UDC 004: 316.6 **doi: 10.26906/SUNZ.2020.4.109**

I. Havryk[1], A. Shyshatskyi[3], O. Sova[3], A. Lyashenko[3], S. Palamarchuk[3] , Ye. Neroznak[3], V. Velychko[3]

[1] National Defence University of Ukraine named after Ivan Chernyakhovsky, Kyiv, Ukraine
[2] Central Research Institute of Weapons and Military Equipment of Armed Forces, Kyiv, Ukraine
[3] Military institute of telecommunications and information named after Heroes of Krut, Kyiv, Ukraine

METHODS OF CYBER SECURITY ASSESSMENT IN THE SPECIAL PURPOSE INFORMATION AND TELECOMMUNICATIONS SYSTEM

Abstract. To increase the effectiveness of the fight against cybercrime, developed countries have begun the relevant work to increase the security of their own information and telecommunications networks of general and special purpose. Current global trends in the spread of cybercrime and the intensification of cyberattacks indicate the growing importance of combating it for the further development of society, which in turn leads to the attribution of certain groups of public relations of the cybersphere to the competence of legal regulation. The current situation with cybercrime requires constant improvement of methods of combating cybercrime, development of information systems and methods aimed at ensuring cybersecurity in the country. That is why the authors of this article developed a method for assessing cybersecurity in a special purpose information and telecommunications system. During the research, the authors used the main provisions of communication theory, queuing theory, artificial intelligence, as well as general scientific methods of analysis and synthesis. The difference between the proposed method from the known ones, which determines its novelty, is the possibility of: detection and qualitative interpretation of cyber threats; modeling scenarios of extreme situations caused by the implementation of cyber threats; assessment of risks that have the characteristics of several classes and ranking of assets of the information and telecommunications system according to the degree of their criticality; perform an assessment of the number of critically vulnerable assets of the information and telecommunications system; substantiate the composition and probability of cyber threats that can cause extreme situations in the information and telecommunications system; conducting risk assessment of their implementation in the information and telecommunications system. The practical significance of the proposed method is fatigue, that its application allows to automate the process of analysis of cyber threats and risk assessment of cybersecurity of information and telecommunications system.

Keywords: cyberspace; cyberattacks; protection; cybersecurity; state security, information and telecommunication networks, artificial intelligence.

Introduction

The experience of operations (combat operations) in recent years shows the growing role of information and telecommunications systems (ITS) for special purposes in achieving the goal of the operation (combat operations).

The specificity of special-purpose ITS is that on the one hand they solve the problem of transmission and processing of information, and on the other hand they should meet the requirements of survivability while influencing on the enemy.

In order to disorganize management and achieve information of superiority by the enemy, devices of electronic warfare and cybernetic influence on special-purpose ITS are widely used [1-5].

Cyberattacks on ITS have become a real threat and they are one of the priority issues of national security and risk management.

Cybersecurity encompasses all security measures that can be taken to protect 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 defenses and adopt national cybersecurity strategies. Therefore, the problem of ensuring the protection of cyberspace in the world is relevant.

In order to develop measures to combat cyber influences on special-purpose ITS, the authors propose to develop a methodology for assessing cybersecurity in special-purpose ITS [6-8].

That is why ***the purpose of this article*** should be considered a method of assessing cybersecurity in the information and telecommunications system of special purpose.

Presentation of the main material

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

1. Entering the output data. At this stage, the operational situation and available data on the possibilities of cybernetic impact on special-purpose ITS are introduced.

2. Analysis of cyber threats. During the implementation of this procedure, the following steps are performed: 1) establishing the context of ITS; 2) conducting a security audit in ITS, which includes: questionnaires; detection of cyber threats in ITS assets; valuation of ITS assets; threat detection; identification of typical attack vectors and formation of scenario concepts.

The analysis of cyberthreats in the methodology is carried out by comparing the identified cyberthreats with cyberthreats that are available in the knowledge base. Also at this stage, a list of critical assets and identified vulnerabilities corresponding to the cyber threat,

as well as typical attack vectors, which are a chain of vulnerabilities, threats and target assets [6-8].

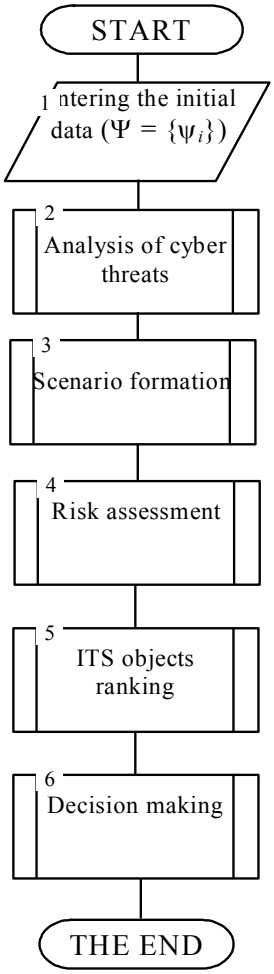

Fig. 1 Algorithm for implementing evaluation methods

Based on the obtained result, concepts and connections 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 (1).

