КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (20), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.20.100110
UDC 004.056

**Hanna Lyashenko**
Military Institute of Telecommunications and Information Technologies named after Heroes of Kruty
ORCID 0000-0002-5318-8663
*1o2l3d@gmail.com*

**Olexandr Shemendiuk**
Military Institute of Telecommunications and Information Technologies named after Heroes of Kruty
ORCID 0000-0002-5594-2973
*1o2l3d@gmail.com*

**Taras Bokhno**
Military Institute of Telecommunications and Information Technologies named after Heroes of Kruty
ORCID 0000-0002-7033-8723
*1o2l3d@gmail.com*

**Oleksiy Cherednychenko**
Military Institute of Telecommunications and Information Technologies named after Heroes of Kruty
ORCID 0000-0002-0816-8321
*1o2l3d@gmail.com*

# DEVELOPING A METHODOLOGICAL APPROACH TO ASSESSING STATE INFORMATION SECURITY

**Abstract.** The article proposes a methodology for assessing the information security of the state. The object of the study is the information security system of the state. The subject of the study is the development of a methodical approach to the assessment of information security of the state.
Scope of practical use of research results: It is advisable to use the proposed scientific results in conducting research and development works on the creation of intelligent systems for collecting, processing and analyzing information about the state of information security of the state and developing requirements for hardware and software of this type of systems.
The difference between the proposed method and the known ones, which determines its novelty, lies in the possibility of:
– identification and qualitative interpretation of threats to information security;
– simulation of scenarios of extreme situations caused by the realization of threats to information security;
– assessment of risks that have characteristics of several classes and ranking of assets of the information security system of the state according to their degree of criticality;
- carry out an assessment of the number of critically vulnerable assets of the state information security system;
- to substantiate the composition and probability of realization of threats to the information security of the state, capable of causing extreme situations in the information and telecommunications system;
- conducting an assessment of risks from their implementation in systems of information collection, processing and transmission.
The application of the proposed methodology allows to automate the process of analyzing threats to information security and assessing the risks of breaching information security in information collection, processing and transmission systems.

**Keywords:** information security, risks, threats to information security.

## INTRODUCTION

The object of the research is the system of information security of the state. The subject of the research is developing a methodological approach to assessing state information security.

ISSN 2663 - 4023

**Problem description**

The experience of operations (combat operations) of recent years shows the growing role of information influence measures on the systems of collection, processing and transmission of special purpose information and decision-making officials.

The specificity of measures to ensure the information security of the state is that, on the one hand, it is necessary to solve the task of collecting, processing and transmitting information, and on the other hand, it is necessary to counteract measures of information influence on the systems of collecting, processing and transmitting information and decision-making officials.

Given this, information attacks have become a real threat and are one of the priority problems of national security and risk management.

Information security covers all security measures that can be taken to protect against these impacts. A significant increase in the complexity and intensity of information attacks in recent years has forced most developed countries to strengthen their defenses and adopt national information security strategies. Therefore, the problem of ensuring the protection of the information space in the world is urgent.

In order to develop countermeasures against informational influences on the systems of collection, processing and transmission of special purpose information and decision-making officials, the authors propose to develop a methodology for assessing the information security of the state [1–8].

That is why the purpose of this article should be considered the method of assessing the information security of the state.

**Suggested solution to the problem**

The existing approaches to ensuring the information security of the state have the following disadvantages:

– take into account individual components of the information security of the state;

– not suitable for complex processing of various types of data;

– unable to adapt to new types and types of threats to information security.

Taking into account the above, *the purpose of the research* is to develop a methodological approach to assessing state information security.

**Research materials and methods**

In the course of the research, let's use:

– classical methods of analysis – to solve the problem of analyzing the conditions and factors affecting the systems of information security of the state;

– methods of resource optimization – for making management decisions on the management of the system of information security of the state;

– the theory of artificial intelligence – for processing various types of data in the course of identification and assessment of challenges and threats to information security of the state.

## RESEARCH RESULTS AND DISCUSSION

### 1. Development of a methodology for assessing the information security of the state

The methodology for assessing the information security of the state consists of the following main stages (Fig. 1):

***1. Input of initial data.*** At this stage, the initial situation for evaluation and the available data on the possibilities of information influence are introduced.

