ІНФОКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ ТА ЕЛЕКТРОННА ІНЖЕНЕРІЯ
INFORMATION AND COMMUNICATION TECHNOLOGIES, ELECTRONIC ENGINEERING

№ 2 (4), 2022

https://doi.org/10.23939/ictee2022.02.033

PROTECTION OF STATE MANAGEMENT OF CRITICAL INFRASTRUCTURE OBJECTS UNDER THE INFLUENCE OF CYBER ATTACKS

S. Toliupa, S. Buchyk[1], O. Kulinich[2], O. Buchyk[1].

[1] Taras Shevchenko National University of Kyiv, 60, Volodymyrska Str., Kyiv, 01033, Ukraine
[2] National university of life and environmental sciences of Ukraine, 15, Heroiv Oborony, Kyiv, 03041, Ukraine

Corresponding author:S. Toliupa (e-mail: tolupa@i.ua)

(Received 1 October 2022)

Critical infrastructure describes physical assets and cyber systems that are so vital to the nation that their incapacitation or destruction would have an important impact on our physical and economic security or public health and safety. The critical infrastructure of country provides essential services that are the foundation of Ukrainian society. Being in the current state of hybrid war significantly increases the threat to critical infrastructure. National security largely depends on the protection of such facilities. The article proposes a method for managing the protection state against external cyberattacks on information systems of critical infrastructure facilities based on distributive identification and dynamic programming. The essence of the method is to use the distributive identification of the external cyberattacks parameters with the choice of applying measures to protect the system with a complete description of the information system and taking into account the strategies of influence on it based on dynamic programming. Unlike similar methods, the developed method makes a management decision on the security state of information resources with a set of input external cyber attacks parameters based on parallel-distributive identification and dynamic programming. The method allows to increase the reliability of making a management decision on assessing the security state of information resources in the information system of a critical infrastructure facility, provided that the time of making a management decision on assessing the security state is no more than similar methods.

Keywords:*cybersecurity, critical infrastructure facilities, model, cyberattack, information system, protection.*
UDC 621.391

1. Introduction

Critical infrastructure describes physical assets and cyber systems that are so vital to the nation that their incapacitation or destruction would have an important impact on our physical and economic security or public health and safety. The critical infrastructure of country provides essential services that are the foundation of Ukrainian society. The current state of hybrid warfare significantly increases the threat to critical infrastructure. National security largely depends on the protection of such facilities.

The relation between national security and critical infrastructure protection is vital for the progress of any society and its proper social functioning. Critical infrastructure protection aims to ensure the supply of essential goods and services such as energy, transportation and healthcare. Critical infrastructures include not only buildings and facilities, but also supply systems and services in the broadest sense. Major disruptions, such as a nationwide power outage, can have far-reaching consequences for the population and cause significant damage to the economy. Critical infrastructure protection consists of a variety of structural, technical, organizational and legal measures aimed at preventing such disruptions or restoring functionality in the event of an incident.

2. Analysis of sources and publications

To reduce the vulnerability of critical infrastructure, a number of laws and recommendations have been adopted in the country [1, 2], which aim to improve the protection of critical infrastructure in all relevant sectors of economic activity. The initiative of all relevant agencies to protect critical information infrastructure is aimed at strengthening the security and resilience of vital information and communication technology (ICT) infrastructures.

Increasing the resilience of critical infrastructure has become a priority for authorities not only in our country but also around the world. New threats and unconventional attacks on critical infrastructure have exposed the limits of traditional risk assessment and mitigation efforts. Some threats cannot be predicted, and reducing all possible risks to the lowest possible level is not always cost-effective. This has shifted the focus to resilience to ensure continuity of service after disruptive events, especially in cases where they cannot be predicted. Today, intrusion and attack detection systems are usually software or hardware-software solutions that automate the process of monitoring events occurring in an information system or network, and independently analyze these events in search of signs of security problems. Since the number of different types and methods of organizing unauthorized intrusions into other people's networks has increased significantly in recent years, attack detection systems (IDS) have become a necessary component of the security infrastructure of most organizations [3–4].

