# ASSESSMENT OF INFORMATION PROTECTION LEVEL AGAINST UNAUTHORIZED ACCESS

**Svitlana Onyshchenko[1], Alina Yanko[2], Alina Hlushko[3], Polina Sabelnikova[4]**

[1]Department of Finance, Banking and Taxation, National University "Yuri Kondratyuk Poltava Polytechnic", Poltava, Ukraine
ORCID: https://orcid.org/0000-0002-6173-4361

[2]Department of Computer and Information Technologies and Systems, National University "Yuri Kondratyuk Poltava Polytechnic", Poltava, Ukraine
ORCID: https://orcid.org/0000-0003-2876-9316

[3]Department of Finance, Banking and Taxation, National University "Yuri Kondratyuk Poltava Polytechnic", Poltava, Ukraine
ORCID: https://orcid.org/0000-0002-4086-1513

[4]Department of Computer and Information Technologies and Systems, National University "Yuri Kondratyuk Poltava Polytechnic", Poltava, Ukraine
ORCID: https://orcid.org/0009-0004-0672-3426

✉Corresponding author: Alina Yanko, e-mail: al9_yanko@ukr.net

Onyshchenko, S., Yanko, A., Hlushko, A., Sabelnikova, P. (2023). Assessment of information protection level against unauthorized access. ScienceRise, 2, 36–44. doi: http://doi.org/10.21303/2313-8416.2023.003211

ARTICLE INFO

*Article history:*
Received date 11.05.2023
Accepted date 22.06.2023
Published date 30.04.2023

*Section:*
Information Technology

DOI

10.21303/2313-8416.2023.003211

KEYWORDS

information protection
protection level assessment
information resource
computer network
information security
security indicators
security graph

ABSTRACT

**The object of research.** The study considers an effective method of assessing the information protection level in a computer network against unauthorized access based on the security graph.
**Investigated problem.** Existing approaches to assessing the information protection level against unauthorized access have certain shortcomings: the real structure of computer networks is not taken into account, losses from unauthorized access are estimated in a monetary unit, which may not always be appropriate, the variability of modern cyber-attack scenarios and dynamic characteristics are not fully taken into account.
**The main scientific results.** The results of the study showed that the proposed method of assessing the information protection level against unauthorized access in computer networks based on the security graph allows for a more accurate description of information resources due to their characteristic vulnerabilities. Based on the calculations of the security indicators of individual resources and the security of all information in the computer network, the ranking of risks and, accordingly, information resources according to the degree of criticality for the organization's activities is carried out. Recommendations have been developed to ensure the necessary information protection level against unauthorized access in the computer network.
**The area of practical use of research results.** The results of the research can be used in practice in corporate computer networks of any organizations, since the proposed method for assessing the information protection level against unauthorized access is easily adapted to the specific needs of the organization, taking into account the specifics of its activities and business.
**Innovative technological product.** The results of the study created an innovative strategy for assessing the information protection level against unauthorized access, which increases the control of information security and the compliance of computer networks with existing eligibility criteria.
**Scope of the innovative technological product.** The results of the research and the created innovative strategies relate to the information security of computer networks of any organizations.



## 1. Introduction

### 1. 1. The object of research

The study considers an effective method of assessing the information protection level in a computer network against unauthorized access based on the security graph.

### 1. 2. Problem description

The organization of the information security regime becomes a critically important strategic factor in the development of any company. At the same time, as a rule, the main attention is paid to the requirements and recommendations of the regulatory and methodological framework in the field of information protection. The goal of protecting any information resource is clear to everyone, and the implementation of protection requires serious resources. However, the greater the demands placed on the information protection system, the harder and more difficult the imple-

mentation of the task. Today, the protection of each individual element loses its significance, and the problem of creating a complex of reliable protection of the entire information infrastructure of the company arises. During the implementation of the protection system, it is necessary to take into account not only the properties of each individual element, but also their interaction, which leads to the presence of specific properties that are inherent to the elements that are connected to each other.