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

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

3. The formation of scenarios of extreme situations in ITS caused by the implementation of cyber threats.

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

As a tool for scenario analysis of the impact of cyber threats on the occurrence of extreme situations in special-purpose ITS, it is proposed to use neurofuzzy models (Fig. 2).

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

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

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 configuration in the DT construction [10];

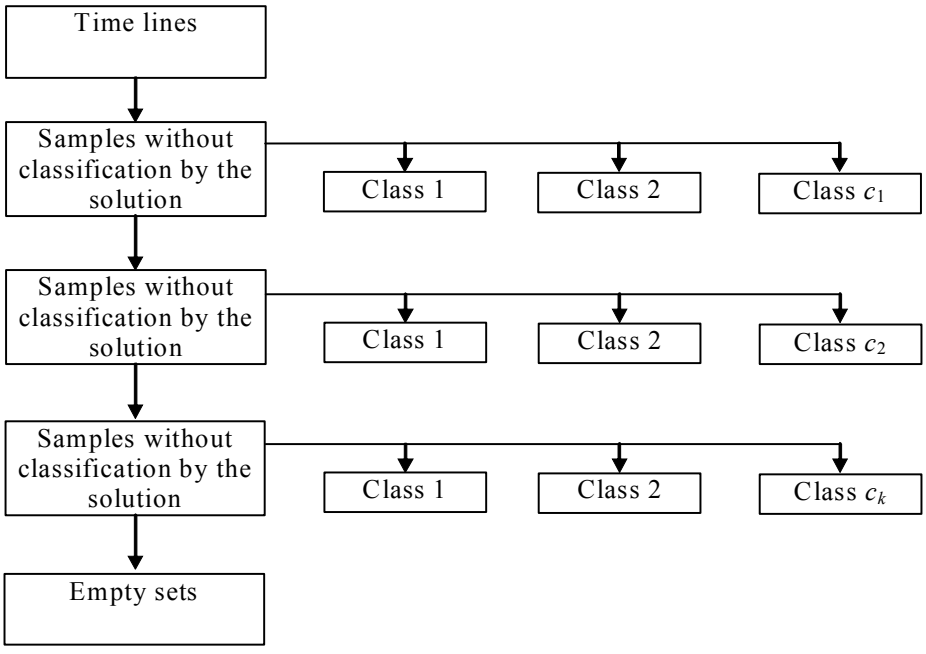

Fig. 2. General view of the decision tree of the fuzzy model

- due to their intuitively attractive topology, the results of classification models are easy to understand [12-14].

However, the main disadvantage of existing fuzzy mathematical models and other methods, which has the nature of the "black box", is the difficulty of interpreting the identification model and lack of understanding (representation) of the interaction between technical indicators and fluctuations (changes) in time series values.

There are cases in which it is difficult to classify an object with high accuracy with one or another feature. These situations are solved due to the possibilities of fuzzy logic, when we talk not just about belonging to a class, sign, attribute, but about its degree of belonging.

The data, which is required for the operation of the algorithm, must be presented in the form of a flat table. All information about objects (following examples) from the subject area should be described as a finite set of features (following attributes). Each attribute must have a discrete or numeric value. The attributes themselves should not change from the example, for example, and the number of attributes should be fixed for all examples.

Let it be that a set of examples *T*, where each element of this set is described by m attributes. The number of examples in the set T will be called the power of this set $|T|$.

Let it be that through $\{C_1, C_2, ..., C_k\}$ marked classes (values of the class label), then there are 3 situations [3-7]:

1. The set *T* has one or more examples belonging to the same class C_k. Then the decision tree for *T* is the letter that defines the class C_k;

2. The set *T* has no example (an empty set). Then it is again a letter, and the class associated with the letter is chosen from another set that is different from *T*.

3. The set *T* has examples belonging to different classes. In this case, it is necessary to divide the set *T* into some subsets.

To do this, choose one of the features that has two or more different values $O_1, O_2, ..., O_n$. T is divided into subsets $T_1, T_2, ..., T_n$, where each subset T_i contains all the examples that are relevant to the selected feature O_i. This procedure will be recursively continued until the finite 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 many examples *T*. The process of building a tree occurs from top to bottom.

In the first step, we have an empty tree (there is only a root) and a source set *T* (associated with the root).