Today, the solution of issues of ensuring security in IS and managing the state of their security is described in the works of domestic and foreign researchers, namely: Buryachok V. L., Buchyk S. S., Hnatiuk S. O., Parkhuts L. T., Evseev S. P., Kazmirchuk S. V., Korchenko O. G., Kuznetsov O. O., Subacha I. Y., PtacekaT., Elmasry G., Albers P., Camp O. and others.

It should be noted that one of the topical areas that is actively developing in the field of information security is the detection of cyber attacks and prevention of intrusions into the IS by unauthorized parties (UAP). It should also be noted that attacks on IP are becoming more sophisticated, global and frequent every year.

Thus, the process of the latest information technologies development and implementation provide unprecedented conditions for the accumulation and use of information, as well as create a fundamental dependence on their normal functioning of all life spheres of society and the state: economy, politics, national and international security, etc. Such dependence becomes a vulnerability in the functioning of systems and critical national infrastructures facilities and enables negatively-minded elements and groups to take advantage of it to carry out illegal actions in cyberspace by violating the integrity, availability and confidentiality of information and causing damage to information resources and information systems. At the same time, the possibility of using information technology in cyberspace in the interests of military-political and power confrontation, terrorism and hacker attacks is of particular concern [5].

3. The main material

Existing information security event management systems provide for decision-making to identify cyber threats based on the processing of a set of heterogeneous data parameters. Reference [6] shows the model of information security management in the information system. Threats in it, in turn, are implemented by multidirectional cyber attacks. Information, while passing through the system, is analyzed according to the relevant parameters to detect security breaches. As a result, the output of the security control unit indicates the presence of a change in the security state of the IS and the ability to counteract threats.

When developing and conducting research on intrusion detection systems, one of the key tasks is the selection of data sets on which testing will be conducted. Large development companies primarily focus on their own databases, specialized for specific tasks and applications.

When developing network attack detection systems, it is important to be able to compare test results with other developments and research, which leads to the need to use known publicly available databases.

Today, the two most common training databases with known attacks are DARPA [7] and KDD [8].The DARPA (Defense Advanced Research Project Agency) training database was formed based on the study of network traffic data and information from the file system to identify simulated intrusions carried out by specialists during the recording of network dumps. The training data contains both real network traffic flow and specially simulated background traffic. The total number of attack types included in the 2019 DARPA test data was 62 attacks. From the attacker's point of view, these attacks can be divided into four categories: Denial of Service (DoS) attacks; Remote to Local (R2L) attacks; User to Root (U2R) attacks; Probing / surveillance (PRB) attacks.

The final training records, adjusted and supplemented in 2020, contain network traffic and audit records, lasting six weeks for training data and two weeks for test data. In total, they contain 95 different attacks. Unlike the DARPA training data, the KDD database contains not dumps of network traffic, but processed information in the form of arrays containing 42 key values. This database has been successfully used by many researchers to analyze the applicability of various mathematical methods in the task of detecting network attacks, mainly due to the possibility of using data arrays from most software tools without performing additional processing.

The composition of 42 parameters considered in the KDD database was justified by several scientific works [11, 12] devoted to the detection of anomalies in network traffic. However, when studying the possibilities of detecting specific network attacks, it is not enough to analyze only the presented parameters, but it is also necessary to consider the payload of network packets–the higher layers of the TCP/IP protocol stack.

Based on the input parameters of the traffic, it is checked for security violations and marked as "violation" or "not violation". The specified record consists of 42 fields. The first 41 fields describe the features of the network traffic, and the last 42nd field indicates the type of traffic that is described. This field can take the value "normal" if this network connection belongs to the "normal" state of traffic, or the name of the attack type (for example, "ipsweep").

When using the second criterion, researchers try to identify the most "interesting" directions. The "interestingness" is usually understood as the extent to which the distribution in a given direction differs from the normal distribution. It can be shown that for a fixed covariance matrix, the maximum entropy falls on the Gaussian distribution. For any other distribution, the entropy is strictly less.