Currently, there are many variations of intrusion detection and prevention systems of various complexity and structure from leading companies, which are organized by hardware, software and/or software-hardware. At the same time, the level of cybercrimes related to unauthorized access (possession, destruction, etc.) of information resources grows exponentially every year [1]. The level of protection of Ukraine against digital threats according to the international rating of The Network Readiness Index is significantly lower than in European countries, which indicates a threat to the beneficial development of digitalization and the generation of cross-border threats to EU countries. Ignoring these threats leads to their entrenchment and shadow institutionalization, which completely nullifies the influence of economic regulators and requires more systematic countermeasures to solve them. Cybersecurity specialists unanimously claim that the main drawback of existing protection mechanisms is the difficulty of assessing the level of security at all stages of the life cycle of an information system [2]. Most methods of assessing the level of protection use indicators of the protection of individual resources, which are not comprehensive. These indicators do not take into account the complex processes of security violations in the computer network, as well as the processes of control and restoration of their protected state. The main problem is choosing an effective protection system for a specific task, and therefore it is necessary to correctly and correctly evaluate protection systems based on the assessment of the information protection level.

### 1. 3. Suggested solutions to the problem

The study proposed a solution to the identified problem by using an effective comprehensive method of assessing the information protection level against unauthorized access in computer networks based on the security graph. The method proposed by them for assessing the information protection level against unauthorized access in computer systems takes into account not only the security indicators of individual resources, but is mainly based on a system approach. The main emphasis is placed on the calculation of the security indicators of all information in the computer network, taking into account the structure (topology) of the network and the roles of network users. On the basis of calculations of information security indicators in the computer network, the ranking of risks and, accordingly, information resources according to the degree of criticality for the organization's activities is carried out.

## 2. Conceptualization, theoretical framework and literature review

Despite significant scientific development, cyber security specialists lack unity in understanding the essence of information security effectiveness criteria, which prevents the formation of systematic ideas about the problematic field of forming adequate management decisions in response to information security threats. The use of modern information security systems requires, on the one hand, tracking rapid changes in information technologies and emerging threats, and on the other hand, taking into account the real characteristics of hardware and software of corporate networks and systems [3]. The procedure for purchasing information security devices is simple. Solving the problem is significantly more difficult – how to protect and which security measures to apply so that the computer network meets the criterion of suitability, taking into account the minimization of costs [4]. In order to maintain the system of protection of information resources at a high level, it is necessary to study approaches to assessing the level of their protection. Such assessment for each individual case is individual and depends on many factors (cost of information, status of the organization, importance of information, level of hardware and software, etc.). Therefore, the prospect of further research is the development of the conceptual foundations of information security in the direction of the approach of assessing the information protection level against unauthorized access.

### 2. 1. Theoretical framework

The theoretical and methodological basis of the conducted analysis are modern concepts of security, research by scientists in the field of information protection systems and digitalization of the economy, international standards of information security.

**2. 2. Literature review**

Assessment of information security has been carried out since the beginning of the emergence of information technologies. There are many works on this topic, but the most relevant and fundamental works are normative documents that made a significant theoretical and practical contribution to solving the problems of information security, namely: the publication [5], which sets out and systematizes the criteria for evaluating computer protection computer systems; European criteria for assessing the security of information technologies [6], which took into account all the shortcomings and limitations outlined in [5]; Canadian criteria for assessing the security of the reliability of computer systems [7]; US federal criteria [8], developed by order of the US government and aimed at eliminating limitations, inconveniences of practical application and shortcomings [5]; International standard ISO/IEC 15408 – "Criteria for evaluating the security of information technologies" [9–11]; Standard CEM-97/017 – "General methodology for assessing the security of information technologies" [12].

Separately, it is necessary to note the publication [13], which considers the use of the emergency factor to determine the information protection level flows for a certain class of computer network architecture.

The considered regulatory documents are the basis of a unified international scientific and methodological base for solving problems of ensuring information security in information resources, systems and technologies. In order to solve the tasks of achieving information security, along with formal methods of modeling processes and evaluating the effectiveness of system functioning, it is necessary to use methods of decomposition and structuring of components of systems and processes, informal methods of evaluating the effectiveness of functioning and decision-making.

The aim of the study is to substantiate an effective method of assessing the information protection level in a computer network against unauthorized access based on the security graph.

