible consequences of such attacks. This model has a flexible architecture, however, the disadvantages of the proposed model include the accumulation of evaluation errors during fuzzification and defuzzification procedures.

The paper [10] proposes the model of resource allocation of an automated special-purpose control system in the conditions of insufficient information on the development of an operational situation. The specified model proposes the mechanisms of resource allocation of the automated control system taking into account the influence of cyber attacks. This allows us to present the solution of the vector optimization problem in binary relations of conflict, assistance and indifference. Also it takes into account the operational situation and allows you to forecast the state of the system taking into account external influences, build utility and guaranteed gain functions, as well as a numerical optimization scheme on this set. However, this model does not allow working with multidimensional indicators.

The paper [11] proposes the hierarchical concept of implementing a management model based on e-government. The paper examines the main threats to critical cyberphysical systems as the basis of mechanisms for performing e-government functions. This hierarchical system is based on the use of symmetric and asymmetric cryptosystems, which does not allow them to be used for identifying cybernetic effects on the system.

The paper [12] proposes the model for selecting the optimal set of cybersecurity insurance policies of a company, given the limited number of policies offered by one or more insurance companies. The model allows you to systematically evaluate different insurance policies as a function of the probability that cybersecurity breaches will occur over the life of policies and policy-related premiums. The proposed model provides a risk-sharing approach that assists RMS cybersecurity policy choices in a way that contributes to an effective cybersecurity insurance market. However, the disadvantages of this approach include the inability to introduce new risks to the knowledge base in the course of operation and a limited number of assumptions. This makes it impossible to work in real time.

The paper [13] discusses the importance of including vulnerability analysis in cybersecurity not only as part of process hazard analysis, but also in terms of protecting the process management network and implementing adequate safeguards against cyber threats in general. Security level analysis is designed to assess potential vulnerabilities and protect critical applications from cyber attack resistance. The integration of cybersecurity into hazard and risk analysis, as well as other elements of process security management are demonstrated by examples, making the plant more resilient to traditional and cyber threats. However, the proposed approach is only suitable for a clear architecture and is not intended to be configured in the course of operation.

The paper [14] proposes the risk management process for detecting, analyzing, evaluating, responding to cyber threats and monitoring risks at each stage of the cybersecurity chain. This approach can be used in organizations that intend to implement security mechanisms to align them with current requirements or reduce cyber risks to an accepted level. The risk assessment method is based on a continuous Markov chain. However, the disadvantages of the proposed method include the inability to simultaneously take into account both quantitative and qualitative indicators, and the inability to adapt to new system threats.

The paper [6] proposes the theoretical and analytical approach to the analysis of the impact of information transmission delays in traffic regulation caused by cybernetic impact. The evaluation is performed using the method of successive averages. However, this approach is limited to the use only in traffic control systems and is not suitable for other systems.

The paper [15] proposes to consider cybersecurity of an object in the form of a transient graph. This approach allows you to describe the threats that affect the object and determine their degree of impact on cybersecurity. The disadvantages of the proposed approach include the ability to work only with one-dimensional quantities and the inability to add new threats in the course of the proposed approach.

The paper [16] presents the method of creating and solving a game theory model for solving cybersecurity issues, especially for advanced production systems with high-level computer integration. This method introduces a unique approach to determining the content of the game win matrix, including support for defense strategies, production losses and recovery from attacks as part of the cost function. The disadvantages of the proposed method include high computational complexity and the ability to work only with one-dimensional quantities.

Therefore, summarizing the above, a common disadvantage of all these approaches is the inability to work with multidimensional data in real time. Let us consider the known works that allow solving this shortcoming. Several different solutions have been proposed to address this shortcoming.

Thus, the paper [17] proposes to use neuro-fuzzy systems to predict the efficiency of building structures. This approach allows predicting the efficiency of building structures under probabilistic and non-probabilistic uncertainty. The disadvantages of this approach include the inability to train the architecture and parameters of the artificial neural network, as well as the accumulation of errors during system operation.

The paper [18] proposes to use fuzzy expert systems for assessing the creative abilities of a person. This approach is based on the use of fuzzy logic to assess the creative abilities of a person in recruitment. The disadvantages of this approach include the accumulation of errors during fuzzification and defuzzification procedures.

The paper [19] proposes to use fuzzy expert systems for forecasting the load on electric networks. The genetic algorithm and the ant colony algorithm are used to speed up the solution. The disadvantages of this approach include the accumulation of errors during fuzzification and defuzzification procedures, as well as no reduction in the dimensionality of the feature space.

The paper [20] proposes the intelligent evaluation methodology based on fuzzy logic and expert systems. The principle of this methodology is to transform abstract concepts of human expertise into a numerical inference engine applied to evaluation. Therefore, it reproduces the cognitive mechanisms of evaluation experts. In addition, due to flexibility, various types of extensions are possible by updating the basic rules and adapting to new possible architectures and new types of evaluation. The disadvantages of this approach include the accumulation of errors during fuzzification and defuzzification procedures, as well as no reduction in the dimensionality of the feature space.

The paper [21] proposes to use an adaptive neuro-fuzzy inference system to control the speed of a DC motor, optimized by the collective swarm intelligence. The controller is designed according to fuzzy rules, it has an advantage in the expert knowledge of the fuzzy inference system and the ability to train neural networks. However, this neuro-fuzzy system implements the training mechanism only by adjusting synaptic weights and does not take into account the uncertainty about the state of the object.