Solving the problem of cyberattack classifying (for example, by its signature), the security state management subsystem matches the above network traffic parameters with 62 types of the most commonly used attacks. The classified parameters of input data (attacks) relate to a set of management decisions on response options for each individual type of attack. As a result, the IS security state is managed.

In the light of the above views, the developed method of managing the protection state against external cyberattacks takes into account the following features of the IS: different dimension of networks; geographically dispersed components of the IS; the output of IS elements outside the controlled area; not only PCs are used to access the processed resources; high requirements for the availability of information resources; the configuration of the IS changes (changes in the composition of users and their privileges, updated versions of programs, new services, equipment, etc.); interconnection and interdependence of IS elements.

Designation of input data. The situation of the system being in an equal probability state of IS security violations is considered. At the same time, there are both security breaches from external cyber attacks on the IS and the search for countermeasures to detected changes in the security state. To model such a situation, a training sample, which has 20 % of normal information messages and 80 % of abnormal information messages containing types of attacks, is built. A database with countermeasures for the set of detected violations is also built. Since each phase of the attack is characterized by a set of techniques and is implemented by an internal or external attacker, therefore, in order to manage the security state against external cyber attacks, the types of violations are identified based on data parameters that are specific to external attacks. The total number of parameters x_i = 18.

During the detection of attacks, a logical inference mechanism will be used to describe the base of input parameters. Based on the comparison of input parameters, the system will form a decision on their clustering. Clustering methods group data into clusters based on the similarity of objects and parameters. Most clustering methods start by selecting a center point for each cluster, and a lot of items are distributed across the clusters. After that, the centers are adjusted and the elements are redistributed. Clustering allows to examine and detect anomalies without requiring an explicit set of classes or anomalies types. Clustering is widely used to detect network anomalies [13]. Detection of unknown network attacks is often based on clustering methods. Homogeneous groups with similar characteristics or clusters are formed by splitting a set of elements without any labels. In the system, it is extremely important to identify correctly clusters in order to remove them from outliers as much as possible. The ultimate goal of these methods is to determine the degree to which outliers deviate from the clusters. Using a simple comparison with a threshold value, outliers with a high degree of deviation from the clusters are marked as anomalies [10].

The input value is: $X = XH \cup XM \cup XL$ – parameters of incoming traffic;

$XM = \{x_i(t), i = \overline{1,18}\}$ – a set of traffic parameters that are characteristic of external cyber attacks;

$XH = \{x_h(t), h = \overline{1,15}\}$ – a set of traffic parameters that are characteristic of internal cyber attacks;

XL–a set of traffic parameters that are not involved in the implementation of the method.

Limitations and assumptions: Attack types are identified: DoS, U2R, R2L, Probe, Side. Abnormal behavior is identified as a newly detected security state. The process of security state management is quasi-stationary on the time interval $(t_0 ... T)$.

It is necessary: to increase the reliability of managerial decision-making on assessing the state of protection of IP D from external cyber attacks, provided that the time of managerial decision-making will not be more than that of similar methods:

$$\begin{cases} D \to \max; \\ D > D_{isn} \\ T \le T_{isn} \end{cases},$$

The essence of the method is: the use of distributive identification of the parameters of external cyber attacks with the choice of applying measures to protect the system with a complete description of the IS and taking into account the influence strategies on it based on dynamic programming.

Management of the state of IS protection against external cyber threats can take place when identifying the parameters of violations that are implemented by a set of multidirectional and different in content attacks.

Therefore, we will identify the input data (data parameters) of the traffic.

I. Under identification we understand finding the optimal model built on the basis of observations of the input and output variables of the object, namely the set of traffic parameters. The task of identification is the reverse task of system synthesis.

Taking into account the tasks of identification, there are two types:

- structural identification, which allows you to determine the shape of the model from some given class of functions;
- parametric identification, which determines the parameters of the model.

However, based on the task, to identify the input data based on the parameters of cyber attacks (signatures), parametric identification will be applied.