**3. Materials and Methods**

Among the well-known Ukrainian and foreign methods of quantitative assessment of the information protection level against unauthorized access, the approach based on information risk analysis, in particular, the Clements security system model, has become the most widespread. On the basis of risk analysis, such security assessment tools as:

– Microsoft Baseline Security Analyzer (MBSA);

– Central Computer and Telecommunications Agency (CCTA) Risk Analysis and Management Method (CRAMM);

– CounterMeasures;

– BCM-Analyser;

– "Vulture";

– "Risk Manager".

But they have certain drawbacks: the real structure (topology) of the computer network is not taken into account, losses from unauthorized access are estimated in a monetary unit, which may not always be appropriate, the variability of unauthorized access implementation scenarios and dynamic characteristics are not fully taken into account.

The information protection level in a computer network against unauthorized access is determined by the security of each protected resource, therefore, to assess the level of protection, it is advisable to use complex indicators that take into account both the processes of breaching the security of resources in the computer network, and the processes of control and restoration of their protected state [14].

In 2012, a group of Ukrainian scientists proposed their method of assessing the information protection level against unauthorized access in their paper "Method of assessing the information protection level against unauthorized access in computer networks based on the security graph". The method proposed by them for assessing the information protection level against unauthorized access in computer networks considered the system as a set of elements (subsystems). The method provided for the calculation of the security indicators of individual resources and the construction of security graphs by types of information security threats based on the design of computer networks. That is, this method took into account the structure of computer networks when assessing information security, but the problem of creating a comprehensive information protection level against unauthorized access was not solved.

In this study, this method of assessing the information protection level against unauthorized access in computer networks based on the security graph was improved. The proposed method consists of the following stages:

1) collection and analysis of raw data;

2) calculation of security indicators of individual resources;

3) construction of security graphs by types of information security threats based on the computer network project;

4) calculation of security indicators of all information in the computer network;

5) assessment of the information protection level against unauthorized access in the computer network according to the selected criterion;

6) development of recommendations for ensuring the necessary information protection level against unauthorized access in the computer network to officials responsible for information protection in the organization.

The initial data for assessing the information protection level against unauthorized access in a computer network are:

– list of protected resources and their location;

– composition and parameters of the functioning of resource protection means;

– intensity of violations of the security of information resources;

– intensity of restoration of resource security.

After the analysis of the raw data, the indicators of the protection of resources against three main types of threats – confidentiality, integrity and availability are calculated. The resource protection factor for each type of threat is calculated using the following expression:

$$\begin{cases} k_C = \dfrac{\mu_C}{\lambda_C + \mu_C}; \\ k_I = \dfrac{\mu_I}{\lambda_I + \mu_I}; \\ k_A = \dfrac{\mu_A}{\lambda_A + \mu_A}. \end{cases} \quad (1)$$

where $k_C$, $k_I$, $k_A$ – coefficients of protection of resources from threats of confidentiality, integrity and availability, respectively;

$\mu_C$, $\mu_I$, $\mu_A$ – intensity of restoration of security for confidentiality, integrity and availability of resources, respectively;

$\lambda_C$, $\lambda_I$, $\lambda_A$ – intensity of violations of confidentiality, integrity and availability of resources, respectively.

For brevity, expression (1) can be written in the form:

$$k_{C,I,A} = \frac{\mu_{C,I,A}}{\lambda_{C,I,A} + \mu_{C,I,A}}. \quad (2)$$

This method of calculating security indicators of all information in a computer network is focused on the use of security graphs by types of information security threats. When analyzing a computer network for security, the availability of alternative means of protection (AMP) should first of all be taken into account.

The following rules should be followed when constructing graphs:

– if the functioning of the computer network requires that the state of all resources be protected (the violation of the functioning of the computer network occurs when the security of at least one resource is violated) and at the same time, additional AMPs are not used to protect resources, and there are no alternatives from the point of view of security reserve resources, then in such a computer network, a consistent security graph is put in accordance;

– if AMP is used to protect the resource in addition to the main one, then in this case a parallel security graph will correspond, the number of elements in which corresponds to the total number of means of protection of this resource;

– if in the case of a resource security violation, there are options for solving the corresponding computer network problem using another alternative resource. In this case, a parallel security graph is matched.