The paper [22] presents the results of analytical review and comparison of the most common management decision support technologies: hierarchy analysis method, neural networks, fuzzy set theory, genetic algorithms and neuro-fuzzy modeling. The advantages and disadvantages of these approaches are indicated. The spheres of their application are defined. It is shown that the hierarchy analysis method works well if the initial information is complete, but due to the need for experts to compare alternatives and choose evaluation criteria, it has a high degree of subjectivity. The use of fuzzy set theory and neural networks is justified for forecasting problems in conditions of risk and uncertainty. The technology of collective decision-making, used both in general elections and in a group of experts, is also considered. It allows reducing the time for conciliation meetings to reach a consensus by pre-analyzing all opinions presented on the plane in the form of points. The consistency of opinions is determined by the distances between them.

In [23], the development of a fuzzy expert system for the diagnosis of cystic fibrosis was carried out. The results showed that the proposed system can be used as a powerful tool with an accuracy of 93.02 %, specificity of 89.29 %, sensitivity of 95.24 % and accuracy of 92.86 % for the diagnosis of cystic fibrosis. However, the proposed fuzzy expert system does not implement the training mechanism and does not take into account the uncertainty about the state of the object.

In [24], the method of information security risk assessment was developed. The method is based on an attack tree model with fuzzy set theory and risk probability estimation technology used in a ship control system risk scenario. Fuzzy numbers and expert knowledge are used to determine the factors that affect the probability of leaf nodes that are quantified to obtain the probability of an interval. The disadvantages of the proposed method include the accumulation of errors during operation and failure to take into account the uncertainty about the state of the object.

In [25], we show the creation of a fuzzy expert system for the early diagnosis of infections in newborns. This fuzzy expert system allows the early diagnosis of infections by many indicators. However, this system does not reduce the feature space, which in turn requires significant computing resources of the system.

The paper [26] created a fuzzy expert system with a soft expert set, which allows checking the adequacy of the information provided by the expert and increasing the accuracy of assessment. However, the disadvantages of this approach include the accumulation of evaluation errors and non-consideration of uncertainty about the state of the evaluation object.

The analysis showed that the known methods (techniques) [6–26]:

– do not adjust the results taking into account the evaluation error;

– training occurs only by adjusting synaptic weights;

– require significant computing resources;

– do not reduce the dimensionality of the feature space;

– do not take into account uncertainty about the state of the evaluation object;

– are not able to adapt the architecture of the artificial neural network depending on the amount of information received at the input of the artificial neural network;

– have low linguistic interpretability of data;

– have high computational complexity in extracting conjunctive patterns from a large array of data and generating fuzzy rules;

– are not able to assess the individual object and the situation as a whole.

Therefore, it is necessary to develop a method for assessing cybersecurity in special-purpose information systems, which is able to effectively assess the cybersecurity of an object in conditions of uncertainty, as well as shortage of computing resources.

3. The aim and objectives of the study

The aim of the study is to develop a method for assessing cybersecurity in special-purpose information systems.

To achieve the aim, the following objectives are set:

– to provide a mathematical formulation of the problem of analyzing the cybersecurity of special-purpose information systems;

– to develop an approach for assessing cybersecurity in special-purpose information systems;

– to evaluate the effectiveness of the proposed method of assessing cybersecurity in special-purpose information systems.

4. Mathematical formulation of the problem of analyzing the cybersecurity of special-purpose information systems

Let us suppose that as a result of the analysis of cyber threats, a vector model of cybersecurity of special-purpose information systems is obtained. The model determines the type of monitoring object, so the studied monitoring objects are divided into elementary components according to the characteristics that make up the set of V elementary components of the analyzed monitoring object. The obtained information is interpreted to a particular structural unit. The special-purpose information system can be presented as a set of monitoring objects (objects to be analyzed):

$$Ob = \left(Ob_1, Ob_2 \ldots Ob_n\right), \qquad (1)$$

where Ob_n is the total number of monitoring objects included in the special-purpose information system. Each of the monitoring objects has its own rank of importance, so taking into account the importance, expression (1) will have the following form

$$Ob = \left(Ob_1 \cdot w_1,\ Ob_2 \cdot w_2\ \dots\ Ob_n \cdot w_n\right), \tag{2}$$

where w is the importance of monitoring objects.

The objects of monitoring in solving the problem of analyzing the cybersecurity of special-purpose information systems include control points of brigades, operational commands, operational and tactical groups of troops (forces), information and telecommunication nodes of control points and communication lines between them.

The information about the security of the information system is stored in computer memory in digital form. It is presented as a matrix R of dimension (M*N) and has the following form [2, 4]:

$$R = \left\| r_{i,j} \right\|,$$

where

$$i = 1,\dots,M; \quad j = 1,\dots,N. \tag{3}$$

where M is the number of matrix rows; N is the number of matrix columns.

Each element of the matrix R is a vector of parameters that characterize each (i, j)-th elementary parameter of cybersecurity on some m-th m=(1,..., T) set of thematic properties of the unit (element):

$$r_{i,j} = \left(r_{i,j}^1,\dots,r_{i,j}^T\right), \tag{4}$$

the nature of the components of the vectors $r_{i,j}$ in general does not play a fundamental role.

Let the set of thematic properties $\{P_n\}$, (n=1,..., K) be set to classify the studied data and threshold restriction values.

It is necessary to match each P_n according to their threshold limits to the set $P_n, V_t \in V$, $\left(1 \le t \le (M \times N)\right)$ of elementary components of the object (system element), which have the property P_n. Threshold limits for each of the thematic properties are determined for each of the special-purpose information systems during design and operation.

Then, showing all possible options of feature values within the constraint thresholds for each k-th reference table at the output, we have the rating matrix Γ^{kl}

$$\Gamma^{kl} = \left\| q_{u,v}^{kl} \right\|, \ q_{u,v}^{kl} \in [0,1], \tag{5}$$

$q_{u,v}^{kl}$ are the options of feature values within the constraint thresholds, where the answer 1 means that a decision is made on belonging to one of the membership classes based on the set of features and their constraint thresholds and 0 – otherwise, l is the number of options.