In parametric identification, data about an object is processed to obtain a posteriori information about it. In this case, the parameters of the selected model are estimated. In the simplest cases, such estimation can be performed by the transient response graph.

When building a security assessment model based on experimentally obtained data, there is a common situation for which almost all the information used by the processor to solve the problem is limited to a sample of the original data. Therefore, to solve the problem of parametric identification, methods are used that focus exclusively on information about the discrepancy between the outputs of the object and the model.

In general, for any model of a known structure, the level of discrepancy between the outputs of the object and the model depends on the choice of model parameters. Therefore, if we introduce an indicator of the quality of parametric identification, which integrates all the information about the levels of discrepancies and contains information about the dependence of the level of discrepancy between the outputs of the object and the model on the values of the model parameters, then minimizing this indicator will allow us to determine the optimal model parameters.

Determining the acceptable value of IP risk. The acceptable value of risk is understood as a reasonable amount of losses with which the ICS management can agree and act in the conditions of its existence. Informational risks are those associated with the possibility of losses when the institution uses IP. To determine the acceptability of risk in the construction of information security management systems, the average value of losses is determined [11]:

$$A_{cp} = \frac{\sum_{i=1}^{m} A_i}{m} = \frac{\sum_{i=1}^{m} (P_{план.} - P_i)}{m},$$

where i – the number of measurements performed over a period of time.

To determine the acceptable values of the frequency of losses, the equation: $a_1x_1 + a_2x_2 + ... + a_jx_j + a_nx_n = r_n, j \in (1,n)$ is used. The value of the losses a_j is determined by assessing the information resource by the owners, the frequency of x_j is calculated by appropriate methods. In real conditions, it is often allowed to determine estimates of acceptable risk r_{np} and losses a_j with an accuracy of integers.

Taking into account the strategies of cyberattacks on IS, the probability of j_z cyberattacks on a set of IS objects l is calculated:

$$P(j_z, l) = \prod_{i=1}^{l} P_i^{j_z}. \tag{1}$$

The problem of parametric identification can be formulated as follows: to select on the set $\{X\}$ of possible values of parameters such values $\widetilde{X}$, so that the differences of indicators reach their minimums, that is, the purpose of this analysis is to search:

$$\tilde{X}(t) = \arg\min_{y \in \hat{X}} \sum_{i=1}^{18} (y_i(t) - x_i(t))^2, \tag{2}$$

where $\hat{X}$ – traffic parameters described in the database; $x_i(t)$ – parameters describing the flow of incoming traffic data and obtained from the data distribution block.

II. The next step will be to manage the state of IS security against external cyber attacks on IP and information, the requirement for the protection of which is established by law, based on the identified data and finding the correspondence of these data to the set of options for counteracting violations. To do this, a set of data on the state of IS security is obtained from the database $XM(t) = \{x_1,..., x_{18}\}$, a set of data on possible security breaches $\Lambda = \{\lambda_1,..., \lambda_n\}$, where n is the number of variants of the sets contained in the database and the sets of signatures and possible violations are compared.

The security state is a period of time of the information security property and is described by the value of the corresponding indicator at a certain fixed point in time in models characterized by a dynamic structure of construction, to which the IS belongs

The process of obtaining an assessment of the state of IS protection and the process of applying security measures are implemented in steps. At each k step, a certain set of data on the state of IS security $X(t) = \{x_1,..., x_{18}\}$ is obtained, which depends on possible security breaches $\Lambda = \{\lambda_1,..., \lambda_n\}$, characterizing the state of IS security and affecting the choice of the used security measures. Using the obtained and already available information about the state of IS security $X_k, X_{k-1},...,$, a managerial decision is made on the use of security measures $U_k = U(t) = \{u_1,...,u_n\}$, which may depend on previously made decisions U_{k-1}, U_{k-2}. Thus, the full set of data on the state of security of the system X, decisions on the use of security measures U and the implemented options for influencing security breaches Λ can be described:

$$X(t) = \{x_1,..., x_{18}\},\ U = \{U_1,..., U_k\},\ \Lambda = \{\Lambda_1,..., \Lambda_k\},\ k = 1,2,..., N.$$

It should be counted that the security measures U_k involved at any step may affect possible security breaches $\Lambda_{k+1}, \Lambda_{k+2},...$ at the following steps, as well as the amount and quality of data obtained at these steps on the state of IS security $X(t)$. Such feedback is typical for general-type IS, in which all or some components of the solution U_k are actions that manage possible security breaches Λ_k. In other words, the taken measures affect the value of Λ_k and further steps, and such multi-step decision-making processes are manageable [16].