***2. Analysis of information security threats.*** In the course of the specified procedure, the following actions are performed:

1) establishing the context of information threats;

2) conducting an information security audit, which includes: questionnaires; detection of information security threats; assessment of assets of information collection, processing and transmission systems; detection of threats; identification of typical attack vectors and formation of scenario concepts.

Analysis of threats to information security in the methodology is carried out by comparing identified threats to information security with threats that are available in the knowledge base. Also, at this stage, a list of critical assets and identified vulnerabilities corresponding to information security threats is formed, as well as typical attack vectors representing a chain of vulnerabilities, threats, and target assets [5–10].

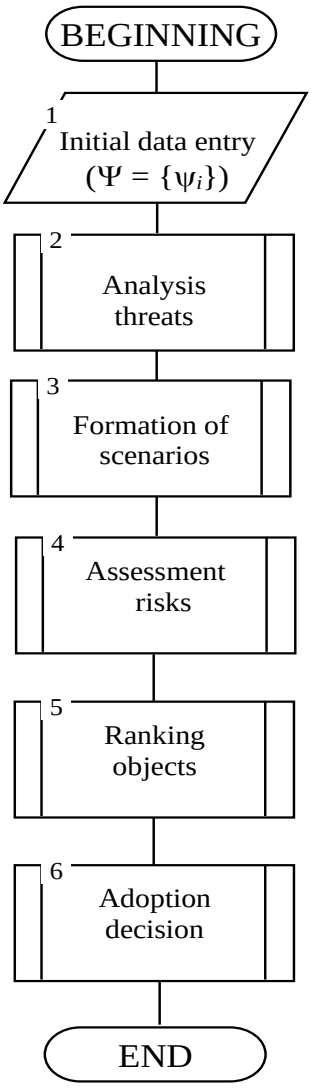


*Fig. 1 Algorithm for the implementation of the methodology for assessing the information security of the state*

On the basis of the obtained result, concepts and connections between them are formed for the further construction of scenarios. Formally, the initial data of the first stage of information security threat analysis and risk assessment are represented by formula (1):

$$P = \left\{ V_i, T_j, A_k, R_a^v \right\}, \quad (1)$$

ISSN 2663 - 4023

$P$ – attack model represented by a chain of vulnerabilities and threats; $V_i$ – identified vulnerabilities of information collection, processing and transmission systems; $T_j$ – threats to information security; $A_k$ – target assets of attacks; $R_a^v$ – attack vectors.

***3. Formation of scenarios of extreme situations caused by the implementation of threats to information security.***

This procedure is based on system analysis and information security research. As a tool for scenario analysis of the impact of information threats on the occurrence of extreme situations, it is proposed to use neurofuzzy models (Fig. 2).