In general, the security graph of a computer network can contain both serial and parallel connections. It is advisable to build security graphs separately for each of the main types of threats to information security – threats to confidentiality, integrity, and availability. Based on these graphs and calculated security indicators, the stage of calculating information security indicators in the computer network is carried out [15].

In the general case, it is assumed that security violations are independent events and are calculated using the multiplication theorem for independent events. For a serial connection, the following formula is used to calculate the security factors of the computer network:

$$K_{C,I,A} = \prod_{i=1}^{N_p} k_{C,I,A_i}, \tag{3}$$

where $K_{C,I,A}$ – computer network security coefficients;

$N_p$ – the number of protected resources;

$k_{\tilde{N},I,\hat{A}_i}$ – security coefficients of the *i*-th resource.

For parallel connection:

$$K_{C,I,A} = 1 - \prod_{i=1}^{N_p} \left(1 - k_{C,I,A_i}\right). \tag{4}$$

For a serial connection, provided that the computer network has unlimited resources to restore the security of resources:

$$K_{C,I,A} = \prod_{i=1}^{N_p} \left( \frac{\mu_{C,I,A}}{\lambda_{C,I,A} + \mu_{C,I,A}} \right). \tag{5}$$

For serial connection with limited security resources:

$$K_{C,I,A} = \frac{1}{\sum_{i=1}^{N_p} \frac{N_p!}{\left(N_p - 1\right)!} \cdot \left( \frac{\lambda_{C,I,A}}{\mu_{C,I,A}} \right)^i}. \tag{6}$$

When reserving and applying AMP for main and reserve resources, the security graph has a series-parallel structure [16], and the security coefficients of the computer network are determined by the following expression:

$$K_{C,I,A} = \prod_{i=1}^{N_p} \left( 1 - \prod_{j=0}^{N_r^i} \prod_{k=0}^{N_{AMP}^i} \left(1 - K_{C,I,A_{ijk}}\right) \right), \tag{7}$$

where $N_r$ – the number of reserve resources;

$N_{AMP}$ – the number of alternative means of protection;

$K_{C,I,A_{ijk}}$ – protection coefficients of the *i*-th resource in the *j*-th reserved group using the *k*-th means of protection.

For a series-parallel security graph with the constant use of the same amount of AMP in addition to the main assets, as well as with the same intensity of resource security violations and the intensity of resource security restoration, the formula looks like this:

$$K_{C,I,A} = \left( 1 - \left[ 1 - \frac{\mu_{C,I,A}}{\lambda_{C,I,A} + \mu_{C,I,A}} \right]^{N_{MP} + N_{AMP}} \right)^{N_p}, \tag{8}$$

where $N_{MP}$ – the number of means of protection.

After such calculations, an assessment of the information protection level in the computer network against unauthorized access is carried out according to the accepted criterion, after which deficiencies in the protection system are revealed. And finally, on the basis of the obtained results, recommendations are developed to improve protection to ensure the required information protection level.

**4. Results and Discussions**

To illustrate the practical effectiveness of the proposed method of assessing the information protection level against unauthorized access in computer networks based on the security graph, consider a specific example.

As an example, let's calculate the security level of a computer network with parameters: the number of automated workplaces is 50 (Users), which work under the control of the Microsoft Windows operating system. These workstations store computer network data intended for the user. All users are interconnected by a computer network, which has 4 servers based on the Microsoft Windows 2008 Server operating system, which ensure the functioning of general system and application software. Two of the four servers are in a failover cluster, and one is a single-time server.

When analyzing the output data: each User has one critically important resource for protection, two servers (Server-1, Server-2), united in a fault-tolerant cluster, ensure the functioning of the MS SQL Server 2008 database management system and mail server MS Exchange Server 2010, so it is possible to say that they have 2 resources that are protected. The third server (Server-3) provides the instant messaging system and the Web server, so it also has 2 protected resources. The fourth server (Server-4) is designed for the operation of the single-time system and, therefore, has one protected resource.