The mathematical reflection of this feedback is the dependence of the probability distributions of the values Λ_k and $X(t)$ on the sequence of previously applied security measures $U_{k-1},...,U_k$. A complete statistical description of the multi-step process for any set of adopted security measures is achieved by setting a sequence of conditional probability distributions for the observed data and parameters for all values of $k = 1,2,...,N$. When making managerial decisions on the application of the necessary security measures U_k, we use only those observation data that are obtained up to and including the k step. Therefore, the decision-making rule on the application of the security measures U_k can be set by the probabilistic measure p_k, which depends on X_k, as well as on the set of previous decisions $\{u_1,..., u_n\} = U_{k-1}$. In this case, the value of p_k will be determined by the expression:

$$p_k = p_k(U_k \mid X_k, U_{k-1}). \tag{3}$$

Finding the optimal sequence of decision-making for a multi-step procedure is carried out by dynamic programming methods in a general stochastic form, which, under certain restrictions on the probability distribution for X_k and Λ_k and the function of changing the security state (losses function) $g(U_k, \Lambda_k, X_k)$, $k = 1,..., N$, allow to build an effective computational procedure for finding optimal solutions. At the same time, the optimal sequence of decision-making on the use of security measures is determined by the recurrence relation, which contains a sequence of minimizations and averages for the values of a posteriori risks.

The average value of the risk of violations is determined by the expression:

$$R(t) = M\{g(U, \Lambda_k, X_k)\}, U = \left\{U_1, U_2, ..., U_k\right\}, \tag{4}$$

where M is the mathematical expectation.

Then the minimum (Bayesian) average risk for the optimal decision rule at k -th step:

$$R(A)=\min_{U_1,...,U_k} M\{g(U,\Lambda_k,X_k)\}=\min_{U_1,...,U_{k-1}}(\min_{U_k} M\{M\{g(U,\Lambda_k,X_k)\,|\,X_k,U\}\}), \tag{5}$$

where the conditional mathematical expectation represents the posteriori risk function for a set of decisions U_k and observation data X_k :

$$R_k(U,X_k)=M\{g(U,\Lambda_k,X_k)\,|\,X_k,U\}. \tag{6}$$

Taking into account (5), the mathematical expectation of the function of changing the security state is determined:

$$M\{g(U,\Lambda_k,X_k)\}=M\{R_k(U,X_k)\}=M\{M\{R_k(U,X_k)\,|\,X_k,U_{k-1},...,U_1\}\}. \tag{7}$$

From which it follows that

$$\min_{U_k} M\{M\{g(U,\Lambda_k,X_k)\,|\,X_k,U\}\}=M\{\min_{U_k} R_k(U,X_k)\}. \tag{8}$$

Thus, the optimal Bayesian decision rule at k -th step is determined from the condition:

$$\min_{U_k} R_k(U,X_k)=\min_{U_k} M\{g(U_k,\Lambda_k,X_k))\,|\,X_k,U_k\}. \tag{9}$$

The structure of the algorithm for implementing the method of managing the state of protection against external cyberattacks on the IC based on the algorithm of distributive identification and dynamic programming is shown in Fig. 1.