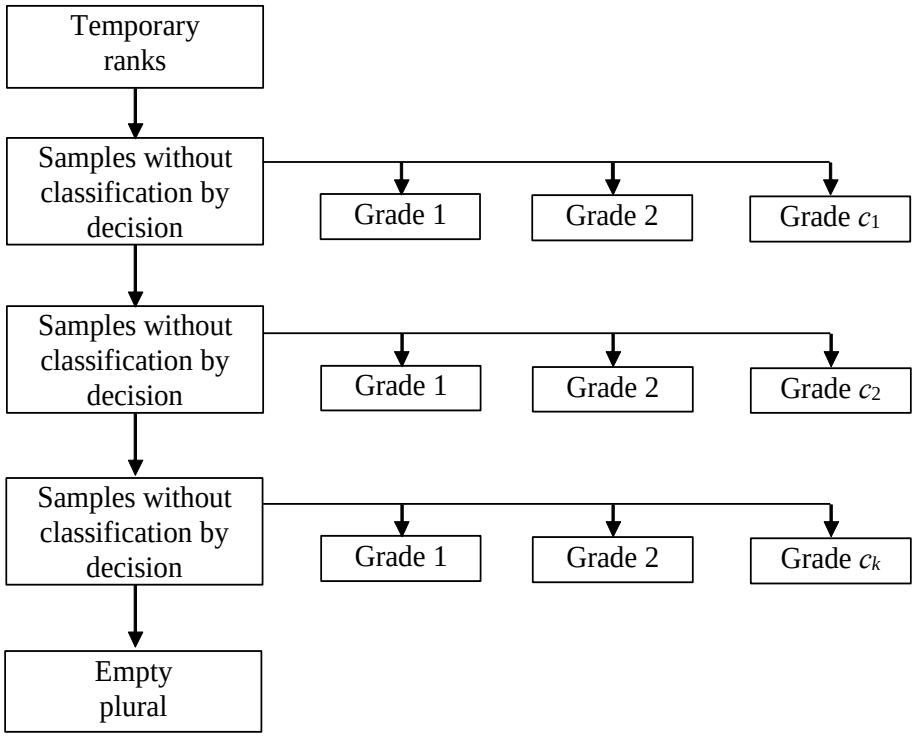


*Fig. 2 General view of the decision tree of the neurofuzzy model*

The architecture of decision trees is implemented using fuzzy "IF-THEN" rules, which are considered as general building blocks of a decision tree [8].

Decision tree (DT) is one of the most famous methods used to obtain classified data from large datasets.

There are several reasons for their widespread use:

– in many cases, the accuracy of decision trees is comparable or higher than other classification models [9];

– most decision trees do not require a large number of parameters for their adjustment in the DT design [10];

– due to their intuitively attractive topology, the results of classification models are easy to understand [11, 12].

However, the main drawback of existing neurofuzzy mathematical models and other methods, which represents the nature of a “black box”, is the complexity of interpreting the identification model and the lack of providing an understanding (presentation) of the interaction between technical indicators and fluctuations (changes) in the values of time series.

There are cases in which it is rather difficult to classify an object with one or another feature with high accuracy. These situations are solved thanks to the possibilities of fuzzy logic,

when we talk not just about belonging to some class, feature, attribute, but about its degree of belonging.

The data necessary for the operation of the algorithm should be presented in the form of a flat table. All information about objects (hereinafter examples) from the subject area should be described in the form of a finite set of features (hereinafter attributes). Each attribute must have a discrete or numeric value. The attributes themselves must not vary from instance to instance, and the number of attributes must be fixed for all instances.

Let *T* be a given set of examples, where each element of this set is described $m$ attributes. Number of examples in the plural *T* will be called the power of this set $|T|$.

Let through $\{C_1, C_2, ..., C_k\}$ labeled classes (class label values), then there are 3 situations[3–7]:

1. Plural *T* has one or more instances belonging to the same class $C_k$. Then the decision tree for *T* – this is the letter that defines the class $C_k$;

2. Plural *T* does not have a single example, that is, an empty set. Then it is again a letter, and the class associated with the letter is chosen from another set different from *T*.

3. Plural *T* has examples related to different classes. In this case, it is necessary to split the set *T* on some subsets.

For this, one of the signs is chosen, which has two or more different values from each other $O_1, O_2, ..., O_n$. *T* is divided into subsets $T_1, T_2, ..., T_n$, where each subset $T_i$ contains all relevant examples $O_i$ for the selected feature. This procedure will continue recursively until the final set consists of examples belonging to the same class.

The task is to build a hierarchical classification model in the form of a tree from a set of examples *T*. The process of building a tree is top-down.

In the first step, there is an empty tree (there is only the root) and the original set *T* (which is associated with the root).

Then, as a result of partitioning, n (by the number of attribute values) subsets are obtained and n descendants of the root are created, each of which is matched with its own subset obtained by partitioning the set *T*. This procedure is then applied recursively to all subsets (descendants of the root) and beyond.

The advantage of this approach is that attribute reuse is not excluded when building a tree, and any of the attributes can be used an unlimited number of times when building a tree. Let's have a check $X$ (any attribute can be selected as a check) that accepts $n$ values $A_1, A_2, ..., A_n$.

The only information available to us is how the classes are distributed over the set *T* and its subsets obtained by dividing by $X$. This is exactly what we use when defining the criterion. Let $Freq(C_j, S)$ – a set of examples from some set belonging to the same class $C_j$. Then the probability that an example is randomly selected from the set $S$ will belong to the class $C_j$.