Considering a large number of different parameters (gradations of their change) in assessing the cybersecurity of special-purpose information systems, it is advisable to use neural-fuzzy artificial networks to solve this problem. However, even with all the advantages of neural fuzzy artificial networks, they have some disadvantages. Among them [7–10]:

– accumulation of evaluation errors during fuzzification and defuzzification procedures;

– the artificial neural network used to form knowledge bases has a rigid architecture and is not able to adapt during computing;

– training of the artificial neural network is limited only by learning synaptic weights between neurons;

– low productivity of solution search methods, even with a small number of rules;

– great computational complexity of solution search methods;

– large dimension of the feature space.

Therefore, it is necessary to develop a method for assessing cybersecurity in special-purpose information systems.

Given the above, the mathematical formulation of the problem of analyzing the cybersecurity of special-purpose information systems can be represented as (6):

$$\begin{cases} R = \left\| r_{i,j} \right\| \to \max; \\ P_n, V_t \in V; \\ t_{\text{des}} \le t_{\text{des prob}}; \\ BER \le BER_{\text{prob}}. \end{cases} \tag{6}$$

where t_{des} is the time of decision-making on the state of cybersecurity in special-purpose information systems, $t_{\text{des prob}}$ is the allowable time of decision-making on the state of cybersecurity in special-purpose information systems; BER is the bit error probability of information transmitted in the system; BER_{prob} is the allowable bit error probability of information transmitted in the system.

Thus, the mathematical formulation of the problem of analyzing the cybersecurity of special-purpose information systems (6) is a solution to the optimization problem. The parameters of cybersecurity are accepted as the objective function, and optimization consists in maximizing them. At the same time, restrictions are imposed on the time of cybersecurity decision-making and error magnitude.

5. Development of an approach for assessing cybersecurity in special-purpose information systems

The method of assessing cybersecurity in special-purpose IS consists of the following main stages (Fig. 1):

1. Entering initial data. At this stage, the operational situation and available data on the possibilities of cybernetic impact on special-purpose IS are entered. At this stage, expressions (1)–(5) are used for further formulation of the concept and the relationships between them.

2. Analysis of cyber threats. During this procedure, the following steps are performed:

1) determining the IS context;

2) conducting a security audit in IS, including: questionnaires; detection of cyber threats in IS assets; evaluation of IS assets; detection of threats; detection of typical attack vectors and formation of scenario concepts.

Analysis of cyber threats is carried out by comparing the identified cyber threats with those available in the knowledge base. Also at this stage, we make a list of critical assets and identified vulnerabilities that correspond to cyber threat, as well as typical attack vectors, which are a chain of vulnerabilities, threats and target assets [7–9].

Based on the obtained result, concepts and relationships between them are formed for further construction of scenarios. Formally, the initial data of the first stage of cyber threat analysis and risk assessment are presented by formula (7).

$$P = \left\{V_i, T_j, A_k, R_a^v\right\}, \tag{7}$$

where P is the model of intruder attacks represented by a chain of vulnerabilities and threats; V_i is the identified vulnerabilities of special-purpose IS; T_j is cybersecurity threats; A_k is the target assets of attacks; R_a^v is the attack vectors.

3. Formation of scenarios of extreme situations in IS caused by cyber threats.

This procedure is based on systematic analysis and information security research.

It is proposed to use a fuzzy network for scenario analysis of the impact of cyber threats on the occurrence of extreme situations in special-purpose IS (Fig. 2). The architecture of decision trees is implemented using "IF-THEN" fuzzy rules, considered as general building blocks of the decision tree [9].

The decision tree (DT) is one of the most well-known methods to obtain classified data from large data sets.

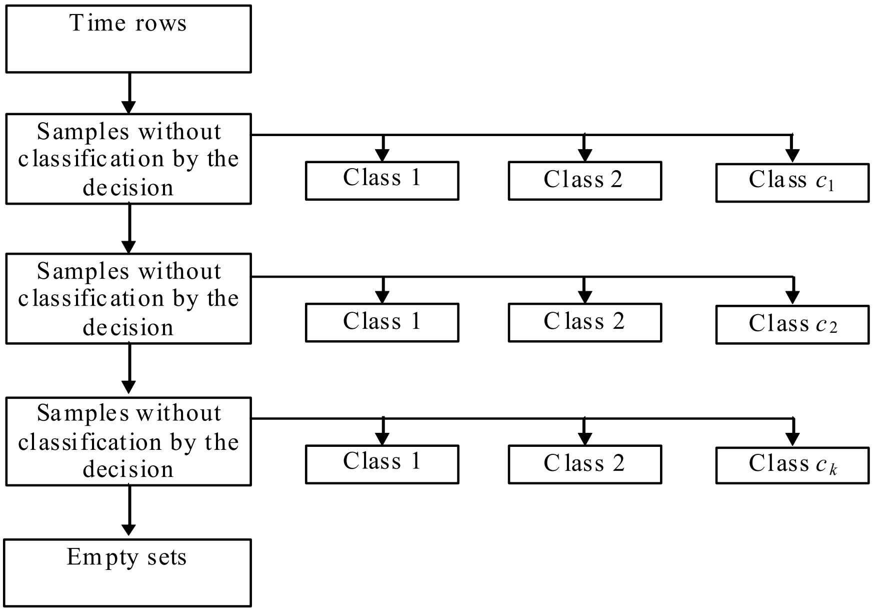
Time rows
Samples without classification by the decision
Class 1
Class 2
Class c_1
Samples without classification by the decision
Class 1
Class 2
Class c_2
Samples without classification by the decision
Class 1
Class 2
Class c_k
Empty sets