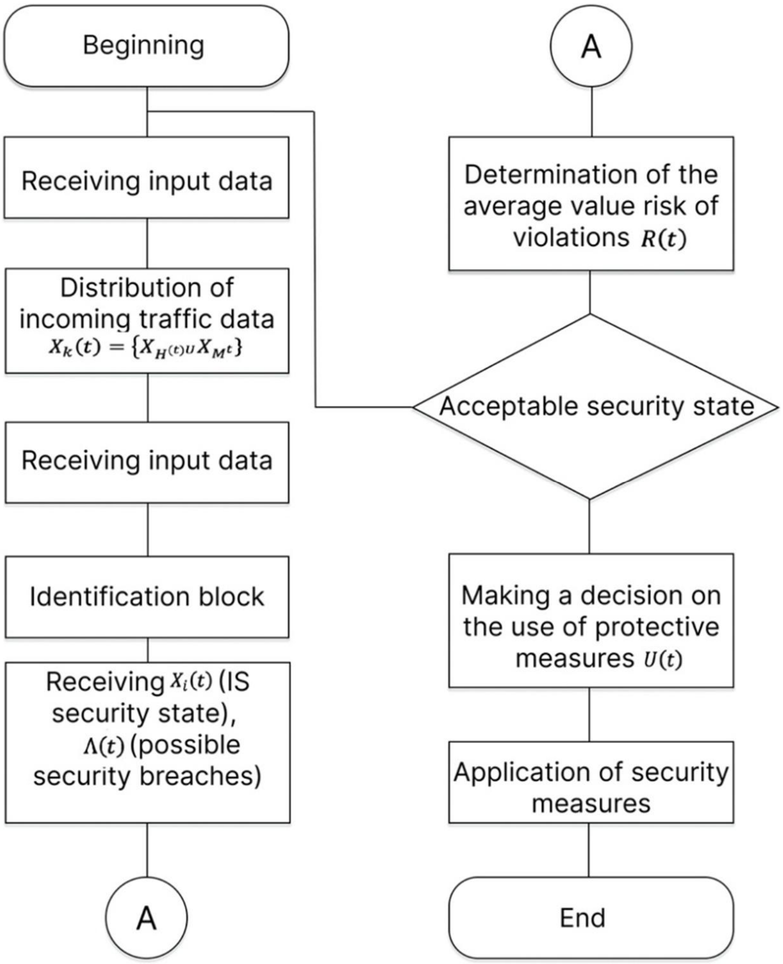
Beginning
Receiving input data
Distribution of incoming traffic data $X_k(t)=\{X_{H(t)}uX_{M^t}\}$
Receiving input data
Identification block
Receiving $X_i(t)$ (IS security state), $\Lambda(t)$ (possible security breaches)
A
A
Determination of the average value risk of violations $R(t)$
Acceptable security state
Making a decision on the use of protective measures $U(t)$
Application of security measures
End

Fig. 1. Structure of the algorithm for implementing the method of managing the state of protection against external cyber attacks

Together with the expressions (3) and (4) for the final value of the posteriori risk, the relation (9) determines the optimal sequence of application of counteraction to violations (management decision-making).

Conclusion

Consequently, the article proposes a method of managing the security state against external cyberattacks on ICS based on distributive identification and dynamic programming. The essence of the method is to use the distributive identification of the parameters of external cyberattacks with the choice of applying measures to protect the system with a complete description of the IS and taking into account the influence strategies on it based on dynamic programming. Unlike similar methods, the developed method makes a management decision on the state of IP security with a set of input parameters of external cyber attacks based on parallel-distributive identification and dynamic programming. The method allows to increase the reliability of making a management decision on assessing the state of IP security in the IS, provided that the time of making a management decision on assessing the state of security is not more than that of similar methods.

References

[1] *Law of Ukraine "On Critical Infrastructure" (1882-IX dated November 16, 2021). [Electronic resource]. Resolution of the CMU dated 09.10.2020 No. 1109 "Some issues of critical infrastructure facilities".[Electronic resource].*

[2] *Lukova-Chuiko N. V. Methods of intelligent data distribution in network intrusion detection systems and functional resistance of information systems to cyber attacks. / N.V. Lukova-Chuiko, S. V. Toliupa, V. S. Nakonechnyi, M. M. Brailovsky: monograph. K.: Format, 2021. 370 p.*