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

According to information theory, the amount of information contained in a message depends on its probability:

$$\log_2\left(\frac{1}{P}\right), \quad (3)$$

ISSN 2663 - 4023

Since there is a logarithm with a binary base, expression (3) gives a quantitative estimate in bits.

$$Info(T) = \sum_{j=1}^{k} \frac{freq(C_j, T)}{|T|} \cdot \log_2 \frac{freq(C_j, T)}{|T|}. \quad (4)$$

get an estimate of the average amount of information needed to determine the class of an example from a set. The algorithm uses an information-theoretic approach. To choose the most appropriate attribute, it is suggested to use the following criterion:

$$Info(T) = \sum_{j=1}^{k} \left| \frac{T_i}{T} \right| \cdot Info(T_i), \quad (5)$$

Then the criterion for selecting an attribute will be the following formula:

$$Gain(X) = Info(T) - Info_x(T). \quad (6)$$

Criterion (6) is calculated for all attributes. The attribute that maximizes the given expression is chosen. This attribute will be a check in the current node of the tree, and then further construction of the tree takes place on this attribute.

That is, the value of this attribute will be checked in the node and further movement along the tree will take place depending on the experience gained.

Criterion (6) must be maximized. From the properties of entropy, it is known that the maximum possible value of entropy is reached in the event that all its messages are equally likely.

In our case, entropy (5) reaches its maximum when the frequency of occurrence of classes in the examples of the set T is equally probable. It is necessary to choose such an attribute that, when broken down by it, one of the classes has the highest probability of appearance. This is possible in the case when entropy (5) will have a minimum value and criterion (6) reaches its maximum.

In the case of numeric attributes, it is necessary to choose some threshold against which all values of the attribute should be compared. Let a numeric attribute have a finite number of values. Let's mark them $\{V_1, V_2, ..., V_n\}$.

Let's pre-sort all the values. Then any value between $V_i$ and $V_{i+1}$, divides all examples into two sets: those to the left of this value $\{V_1, V_2, ..., V_n\}$, and those on the right $\{V_{i+1}, V_{i+2}, ..., V_{i+n}\}$.

As a threshold, it is possible to choose the average between these values $V_i$ and $V_{i+1}$:

$$TH_i = \frac{V_i + V_{i+1}}{2}. \quad (7)$$

Thus, the task of finding the threshold is significantly simplified, and let's bring everything to consideration $n-1$ potential threshold values $TH_1, TH_2, TH_3, ..., TH_{n-1}$.

Formulas (4), (5) and (6) are used sequentially for all potential threshold values, and the one that gives the maximum value according to criterion (6) is chosen among them. This value is then compared with the values of criterion (6) calculated for other attributes.

If it turns out that among all the attributes, the specified numerical attribute has the maximum value according to criterion (6), then it is chosen as a check.

***4 Assessment of information security breach risks.***

The specified procedure is aimed at identifying risks, their qualitative and quantitative assessment, as well as the ranking of the considered objects according to the established criteria,

which can be the values of both the integral risk indicator for the object and the indicators of individual types of risks.

The specified procedure contains recommendations on risk description, qualitative and quantitative assessment, selection of assessment scales, and facility energy ranking. The procedure for assessing the risks of breach of information security includes 3 main stages: description of risks; qualitative and/or quantitative risk assessment; ranking of objects.

***5. Ranking of objects in information collection, processing and transmission systems.***

Within the framework of the specified technology, objects are ranked in accordance with the magnitude of risks that may be caused by cybernetic influence, information about which is included in the database of external and internal threats or factors.

The proposed ranking criterion:

$$K^S = \{C, R, \Theta\}, \quad (7)$$

$K^S$ – significance criterion; $C$ – risk assessment criterion; $R$ – an integral indicator of the risks of the affected objects; $\Theta$ – the object is represented by a set of characteristics.

**2. Results of the analysis and discussion of the results**

Based on the developed approach, the basic architecture of the intelligent system for information security needs is presented in Fig. 3.

It is based on MySQL database management system, server subsystem and client subsystem.