To protect against unauthorized access, the main means of protection (MP) and an additional means of protection are used. General represents personal passwords for entering the system for each user and administrator. Additional APM – authentication of users and administrators by identification card. Also, let's assume that the organization's information security officials are able to restore the confidentiality, integrity, and availability of any number of resources in 3 hours. From publicly available statistics on the detection of vulnerabilities in the Windows OS over the last year, it can be concluded that the approximate intensity of information privacy violations is 9.96 violations per month, the intensity of integrity violations is 9.75, and the intensity of information availability violations is 10.04. For the convenience of calculations, let's convert these data from months to hours:

$$\lambda_C = \frac{9.96}{720} = 0.0138 \text{ hour}^{-1};\ \lambda_I = \frac{9.75}{720} = 0.0135 \text{ hour}^{-1};\ \lambda_A = \frac{10.04}{720} = 0.0139 \text{ hour}^{-1}.$$

Next, using formula (1), let's find the coefficients of protection of resources from threats to confidentiality, integrity and availability, respectively:

$$k_C = \frac{3}{0.0138+3} \approx 0.99542;\ k_I = \frac{3}{0.0135+3} \approx 0.99552;\ k_A = \frac{3}{0.0139+3} \approx 0.99539.$$

The main volume of work related to the construction of security graphs by types of information security threats is recommended to be carried out at the stage of computer network design. The security graph is built based on the analysis of the computer network structure. The graphs of computer network security against threats to confidentiality, integrity, and availability of information are shown in **Fig. 1–3** respectively.

Based on the constructed graphs, using formulas (3), (4) and (8), it is possible to find the security factor of the computer network:

$$K_C = 0.845;\ \ K_I = 0.849;\ \ K_A = 0.997.$$

Security control of the information processed in the computer network should be based on the suitability criterion $K_{\tilde{N},I,\dot{A}} > 0.99$ [13].