Fig. 2. General view of the decision tree of the neuro-fuzzy model

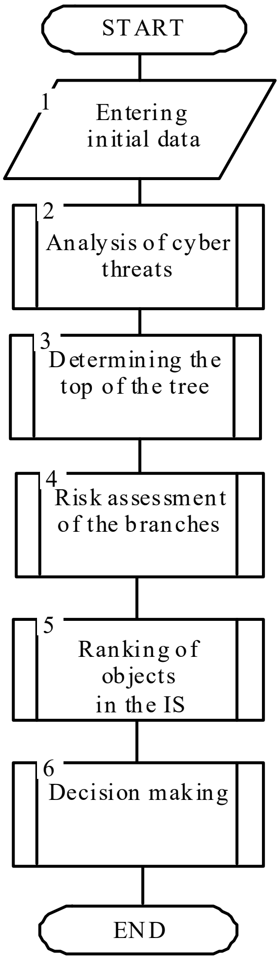
START
1 Entering initial data
2 Analysis of cyber threats
3 Determining the top of the tree
4 Risk assessment of the branches
5 Ranking of objects in the IS
6 Decision making
END

Fig. 1. Algorithm for implementing the evaluation method

There are several reasons for their widespread use:

– the accuracy of decision trees is often comparable or higher than in other classification models [10];

– most decision trees do not require a large number of parameters for their configuration in the DT design [11];

– due to their intuitively attractive topology, the results of classification models are easy to understand [6, 13, 14].

However, the main disadvantage of neuro-fuzzy mathematical models and other methods is the difficulty of interpreting the identification model and the lack of understanding of the interaction between technical indicators and fluctuations in time series values. There are cases when it is difficult to classify an object with one or another feature with high accuracy. These situations are solved due to the possibilities of fuzzy logic, when we talk not just about belonging to a class, feature, attribute, but about its degree of membership.

Let us consider the initial conditions. So, this set of examples is denoted as T. The set of examples of each element is described by certain attributes m. The number of examples for each set of examples T is the power of the specified set $|T|$.

Thus, when classes $\{C_1, C_2, ..., C_k\}$ are designated, there may be the following 3 situations [3–5, 7, 8]:

1. T has one or more examples that belong to the same class C_k. In this case, the decision tree for the set T is the leaf that defines the class C_k.

2. T is an empty set, so the class associated with the leaf is selected from another set.

3. T has examples belonging to different classes. In this case, it is necessary to divide T into subsets.

In this case, we select one of the features that has different values $T_1, T_2, ..., T_n$. T is divided into subsets $T_1, T_2, ..., T_n$. Each subset T_i contains all examples, these examples have the value O_i for a specific feature. The task is to build a hierarchical classification model in the form of a tree with the set of examples T. The process of building a tree occurs from top to bottom.

As a result, we get n subsets. These n subsets create a certain number n of root descendants. Each of the roots is matched to the defined subset obtained by partitioning the specified set *T*.

Therefore, the advantage of this approach is that it does not preclude the reuse of the attribute. Thus, any of the attributes can be used an unlimited number of times while building a tree.

Let us have a check *X* that accepts *n* values $A_1, A_2, ..., A_n$. Then dividing *T* by the check *X* will give us subsets $T_1, T_2, ..., T_n$, with X equal to $A_1, A_2, ..., A_n$, respectively.

$freq(C_j, S)$ is the set of examples from the set *S*, which belong to a certain class C_j. In this case, the probability that a random example from the set *S* will belong to the class C_j is determined by the expression.

$$P = \frac{freq\left(C_j, S\right)}{|S|}.$$

It is known that the amount of information contained in the message depends on its probability

$$\log_2\left(\frac{1}{P}\right). \quad (8)$$

Since the logarithm has a binary base, the expression (8) gives a quantitative estimate in bits.

$$Info(T) = \sum_{j=1}^{k} \frac{freq\left(C_j, T\right)}{|T|} \cdot \log_2 \frac{freq\left(C_j, T\right)}{|T|}, \quad (9)$$

we obtain an estimate of the average amount of information required to determine the class of the example from the set. The algorithm uses a theoretical and information approach. To select the most appropriate attribute, it is proposed to use the following criterion:

$$Info(T) = \sum_{j=1}^{k} \left|\frac{T_i}{T}\right| \cdot Info\left(T_i\right). \quad (10)$$

The criterion for selecting the attribute is the following formula:

$$Gain(X) = Info(T) - Info_x(T). \quad (11)$$

The criterion (11) must be calculated for the whole set of attributes. The specified attribute is the check in the current tree node. Further, the tree is constructed using this attribute.

The value of this attribute will be checked in the tree node. Movement on the tree will occur depending on the experience gained.

Let us assume that a numeric attribute has a finite number of values. Let us note the numeric attributes $\{V_1, V_2, ..., V_n\}$.

As a threshold, you can choose the average value between V_i and V_{i+1}

$$TH_i = \frac{V_i + V_{i+1}}{2}. \quad (12)$$

Thus, the task of finding the threshold is significantly simplified, and only *n*-1 potential thresholds $TH_1, TH_2, ..., TH_{n-1}$ are considered.

The formulas (9)–(11) are consistently used for all potential threshold values and we choose the one that gives the maximum value according to the criterion (8).

4. Assessment of cybersecurity risks in IS

This procedure is aimed at identifying risks, their qualitative and quantitative assessment, as well as ranking the considered objects according to the set criteria, which can be the values of both the integrated object risk indicator and indicators of individual risk types.

This procedure contains recommendations for risk description, qualitative and quantitative assessment, selection of assessment scales and ranking of energy facilities. The procedure for assessing cybersecurity risks in information and telecommunications systems includes 3 main stages: risk description; qualitative and/or quantitative risk assessment; objects ranking.