Physically, this suite of applications can be hosted on a server under the management of any server operating system, such as Windows 2016 Server, Ubuntu 18.04 Server, etc.

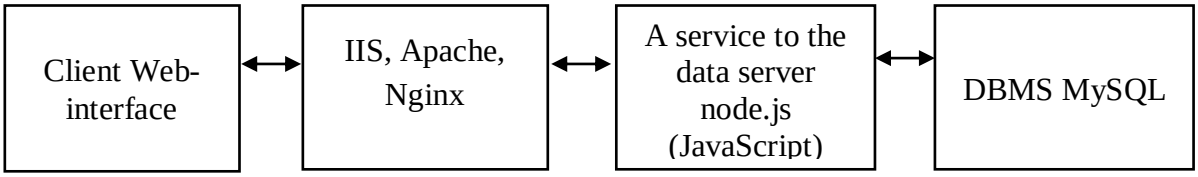


*Fig. 3. Functional scheme of the complex of programs of intellectual system*

The basis of the system of storage and accumulation of data in the “Data lake” in physical form is the MySQL database. The structure of the MySQL database table of information security consists of the following tables:

table1 contains information obtained from open sources of information. In addition, the table includes fields to identify the operator that has entered data into the “Data Lake” and possible conclusions that are drawn by the data user;

the source1 table contains information on the number and type of information on resources that are involved in the information security. This information has a personal stamp. Therefore, the mentioned system should have access to protected information systems, in which information with the secrecy mark is circulated “secretly” and above;

– the pidrozd table contains fields that allow revealing the belonging of a subdivision to the group, as well as to specify its geographical coordinates if available. This information has a secret stamp. Therefore, the mentioned system should have access to protected information systems, in which information with the secrecy mark is circulated “secretly” and above;

– the user and owner tables are created to separate users and grant them access to the system and to monitor a specific group of messages.

The proposed method allows:

– to justify the methods of researching the state of the information security system;

– to define and identify challenges and threats to national security;

– to justify the necessary management decisions in the management of the information security system.

The advantages of the research include:

– adaptation to new challenges and threats to information security;

– reasonableness of management decisions in the management of the information security system;

– taking into account different raw data that are different in origin and measurement units;

– analyzing large data sets.

The shortcomings of the research include:

– the need for adequate software to implement possible research methods;

– availability of time to carry out calculations of the state of the information security system.

It is advisable to implement the specified method in algorithmic and program software during research of the state of the information security system.

The limitations of this study are:

– the need to have complete initial data for adequate operation of the intelligent system;

– availability of time for system training;

– the need for a sufficient number of training and test samples;

– sufficient computing resources for processing various types of data and training in real time.

Further improvement of the mentioned approach for an objective and complete approach should be considered as the direction of further research of the state of the information security system.

## CONCLUSIONS

1. In the course of the research carried out by the authors, the authors developed a methodology for assessing the information security of the state.

The difference between the proposed method and the known ones, which determines its novelty, lies in the possibility of:

– detection and qualitative interpretation of information security threats;

– modeling scenarios of extreme situations caused by the implementation of threats to information security;

– assessment of risks that have the characteristics of several classes and ranking of assets of the information security system of the state according to the degree of their criticality;

– carry out an assessment of the number of critically vulnerable assets of the state information security system;

– to justify the composition and probability of realization of threats to the information security of the state, capable of causing extreme situations in the information and telecommunications system;

– conducting an assessment of risks from their implementation in systems of information collection, processing and transmission.

2. The application of the proposed methodology allows automating the process of analyzing information security threats and assessing the risks of information security violations in information collection, processing, and transmission systems.

## REFERENCES

1 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 (1.2), 1–6.

2 Sova, O., Turinskyi, O., Shyshatskyi, A., Dudnyk, V., Zhyvotovskyi, R., Prokopenko, Y. et al. (2020). Development of an algorithm to train artificial neural networks for intelligent decision support systems. Eastern-European Journal of Enterprise Technologies, 1 (9 (103)), 46–55. https://doi.org/10.15587/1729-4061.2020.192711

3 Makarenko, S. I., Mikhailov, R. L. (2013). Otcenka ustoichivosti seti sviazi v usloviiakh vozdeistviia na nee destabiliziruiushchikh faktorov. Radioengineering and Telecommunication Systems, 4, 69–79.