[3] *Toliupa S. V., Shtanenko S. S., Berestovenko G. Classification characteristics of attack detection systems and directions of their construction. Collection of scientific works of the Military Institute of Telecommunications and Informatization named after Heroes of Krut. Iss. No. 3. 2018. Pp. 56–66.*

[4] *Toliupa S., Nakonechnyi V., Uspenskyi O. Signature and statistical analyzers in the cyber attack detection system. Information technology and security. Ukrainian research papers collection. Vol. 7, Iss.1 (12). Pp. 69–79.*

[5] *Toliupa S. V., Semko V. V., Buryachok V. L., Skladanniy P. M. Model of information protection management in the information and telecommunications system. Bulletin of the National University.*

[6] *DARPA Intrusion Detection Data Sets. [Electronic resource]. URL: https://www.ll.mit.edu/ideval/data/.*

[7] *KDD Cup 1999 Data. [Electronic resource]. URL: http://kdd.ics.uci.edu/databases/kddcup99/.*

[8] *Salnyk S. V., Storchak A. S., Mykytyuk A. V. Model of violation of the security of information resources of communication systems // Information Technology And Security,2019.No. 7(1).Pp. 25–34.*

[9] *Storchak A. S., Salnyk S. V. A method of assessing the level of security of the network part of a special purpose communication system against cyber threats // Information processing systems. 2019. No. 3(158). Pp. 98–109.*

[10] *Hryshchuk R. The method of evaluating the informativeness of the input data flow parameters for network attack detection systems [Text] / R. Hryshchuk, V. Mamarev // Information processing systems. 2012. Vol. 1, No. 4(102). Pp. 103–107.*

[11] *Northcutt S., Novak J. Network Intrusion Detection Text. 3rd edition. Indianapolis, Indiana 46290: "New Riders", 2002. 456 p.*

[12] *Lande D. V., Subach I. Yu., Boyarynova Yu. E. Fundamentals of the theory and practice of intelligent data analysis in the field of cyber security: a study guide. K.: ISZZI KPI named after Igor Sikorsky", 2018. 300 p.*

УПРАВЛІННЯ СТАНОМ ЗАХИЩЕНОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВПЛИВУ КІБЕРАТАК

С. Толюпа, С. Бучик[1], О. Кулініч[2], О. Бучик[1]

[1] Київський національний університет імені Тараса Шевченка, Володимирська, 60, Київ, 01033, Україна
[2] Національний університет біоресурсів і природокористування,
Героїв Оборони, 15, Київ, 03041, Україна

Критична інфраструктура описує фізичні активи та кіберсистеми, які є настільки життєво важливими для держави, що їх непрацездатність або знищення матиме важливий вплив на нашу фізичну чи економічну безпеку чи громадське здоров'я та безпеку. Критична інфраструктура країни надає необхідні послуги, які є основою украинского суспільства. Перебування в нинішньому стані гібридної війни значно підвищує загрозу об'єктам критичної інфраструктури. Від захисту таких об'єктів багато в чому залежить національна безпека. В статті запропоновано метод управління станом захищеності від зовнішніх кібератак на інформаційні системи об'єктів критичної інфраструктури на основі розподільчої ідентифікації та динамічного програмування. Сутність методу полягає у використанні розподільчої ідентифікації параметрів зовнішніх кібератак з проведенням вибору щодо застосування заходів із захисту системи при повному описі інформаційної системи та врахуванням стратегій впливу на неї на основі динамічного програмування. На відміну від подібних методів, розроблений метод приймає управлінське рішення щодо стану захищеності інформаційних ресурсів при множині вхідних параметрів зовнішніх кібератак на основі паралельно-розподільчої ідентифікації та динамічного програмування. Метод дозволяє збільшити достовірність прийняття управлінського рішення щодо оцінювання стану захищеності інформаційних ресурсів в інформаційній системі об'єкта критичної інфраструктури за умов часу прийняття управлінського рішення щодо оцінювання стану захищеності не більше, ніж у подібних методів.

Ключові слова: *кібербезпека, об'єкти критичної інфраструктури, модель, кібератака, інформаційна система, захищеність.*