5. Objects ranking in IS

In this technology, objects are ranked in accordance with the magnitude of the risks that may be caused by cyber influences, information about which is included in the database of external and internal threats or factors.

The proposed ranking criterion:

$$K^S = \{C, R, \Theta\}, \quad (13)$$

K^S is the significance criterion; *C* is the risk assessment criterion; *R* is the integrated risk indicator of affected objects; Θ is the object represented by a set of characteristics.

6. Evaluation of the effectiveness of the proposed method of assessing cybersecurity in special-purpose information systems

Therefore, we made the simulation of the method according to the algorithm in Fig. 1 and expressions (3)–(13). We made the simulation of the proposed method in the MathCad 14 software environment (USA).

Initial data for assessing the state of cybersecurity using the proposed method:

– the number of information sources about the state of the monitoring object is 3 (radio monitoring, remote Earth sensing devices and unmanned aerial vehicles);

– the number of information features that determine the state of the monitoring object is 13. The parameters include: affiliation, type of organizational and staff formation, priority, minimum width on the front, maximum width on the front. The number of personnel, minimum depth on the flank, maximum depth on the flank, total number of personnel, number of samples of weapons and military equipment (WME), number of WME types, number of communication means are also taken into account;

– options for organizational and staff formation are company, battalion, brigade (number of computers is 70).

The type of system attacks is DDoS (Distributed Denial of Service).

To make the experiment, a simulation of the flows assigned to the group for users of applications and the process of their processing was performed. A queuing network was used for this purpose.

MikroTik NetMetal 5 broadband radio access station with the following parameters (128-position quadrature amplitude manipulation; radiation bandwidth is 40 MHz, radiation power is 1 W; radiation frequency is 2.1–3) was selected as the radio communication device subjected to a cyberattack. On the basis of the specified initial data, a graph was constructed (Fig. 3). The works [6, 13, 14] were used for analysis and comparison.

The evaluation found that to detect a denial-of-service cyber attack, it is sufficient to analyze 3,433 packets, which increases the efficiency of determining the transmission delay from 20 to 25 % (compared to the WinMTR network connection diagnostic program).

The proposed method allows increasing the efficiency of information processing (reducing the number of computational operations) from 20 to 25 %, depending on the amount of information about the monitoring object (Fig. 3). These dependences were obtained empirically during the experiment.

However, as already mentioned, the known methods accumulate errors, that is why the proposed method uses evolving artificial neural networks.

To demonstrate the effectiveness of training of the evolving artificial neural network, we made a forecast of the time security of the network.

A training sample containing data about the monitored object was used for the experiment. 5,000 observations from this sample were used for experiments. The training sample contained 3,000 observations, the test sample contained 2,000 observations.

The square root of the standard error was used as a criterion of forecasting quality.

A multilayer perceptron (MLP), a radial-basis neural network (RBNN), and an evolving artificial neural network were used to compare forecasting quality.

The results of forecasting for different systems are presented in Table 1.

Table 1

Forecasting results for different systems

System	Number of customized parameters	RMSE (training)	RMSE (test)	Time, s
Multilayer perceptron	51	0.1058	0.1407	0.1081
Radial-basis neural network	21	0.1066	0.2155	0.1081
Evolving cascade system with neo-fuzzy nodes	20	0.0784	0.1081	0.1081

The results of efficiency evaluation are shown in Fig. 4.

Fig. 3 shows that the use of evolving artificial neural networks allows not to accumulate training errors after 3 epochs and we can see a gradual reduction of training errors.