4 Bodyanskyy, E. V., Strukov, V. M., Uzlov, D. Yu. (2017). Generalizedmetrics in the problem of analysis of multidimensional data with different scales. Zbirnyk naukovykh prats Kharkivskoho natsionalnoho universytetu Povitrianykh Syl, 3 (52), 98–101.

5 Semenov, V. V., Lebedev, I. S. (2019). Processing of signal information in problems of monitoring information security of unmanned autonomous objects. Scientific and Technical Journal of Information Technologies, Mechanics and Optics, 19 (3), 492–498. https://doi.org/10.17586/2226-1494-2019-19-3-492-498

6 Zhou, S., Yin, Z., Wu, Z., Chen, Y., Zhao, N., Yang, Z. (2019). A robust modulation classification method using convolutional neural networks. EURASIP Journal on Advances in Signal Processing, 2019 (1). https://doi.org/10.1186/s13634-019-0616-6

7 Shaheen, E. M., Samir, M. (2013). Jamming Impact on the Performance of MIMO Space Time Block Coding Systems over Multi-path Fading Channel. REV Journal on Electronics and Communications, 3 (1-2), 68–72. https://doi.org/10.21553/rev-jec.56

8 Malik, S., Kumar, S. (2017). Optimized Phase Noise Compensation Technique using Neural Network. Indian Journal of Science and Technology, 10 (5), 1–6. https://doi.org/10.17485/ijst/2017/v10i5/104348

9 Rotshteyn, A. P (1999). Intellektual'nyye tekhnologii identifikatsii: nechotkiye mnozhestva, geneticheskiye algoritmy, neyronnyye seti. Vinnitsa: “UNIVERSUM”, 320.

10 Mazhara, O. A. (2015). Treat algorithm implementation by the basic matchalgorithm based on CLIPS programming environmen. Elektronnoye modelirovaniye, 37 (5), 61–75.

11 Bolotova, S. Yu., Makhortov, S. D. (2011). Algoritmy relevantnogo obratnogo vyvoda na osnove resheniya produktsionno-logicheskikh uravneniy. Iskusstvennyy intellekt prinyatiye resheniyi, 2, 40–50.

12 Zhyvotovskyi, R. M., Shyshatskyi, A. V., Petruk, S. N. (2017). Structural-semantic model of communication channel. Problems of Infocommunications. Science and Technology. Kharkiv, 524–529. https://doi.org/10.1109/infocommst.2017.8246454

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (20), 2023
ISSN 2663 - 4023

**Ганна Ляшенко**
Військовий інститут телекомунікації та інформатизації ім. Героїв Крут, Київ, Україна
ORCID 0000-0002-5318-8663
*1o2l3d@gmail.com*

**Олександр Шемендюк**
Військовий інститут телекомунікації та інформатизації ім. Героїв Крут, Київ, Україна
ORCID 0000-0002-5594-2973
*1o2l3d@gmail.com*

**Тарас Бохно**
Військовий інститут телекомунікації та інформатизації ім. Героїв Крут, Київ, Україна
ORCID 0000-0002-7033-8723
*1o2l3d@gmail.com*

**Олексій Чередниченко**
Військовий інститут телекомунікації та інформатизації ім. Героїв Крут, Київ, Україна
ORCID 0000-0002-0816-8321
*1o2l3d@gmail.com*