Then as a result of partitioning *n* (on number of attribute values) subsets are received and *n* descendants of a root are created, to each of which the subset received at partition of set *T* is put. Then this procedure is recursively applied to all subsets (descendants of a root and further).

The advantage of this approach consists in the fact that the reuse of the attribute while building a tree is not excluded and any of the attributes can be used an unlimited number of times while building a tree.

Let it be that we have X check (any attribute can be selected as a check) that takes n values $A_1, A_2, ..., A_n$.

Then the partition T on the test X will give us subsets $T_1, T_2, ..., T_n$, with equal respectively $A_1, A_2, ..., A_n$.

The only information available to us is how the classes are distributed on the set T and its subsets obtained by partitioning by X. This is what we use to define the criterion.

Let be that $Freq(C_j, S)$ is a set of examples from some set S belonging to the same class C_j. Then the probability that a randomly selected example from the set S will belong to the class C_j.

$$P = \frac{freq(C_j, S)}{|S|}. \tag{2}$$

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

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

Since we have a logarithm with a binary base, the expression (3) gives a quantitative estimate in bits.

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

We obtain an estimate of the average amount of information that is necessary 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:

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

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

$$Gain(X) = Info(T) - Info_x(T). \tag{6}$$

The criterion (6) is calculated for all attributes. We selected an attribute that maximizes this expression. This attribute makes a check in the current node of the tree, and then it occurs the further construction of the tree.

Then, the node will check the value of this attribute and further movement on the tree will occur depending on the experience.

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

In our case, the entropy (5) reaches its maximum when the frequency of occurrence of classes in the examples of the set T is equally likely to happen. It is necessary to choose such attribute that at partition on it one of classes had the greatest probability of emergence.

This is possible in the case when the entropy (5) will have a minimum value and criterion (6) reaches its maximum.

In the case of numeric attributes, you must select a threshold with which all attribute values must be compared. Let the numeric attribute have a finite number of values. Let's mark them $\{V_1, V_2, ..., V_n\}$.

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

As a threshold, you can 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 we lead to the consideration of all $n-1$ potential threshold values $TH_1, TH_2, TH_3, ..., TH_{n-1}$.

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

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

4. Assessing the risks of cybersecurity in ITS.

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

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

5. Ranking of objects in ITS.

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

The proposed ranking criterion:

$$K^S = \{C, R, \Theta\}, \quad (8)$$

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

Conclusion

1. Nowadays, the main topic of discussion in the world should be to strengthen cybersecurity and reduce the number of cyber attacks in cyberspace.

This problem needs to be solved as soon as possible, because the created models of cyber weapons have a global reach, almost instantaneous impact without any way to obtain warning about its use.

Cybersecurity is the only thing that can prevent information loss and interference by some countries in the security of others.

2. In the course of the research, the authors developed a methodology for assessing cybersecurity in a special-purpose information and telecommunications system.

The difference between the proposed method from the known, which determines its novelty, consists in the possibility of:

the detection and qualitative interpretation of cyber threats;

modeling scenarios of extreme situations caused by the implementation of cyber threats;

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

the assessment perform of the number of critically vulnerable assets of the information and telecommunications system;

the substantiate of the composition and probability of cyber threats that can cause extreme situations in the information and telecommunications system;

the conduction of the risk assessment of their implementation in the information and telecommunications system.

3. The application of the proposed technique allows to automate the process of analysis of cyber threats and risk assessment of cybersecurity of information and telecommunications system.

Areas of further research should be considered the development of methods for improving the cyber security of information and telecommunication systems.