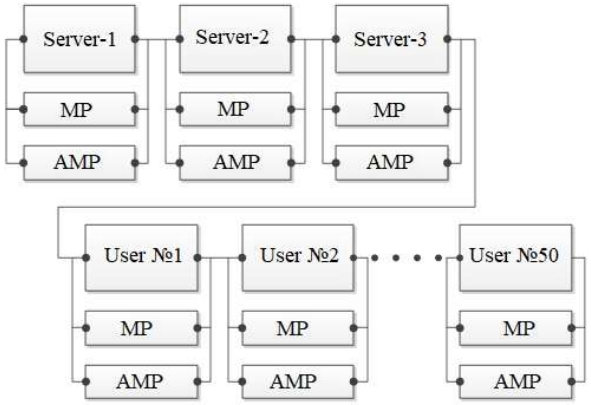


**Fig. 1.** Graph of computer network security against information privacy threats

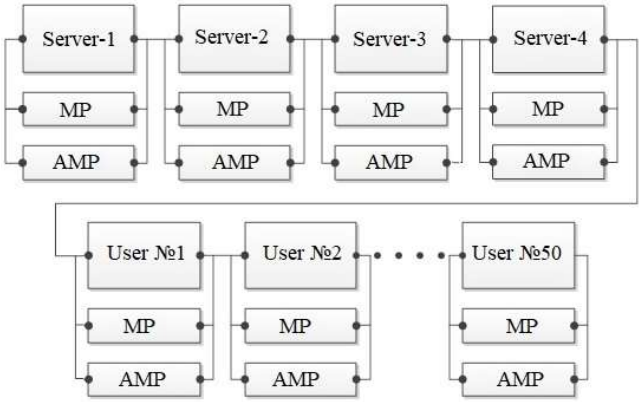


**Fig. 2.** Graph of organization's computer network security against threats to information integrity

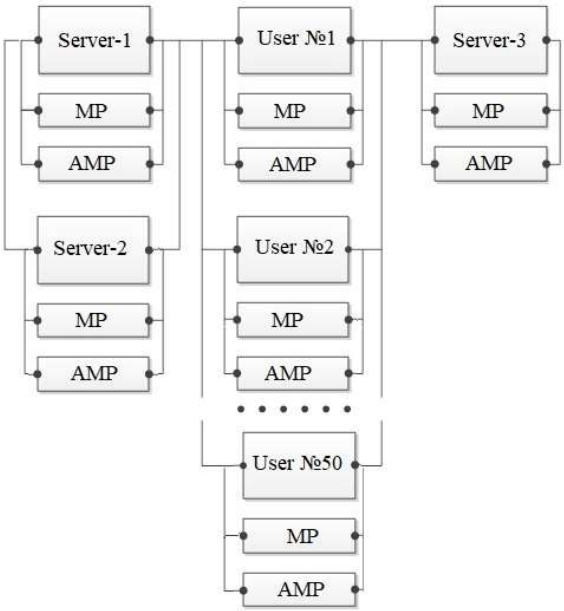


**Fig. 3.** Graph of organization's computer network security against threats to information availability

So, it is possible to in the considered computer network as a whole does not allow to provide an adequate level of protection. The required level is reached only for one type of information security threat, namely availability ($K_A = 0.997$). In order to achieve the required level, comprehensive measures must be taken. For example, improving the skills of workers responsible for protecting

the computer network to the level that will allow restoring the security of resources in 30 minutes, the security coefficients increase to the following values:

$$K_C = 0.995;\ \ K_I = 0.995;\ \ K_A = 0.999.$$

And when adding one more additional APM (for example, based on a fingerprint or a scanner of the three-dimensional shape of a person's face), all coefficients will be equal to approximately 0.999, while the criteria of information security against unauthorized access in a computer network will be met.

The described comprehensive approach to assessing the level of security of information resources has certain limitations. For each individual case of its application, the value of information, the status of the organization, the importance of information, the level of hardware and software must be taken into account. The prospect of further research is the development of the conceptual foundations of information security in the direction of the approach to assessing the information protection level against unauthorized access.

**5. Conclusions**

Today, the design and construction of computer networks is one of the most important tasks at the enterprise. But with the use of such networks, new problems related to information protection appear. To achieve a "secure" computer network, one of the main problems that need to be solved are the confidentiality, integrity and availability of information [17]. In fact, there are two approaches to solving the problem of computer network security: fragmented and complex. A fragmented approach is not appropriate because it is rather narrowly focused and cannot provide a guaranteed level of protection, unlike a comprehensive one. The complex approach is aimed at creating a secure environment for information processing in computer networks. It combines various measures of protection against threats into a single complex, which allows to guarantee a certain level of protection. Therefore, when assessing the information protection level in a computer network against unauthorized access, it is necessary to use complex assessment methods that consider computer networks as a single system, and not network fragments (separate subsystems, resources, devices).

The considered comprehensive approach to assessing the level of security of information resources can be applied at all stages of designing and maintaining computer networks of organizations in any field of activity. Applying the method of assessing the information protection level against unauthorized access in computer networks based on the security graph, the computer network is considered from the point of view of the possible vulnerability of its security measures, and the method is also adapted to the specific needs of the organization, taking into account the specifics of its operation and business. The accuracy of the result depends primarily on the completeness of the list of threats and damage as the main components of risk, the accuracy of the assessment of information resources, as well as the accuracy of the assessment of the probabilistic characteristics of threats.

The research results have been shown that the proposed method of assessing the information protection level against unauthorized access in computer networks based on the security graph allows for a more accurate description of information resources due to their characteristic vulnerabilities. Based on the calculations of the security indicators of individual resources and the security of all information in the computer network, the ranking of risks and, accordingly, information resources according to the degree of criticality for the organization's activities is carried out. Recommendations have been developed to ensure the necessary information protection level against unauthorized access in the computer network.

The advantages of the proposed method are simple implementation, widespread mathematical apparatus, accessibility for understanding. As a disadvantage, it can be noted that this method does not take into account the peculiarities of the functional interaction of protection means. Application of the considered method for evaluating the protection of information resources will reduce the costs of the organization and ensure the selection of the best means of protection.

**Conflict of interest**

The authors declare that there is no conflict of interest in relation to this paper, as well as the published research results, including the financial aspects of conducting the research, obtaining and using its results, as well as any non-financial personal relationships.

**Funding**

The study was performed without financial support.

**Data availability**

Data will be made available on reasonable request.

**Use of artificial intelligence**

The authors confirm that they did not use artificial intelligence technologies when creating the current work.