# РОЗРОБКА МЕТОДИЧНОГО ПІДХОДУ ДО ОЦІНКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

**Анотація.** У статті запропоновано методику оцінки інформаційної безпеки держави. Об'єктом дослідження є система інформаційної безпеки держави. Предметом дослідження є розробка методичного підходу до оцінки інформаційної безпеки держави.
Сфера практичного використання результатів дослідження: Запропоновані наукові результати доцільно використовувати при проведенні дослідно-конструкторських робіт зі створення інтелектуальних систем збору, обробки та аналізу інформації про стан інформаційної безпеки держави та розробки вимог до апаратного забезпечення та програмне забезпечення цього типу систем.
Відмінність запропонованого способу від відомих, що визначає його новизну, полягає в можливості:
– ідентифікація та якісна інтерпретація загроз інформаційній безпеці;
– моделювання сценаріїв екстремальних ситуацій, спричинених реалізацією загроз інформаційній безпеці;
– оцінка ризиків, що мають ознаки кількох класів, та ранжування активів системи інформаційної безпеки держави за ступенем їх критичності;
- провести оцінку кількості критично вразливих активів державної системи інформаційної безпеки;
- обґрунтувати склад та ймовірність реалізації загроз інформаційній безпеці держави, здатних спричинити екстремальні ситуації в інформаційно-телекомунікаційній системі;
- проведення оцінки ризиків від їх впровадження в системах збору, обробки та передачі інформації.
Застосування запропонованої методики дозволяє автоматизувати процес аналізу загроз інформаційній безпеці та оцінки ризиків порушення інформаційної безпеки в системах збору, обробки та передачі інформації.

**Ключові слова:** інформаційна безпека, ризики, загрози інформаційній безпеці.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 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 (1.2), 1–6.
2 Sova, O., Turinskyi, O., Shyshatskyi, A., Dudnyk, V., Zhyvotovskyi, R., Prokopenko, Y. et al. (2020). Development of an algorithm to train artificial neural networks for intelligent decision support systems. Eastern-European Journal of Enterprise Technologies, 1 (9 (103)), 46–55. https://doi.org/10.15587/1729-

4061.2020.192711

3 Makarenko, S. I., Mikhailov, R. L. (2013). Otcenka ustoichivosti seti sviazi v usloviiakh vozdeistviia na nee destabiliziruiushchikh faktorov. Radioengineering and Telecommunication Systems, 4, 69–79.

4 Bodyanskyy, E. V., Strukov, V. M., Uzlov, D. Yu. (2017). Generalizedmetrics in the problem of analysis of multidimensional data with different scales. Zbirnyk naukovykh prats Kharkivskoho natsionalnoho universytetu Povitrianykh Syl, 3 (52), 98–101.

5 Semenov, V. V., Lebedev, I. S. (2019). Processing of signal information in problems of monitoring information security of unmanned autonomous objects. Scientific and Technical Journal of Information Technologies, Mechanics and Optics, 19 (3), 492–498. https://doi.org/10.17586/2226-1494-2019-19-3-492-498

6 Zhou, S., Yin, Z., Wu, Z., Chen, Y., Zhao, N., Yang, Z. (2019). A robust modulation classification method using convolutional neural networks. EURASIP Journal on Advances in Signal Processing, 2019 (1). https://doi.org/10.1186/s13634-019-0616-6

7 Shaheen, E. M., Samir, M. (2013). Jamming Impact on the Performance of MIMO Space Time Block Coding Systems over Multi-path Fading Channel. REV Journal on Electronics and Communications, 3 (1-2), 68–72. https://doi.org/10.21553/rev-jec.56

8 Malik, S., Kumar, S. (2017). Optimized Phase Noise Compensation Technique using Neural Network. Indian Journal of Science and Technology, 10 (5), 1–6. https://doi.org/10.17485/ijst/2017/v10i5/104348

9 Rotshteyn, A. P (1999). Intellektual'nyye tekhnologii identifikatsii: nechotkiye mnozhestva, geneticheskiye algoritmy, neyronnyye seti. Vinnitsa: “UNIVERSUM”, 320.

10 Mazhara, O. A. (2015). Treat algorithm implementation by the basic matchalgorithm based on CLIPS programming environmen. Elektronnoye modelirovaniye, 37 (5), 61–75.

11 Bolotova, S. Yu., Makhortov, S. D. (2011). Algoritmy relevantnogo obratnogo vyvoda na osnove resheniya produktsionno-logicheskikh uravneniy. Iskusstvennyy intellekt prinyatiye resheniyi, 2, 40–50.

12 Zhyvotovskyi, R. M., Shyshatskyi, A. V., Petruk, S. N. (2017). Structural-semantic model of communication channel. Problems of Infocommunications. Science and Technology. Kharkiv, 524–529. https://doi.org/10.1109/infocommst.2017.8246454