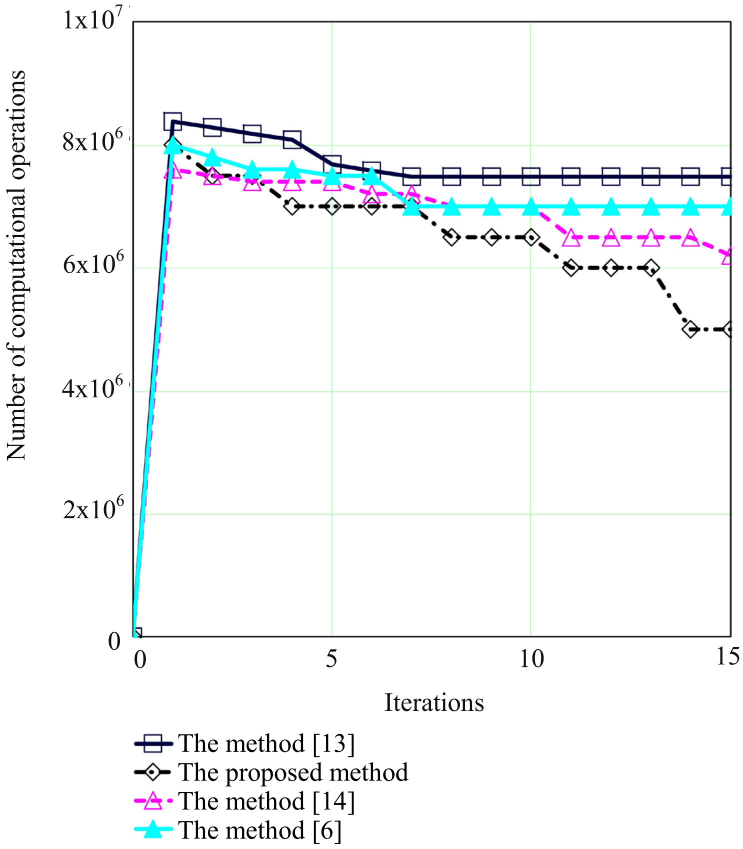

Fig. 3. Results of efficiency evaluation of the proposed method

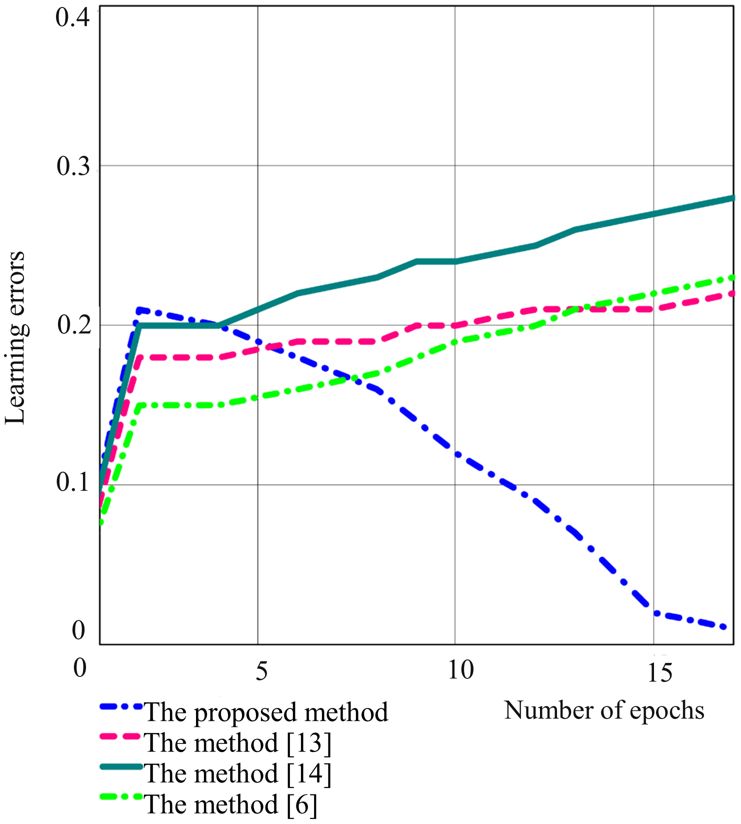

Fig. 4. Efficiency evaluation of evolving artificial neural networks

7. Discussion of the results of developing the method for assessing cybersecurity in special-purpose information systems

The given mathematical formulation of the problem of analyzing the cybersecurity of special-purpose information systems presented in expressions (1)–(6) allows describing a set of factors that affect cybersecurity in special-purpose information systems. This is explained by the vector representation of a set of factors affecting cybersecurity in special-purpose information systems.

An approach for assessing cybersecurity in special-purpose information systems was developed. The advantage of the proposed approach over others is explained by the comprehensive consideration of different data on the state of the monitored object; type of uncertainty about the state of the monitoring object, using evolving ANN and clustering of objects with similar behavior.

The features of the proposed method are as follows:

– allows high-quality processing of large arrays of different data that have a numerical and quantitative nature;

– while clustering the monitored objects, takes into account not only the dynamics of changes in the state of the monitored object, but also the use of resources;

– allows training the method during operation;

– takes into account the degree of awareness about the state of the monitored object;

– allows comprehensive processing of information about the state of the monitored object;

– allows a comprehensive assessment of the operational situation for each unit.

The advantages of this method include:

– minimization of the total time to perform the response task;

– limitation of human participation in the resource management of integrated processing and automatic determination of the option for forming scenarios for solving monitoring tasks.

The limitations of this method include the need for communication channels with high transmission reliability and minimal delay. This is due to the need to process information in close to real-time mode and high requirements for the reliability of information circulating in special-purpose decision support systems.

The disadvantages of this method include the need to process large amounts of data to determine the state of the monitoring object and the operational environment as a whole and the need for an artificial neural network to learn new types of attacks. This is due to the need for a long time for the artificial neural network to learn new types of attacks caused by the need to form test and training samples.

The practical significance of the method consists in the fact that it significantly increases the efficiency of integrated data processing in automated control systems. The proposed method allows solving the following useful tasks from the standpoint of analyzing the operational situation:

– having a set of clusters and information about new monitoring objects, the new monitoring object should be assigned to one or another cluster;

– having a set of clusters, it is possible to assess the change in the "position" of the monitored object in the cluster and possibly its transition to another cluster;

– having a set of clusters, it is possible to estimate changes in the size, structure of clusters (absolute values of differences between the "old" and "new" cluster centroids);

– having the obtained centroids for each cluster, it is possible to estimate their dynamics of changes;

– it is possible to estimate the deviation between the set values and the centroids for the typical average profiles of the monitoring objects set by the official.

It is proposed to use the proposed method in decision support systems of automated control systems (ACS DSS) for artillery units, ACS DSS for aviation and air defense, as well as ACS DSS for logistics of the Armed Forces of Ukraine. This study is a further development of research aimed at developing methodological principles for improving the efficiency of data processing in special-purpose information systems, published earlier [28–32]. Areas of further research should be aimed at reducing computational costs when processing various data in special-purpose information systems.

8. Conclusions

1. The parameters of analyzing cybersecurity in special-purpose information systems are determined, namely: time of decision-making on the state of cybersecurity in special-purpose information systems, allowable time of decision-making on the state of cybersecurity in special-purpose information systems, bit error probability of information transmitted in the system. The influence of cybersecurity analysis parameters on the quality of cybersecurity assessment is determined. The presence of cyber attacks in special-purpose information systems increases the bit error probability, increases the packet delivery time and reduces the share of packets reaching the recipient. These effects should be identified in the minimum time. Their number and measurement units are determined, namely, they have quantitative and qualitative measurement units.

2. The differences between the proposed approach for assessing cybersecurity in special-purpose information systems and known approaches based on game theory, graph theory, theoretical and analytical approaches are as follows:

– while assessing cybersecurity, the type of uncertainty is additionally taken into account;

– evolving artificial neural networks and algorithms for their training were used to increase the efficiency of information processing [26];

– does not accumulate errors of training artificial neural networks as a result of processing the information coming to the input of artificial neural networks by learning the architecture and parameters;

– has less computational complexity in assessing the cybersecurity of special communication systems.