**Acknowledgements**

This article is prepared within the framework of a project EU Erasmus +: «European Experience of Information security and information protection systems under present large-scale cyber-attacks conditions», № 101127542 – EEISIPS – ERASMUS-JMO-2023-HEI-TCH-RSCH.

**References**

[1] Onyshchenko, S. V., Hlushko, A. D. (2022) Analytical dimension of cybersecurity of Ukraine in the conditions of growing challenges and threats.. Economics and Region, 1 (84), 13–20.

[2] Onyshchenko, S., Yanko, A., Hlushko, A., Maslii, O. (2023). Economic cybersecurity of business in Ukraine: strategic directions and implementation mechanism. Economic and cyber security. Kharkiv: PC TECHNOLOGY CENTER, 30–58. doi: https://doi.org/10.15587/978-617-7319-98-5.ch2

[3] Onyshchenko, S., Yanko, A., Hlushko, A., Maslii, O., Skryl, V. (2023). The Mechanism of Information Security of the National Economy in Cyberspace. Proceedings of the 4th International Conference on Building Innovations, 791–803. doi: https://doi.org/10.1007/978-3-031-17385-1_67

[4] Liu, J., Yan, J., Jiang, J., He, Y., Wang, X., Jiang, Z., Yang, P., Li, N. (2022). TriCTI: an actionable cyber threat intelligence discovery system via trigger-enhanced neural network. Cybersecurity, 5 (1). doi: https://doi.org/10.1186/s42400-022-00110-3

[5] Trusted Computer Systems Evaluation criteria (1985). US DoD 5200.28-STD. Available at: https://csrc.nist.gov/files/pubs/conference/1998/10/08/proceedings-of-the-21st-nissc-1998/final/docs/early-cs-papers/dod85.pdf

[6] Information Tecnhology Security Evaluation Criteria, v. 1.2 (1991). Office for Official publications of the European Communities. Available at: https://www.sogis.eu/documents/itsec/itsec-en.pdf

[7] Canadian Tusted Computer Product Evaluation Criteria, v. 3.0 (1993). Canadian System Security Centre, Communications Security Establishment, Government of Canada. Available at: https://buresund.se/books/canadian-trusted-computer-product-evaluation-criteria/

[8] Federal Criteria for Information Technology security (1993). NIST, NSA, US Government. Available at: https://nsrc.org/archives/netadmin/net_adm/security/alt-security

[9] ISO/IEC 15408-1:1999. Information technology. Security techniques. Evaluation criteria for IT security. Part 1: Introduction and general model.

[10] ISO/IEC 15408-2:1999. Information technology. Security techniques. Evaluation criteria for IT security. Part 2: Security functional requirements.

[11] ISO/IEC 15408-3:1999. Information technology. Security techniques. Evaluation criteria for IT security. Part 3: Security assurance requirements.

[12] CEM-97/017. Common Evaluation Methodology for Information Technology Security. Part 1: Introduction and general model.

[13] Yakymenko, I. Z. (2013). Evaluation criteria of networks protection level taking into account its architecture. nformatics and Mathematical Methods in Simulation, 3 (1), 82–90.

[14] Maltsev, G. D., Novikov, S. N. (2022). Criteria for the selection of evaluation indicators of the organization for the control of licensing requirements and conditions in terms of monitoring information security systems. Interexpo GEO-Siberia, 6, 157–165. doi: https://doi.org/10.33764/2618-981x-2022-6-157-165

[15] Khudyntsev, M., Lebid, O., Bychenok, M., Zhylin, A., Davydiuk, A. (2023). Network Monitoring Index in the Information Security Management System of Critical Information Infrastructure Objects. Lecture Notes in Networks and Systems. Springer, 270–290. doi: https://doi.org/10.1007/978-3-031-46880-3_17

[16] Yun, J. (2021). Influencing Factors and Preventive Strategies of University Computer Network Security. Cyber Security Intelligence and Analytics. Springer, 916–920. doi: https://doi.org/10.1007/978-3-030-69999-4_133

[17] Krasnobayev, V., Yanko, A., Hlushko, A. (2023). Information Security of the National Economy Based on an Effective Data Control Method. Journal of International Commerce, Economics and Policy, 14 (3). doi: https://doi.org/10.1142/s1793993323500217