REFERENCES

1. Shyshatskiy, A.V., Bashkirov, O.M. and Kostina, O.M (2015). "Development of integrated systems and data for Armed Forces", Arms and military equipment, No 1(5), pp. 35-40. available at : http://journals.uran.ua/index.php/2414-0651/issue/view/1%285%29%202015 (last accessed november 5, 2019).
2. Zhuk, O.G., Shyshatskiy, A.V., Zhuk, P.V. and Zhyvotovskyi, R.M (2017). "Methodological substances of management of the radio-resource managing systems of military radio communication", Information Processing Systems, Vol. 5(151), pp. 16-25. https://doi.org/10.30748/soi.2017.151.02.
3. Romanenko, I. and Shyshatskyi, A (2017). "Analysis of modern condition of military radiocommunication system", Advanced Information Systems, Vol. 1, No. 1, pp. 28-33, DOI: https://doi.org/10.20998/2522-9052.2017.1.05.
4. AJP-6: Allied Joint Doctrine for Communication and Information System [Electronic Resource]. – Mode of access: https://www.gov.uk/goverment/uploads/system/uploads/attachment_data/file/200016/20110401-ajp6_cis_secured.pdf.
5. AAP-31: NATO Glossary of Communication and Information Systems Terms and Definitions (November 2001). – 119 p.
6. AJP-5: Allied Joint Doctrine for Operational-level Planning – 2013. – 299p.
7. NATO Glossary of Terms and Definitions: AAP-6 [Edition 2018]. – NATO Standardization Agency, 2018. – 2019 p.
8. Electronic Warfare Planning and Management Tool (EWPMT). United States Army Acquisition Support Center. 2016. available at : http://asc.army.mil/web/portfolio-item/iews-electronic-warfare-planning-and-manage ment-tool-ewpmt/ (last accessed august 25, 2020).
9. Popov, A.O. and Tverdokhlibov, V.V(2014). "General tendencies of development of means of electronic warfare ", Arms and military equipment, No. 4 (4), pp. 4-10.
10. Shyshatskiy, A., Kalantaievska, S., Malyk, O., Tiurnikov, M., Zhuk, P. and Pikul, R(2019). "Foundation the ways of radio electronic warfare devices development". Advanced information systems. No. 3(2). pp. 98-103.
11. Romanenko, I. O., Shyshatskyi, A.V., Zhyvotovskyi, R. M. and Petruk, S.M (2017). "The concept of the organization of interaction of elements of military radio communication systems". Science and Technology of the Air Force of the Armed Forces of Ukraine. No 1. pp. 97-100.
12. Salnik, S.V., Salnik, V.V., Sova, O. Ya. and Stampkovskaya, Ya.A (2016). "Model of invasion of mobile radio networks of the class MANET". Proceedings of Kharkiv National University of the Air Force. No.(46). pp. 79-84.
13. Salnik, S.V., Salnik, V.V., Simonenko, O.A. and Sova, O. Ya(2015). "A method for detecting intrusions into mobile radio networks based on neural networks". Science and Technology of the Air Force of the Armed Forces of Ukraine. No. 4(21). Pp. 82-90.
14. Kravchuk, S.A., Minochkin, D.A. and Sova, O. Ya(2013). "Analysis of directions of increasing the efficiency of functioning of modern satellite communication systems". Science and Technology of the Air Force of the Armed Forces of Ukraine. No. 2(11). Pp. 140-147.

Надійшла (received) 16.09.2020
Прийнята до друку (accepted for publication) 04.11.2020

Методика оцінювання кібербезпеки
в інформаційно-телекомунікаційній системі спеціального призначення

І. С. Гаврик, А. В. Шишацький, О. Я. Сова, О. О. Троцько, Г. Т. Ляшенко,
С. А. Паламарчук, Є. І. Нерознак, В. П. Величко

Анотація. Для підвищення ефективності боротьби з кіберзлочинністю, розвинені країни світу досить давно почали відповідні роботи, необхідні для підвищення захищеності власних іфнормаційно-телекомунікаційних мереж загального та спеціального призначення. Сучасні світові тенденції поширення кіберзлочинності та посилення кібератак свідчать про зростання значення боротьби з нею для подальшого розвитку суспільства, що у свою чергу зумовлює віднесення певних груп суспільних відносин кіберсфери до компетенції правового регулювання. Ситуація, яка склалася на сьогоднішній день з кіберзлочинністю, вимагає постійного удосконалення методів боротьби з кіберзлочинами, розробки інформаційних систем та методів, спрямованих на забезпечення кібербезпеки країни. Саме тому, авторами зазначеної статті проведено розробку методики оцінювання кібербезпеки в інформаційно-телекомунікаційній системі спеціального призначення. В ході проведеного дослідження авторами використані основні положення теорії зв'язку, теорії масового обслуговування, штучного інтелекту, а також загальнонаукові методи аналізу та синтезу. Відмінність запропонованої методики від відомих, що визначає її новизну полягає у можливості: виявлення та якісної інтерпретації кіберзагроз; моделюванні сценаріїв екстремальних ситуацій, викликаних реалізацією кіберзагроз; оцінюванні ризиків, що мають ознаки декількох класів і ранжування активів інформаційно-телекомунікаційної системи за ступенем їх критичності; виконати оцінку кількості критично вразливих активів інформаційно-телекомунікаційної системи; обґрунтувати склад і ймовірність реалізації кіберзагроз, здатних викликати екстремальні ситуації в інформаційно-телекомунікацій системі; проведення оцінювання ризиків від їх реалізації в інформаційно-телекомунікацій системі. Практична значимість запропонованої методики полягає втому, що її застосування дозволяє автоматизувати процес аналізу кіберзагроз та оцінки ризиків порушення кібербезпеки інформаційно-телекомунікацій системі.

Ключові слова: кіберпростір; кібератаки; захист; кібербезпека; безпека держави, інформаційно-телекомунікаційні мережі, штучний інтелект.