3. Evaluation of the efficiency of the proposed method was carried out. This example, in comparison with approaches based on game theory, graph theory, theoretical and analytical approaches, showed an increase in evaluation efficiency of about 20–25 % in terms of information processing efficiency.

Acknowledgments

The author's team expresses its gratitude for assistance to:

The honored worker of science and technology of Ukraine, doctor of technical sciences, professor Slyusar Vadym Ivanovych – chief researcher of the Central Research Institute of Armaments and Military Equipment of the Armed Forces of Ukraine.

The doctor of technical sciences, professor Oleksiy Viktorovych Kuvshinov – deputy head of the Educational and Scientific Institute of the Ivan Chernyakhovskiy National Defense University of Ukraine;

The doctor of technical sciences, senior researcher Sova Oleg Yaroslavovich – head of the Department of Automated Control Systems of the Military Institute of Telecommunications and Informatization named after Heroes of Kruty.

The candidate of technical sciences, associate professor Oleksandr Mykolayovych Bashkirov – leading researcher of the Central Research Institute of Armaments and Military Equipment of the Armed Forces of Ukraine.

References

1. Bashkyrov, O. M., Kostyna, O. M., Shyshatskyi, A. V. (2015). Rozvytok intehrovanykh system zviazku ta peredachi danykh dlia potreb Zbroinykh Syl. Ozbroiennia ta viyskova tekhnika, 1, 35–39.
2. Kalantaievska, S., Pievtsov, H., Kuvshynov, O., Shyshatskyi, A., Yarosh, S., Gatsenko, S. et. al. (2018). Method of integral estimation of channel state in the multiantenna radio communication systems. Eastern-European Journal of Enterprise Technologies, 5 (9 (95)), 60–76. doi: https://doi.org/10.15587/1729-4061.2018.144085
3. Shevchenko, D. (2020). The set of indicators of the cyber security system in information and telecommunication networks of the armed forces of Ukraine. Modern Information Technologies in the Sphere of Security and Defence, 38 (2), 57–62. doi: https://doi.org/10.33099/2311-7249/2020-38-2-57-62.
4. Sokolov, K., Hudyma, O., Tkachenko, V., Shyyatyy, O. (2015). Main directions of creation of IT infrastructure of the Ministry of Defense of Ukraine. Zbirnyk naukovykh prats Tsentru voienno-stratehichnykh doslidzhen Natsionalnoho universytetu oborony Ukrainy imeni Ivana Cherniakhovskoho, 3, 26–30.
5. Kuchuk, N., Mohammed, A. S., Shyshatskyi, A., Nalapko, O. (2019). The method of improving the efficiency of routes selection in networks of connection with the possibility of self-organization. International Journal of Advanced Trends in Computer Science and Engineering, 8 (1), 1–6. Available at: http://www.warse.org/IJATCSE/static/pdf/file/ijatcse01812sl2019.pdf
6. Perrine, K. A., Levin, M. W., Yahia, C. N., Duell, M., Boyles, S. D. (2019). Implications of traffic signal cybersecurity on potential deliberate traffic disruptions. Transportation Research Part A: Policy and Practice, 120, 58–70. doi: https://doi.org/10.1016/j.tra.2018.12.009
7. Wang, J., Neil, M., Fenton, N. (2020). A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. Computers & Security, 89, 101659. doi: https://doi.org/10.1016/j.cose.2019.101659
8. Matheu-García, S. N., Hernández-Ramos, J. L., Skarmeta, A. F., Baldini, G. (2019). Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices. Computer Standards & Interfaces, 62, 64–83. doi: https://doi.org/10.1016/j.csi.2018.08.003
9. Henriques de Gusmão, A. P., Mendonça Silva, M., Poleto, T., Camara e Silva, L., Cabral Seixas Costa, A. P. (2018). Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory. International Journal of Information Management, 43, 248–260. doi: https://doi.org/10.1016/j.ijinfomgt.2018.08.008
10. Shyshatskyi, A., Sova, O., Zhuravskyi, Y., Zhyvotovskyi, R., Lyashenko, A., Cherniak, O. et. al. (2020). Development of resource distribution model of automated control system of special purpose in conditions of insufficiency of information on operational development. Technology Audit and Production Reserves, 1 (2 (51)), 35–39. doi: https://doi.org/10.15587/2312-8372.2020.198082
11. Mohammad, A. (2020). Development of the concept of electronic government construction in the conditions of synergetic threats. Technology Audit and Production Reserves, 3 (2 (53)), 42–46. doi: https://doi.org/10.15587/2706-5448.2020.207066
12. Bodin, L. D., Gordon, L. A., Loeb, M. P., Wang, A. (2018). Cybersecurity insurance and risk-sharing. Journal of Accounting and Public Policy, 37 (6), 527–544. doi: https://doi.org/10.1016/j.jaccpubpol.2018.10.004
13. Cormier, A., Ng, C. (2020). Integrating cybersecurity in hazard and risk analyses. Journal of Loss Prevention in the Process Industries, 64, 104044. doi: https://doi.org/10.1016/j.jlp.2020.104044
14. Hoffmann, R., Napiórkowski, J., Protasowicki, T., Stanik, J. (2020). Risk based approach in scope of cybersecurity threats and requirements. Procedia Manufacturing, 44, 655–662. doi: https://doi.org/10.1016/j.promfg.2020.02.243
15. Promyslov, V. G., Semenkov, K. V., Shumov, A. S. (2019). A Clustering Method of Asset Cybersecurity Classification. IFAC-PapersOnLine, 52 (13), 928–933. doi: https://doi.org/10.1016/j.ifacol.2019.11.313
16. Zarreh, A., Saygin, C., Wan, H., Lee, Y., Bracho, A. (2018). A game theory based cybersecurity assessment model for advanced manufacturing systems. Procedia Manufacturing, 26, 1255–1264. doi: https://doi.org/10.1016/j.promfg.2018.07.162
17. Gerami Seresht, N., Fayek, A. R. (2020). Neuro-fuzzy system dynamics technique for modeling construction systems. Applied Soft Computing, 93, 106400. doi: https://doi.org/10.1016/j.asoc.2020.106400
18. Folorunso, O., Mustapha, O. A. (2015). A fuzzy expert system to Trust-Based Access Control in crowdsourcing environments. Applied Computing and Informatics, 11 (2), 116–129. doi: https://doi.org/10.1016/j.aci.2014.07.001
19. Luy, M., Ates, V., Barisci, N., Polat, H., Cam, E. (2018). Short-Term Fuzzy Load Forecasting Model Using Genetic–Fuzzy and Ant Colony–Fuzzy Knowledge Base Optimization. Applied Sciences, 8 (6), 864. doi: https://doi.org/10.3390/app8060864
20. Salmi, K., Magrez, H., Ziyyat, A. (2019). A Novel Expert Evaluation Methodology Based on Fuzzy Logic. International Journal of Emerging Technologies in Learning (iJET), 14 (11), 160. doi: https://doi.org/10.3991/ijet.v14i11.10280

21. Allaoua, B., Laoufi, A., Gasbaoui, B., Abderrahmani, A. (2009). Neuro-Fuzzy DC Motor Speed Control Using Particle Swarm Optimization. Leonardo Electronic Journal of Practices and Technologies, 15. Available at: http://lejpt.academicdirect.org/A15/001_018.pdf
22. Rybak, V. A., Shokr, A. (2016). Analysis and comparison of existing decision support technology. System analysis and applied information science, 3, 12–18.
23. Hassanzad, M., Orooji, A., Valinejadi, A., Velayati, A. (2017). A fuzzy rule-based expert system for diagnosing cystic fibrosis. Electronic Physician, 9 (12), 5974–5984. doi: https://doi.org/10.19082/5974
24. Shang, W., Gong, T., Chen, C., Hou, J., Zeng, P. (2019). Information Security Risk Assessment Method for Ship Control System Based on Fuzzy Sets and Attack Trees. Security and Communication Networks, 2019, 1–11. doi: https://doi.org/10.1155/2019/3574675
25. Safdari, R., Kadivar, M., Nazari, M., Mohammadi, M. (2017). Fuzzy Expert System to Diagnose Neonatal Peripherally Inserted Central Catheters Infection. Health Information Management, 13 (7), 446–452.
26. Al-Qudah, Y., Hassan, M., Hassan, N. (2019). Fuzzy Parameterized Complex Multi-Fuzzy Soft Expert Set Theory and Its Application in Decision-Making. Symmetry, 11 (3), 358. doi: https://doi.org/10.3390/sym11030358
27. Koshlan, A., Salnikova, O., Chekhovska, M., Zhyvotovskyi, R., Prokopenko, Y., Hurskyi, T. et. al. (2019). Development of an algorithm for complex processing of geospatial data in the special-purpose geoinformation system in conditions of diversity and uncertainty of data. Eastern-European Journal of Enterprise Technologies, 5 (9 (101)), 35–45. doi: https://doi.org/10.15587/1729-4061.2019.180197
28. Dudnyk, V., Sinenko, Y., Matsyk, M., Demchenko, Y., Zhyvotovskyi, R., Repilo, I. et. al. (2020). Development of a method for training artificial neural networks for intelligent decision support systems. Eastern-European Journal of Enterprise Technologies, 3 (2 (105)), 37–47. doi: https://doi.org/10.15587/1729-4061.2020.203301
29. Pievtsov, H., Turinskyi, O., Zhyvotovskyi, R., Sova, O., Zvieriev, O., Lanetskii, B., Shyshatskyi, A. (2020). Development of an advanced method of finding solutions for neuro-fuzzy expert systems of analysis of the radioelectronic situation. EUREKA: Physics and Engineering, 4, 78–89. doi: https://doi.org/10.21303/2461-4262.2020.001353
30. Zuiev, P., Zhyvotovskyi, R., Zvieriev, O., Hatsenko, S., Kuprii, V., Nakonechnyi, O. et. al. (2020). Development of complex methodology of processing heterogeneous data in intelligent decision support systems. Eastern-European Journal of Enterprise Technologies, 4 (9 (106)), 14–23. doi: https://doi.org/10.15587/1729-4061.2020.208554
31. Shyshatskyi, A., Zvieriev, O., Salnikova, O., Demchenko, Y., Trotsko, O., Neroznak, Y. (2020). Complex Methods of Processing Different Data in Intellectual Systems for Decision Support System. International Journal of Advanced Trends in Computer Science and Engineering, 9 (4), 5583–5590. doi: https://doi.org/10.30534/ijatcse/2020/206942020
32. Sova, O., Golub, V., Shyshatskyi, A., Ostapchuk, V., Nalapko, O., Zubrytska, H. (2019). Method of Forecasting the Duration of Data Transmission Routes in Mobile Radio Networks. 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON). doi: https://doi.org/10.1109/ukrcon.2019.8879978
33. Mamdani, E. H., Assilian, S. (1975). An experiment in linguistic synthesis with a fuzzy logic controller. International Journal of Man-Machine Studies, 7 (1), 1–13. doi: https://doi.org/10.1016/s0020-7373(75)80002-2
34. Sugeno, M. (1985). Industrial applications of fuzzy control. Elsevier Science Inc., 269.