КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (13), 2021
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2020.13.158169
UDC 004.056.5

Ihor S. Skiter
PhD in Physical and Mathematical Sciences, Associate Professor, Senior Researcher
National Academy of Science of Ukraine
The Institute for Safety Problems of Nuclear Power Plants, Chornobyl, Ukraine
ORCID ID 0000-0003-2334-2276
i.skiter@ispnpp.kiev.ua

Vorokhob Maksym
Graduate student of the Department of Information and Cyber Security
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID: 0000-0001-5160-7134
m.vorokhob.asp@kubg.edu.ua

CYBER SECURITY CULTURE LEVEL ASSESSMENT MODEL IN THE INFORMATION SYSTEM

Abstract. The paper sets the task of formalizing the processes of assessing the culture of cybersecurity of the information system of the organization. The basis is a comprehensive model that takes into account the technical and organizational parameters of the information system and the risks associated with them. The level of security culture of the information system is assessed on the basis of building an additive model. The model includes the characteristics of system state clusters. Clusters are formed on the basis of arrays of factors that correspond to different classes of information security culture. Classes are formed on the basis of sets of factors. Their impact is assessed using the severity of the consequences for the level of cybersecurity of the information system. In addition, the probability of manifestation of this factor in a particular information system is determined. The value of coefficients and probability distributions for each cluster and set of factors is estimated by expert methods and on the basis of a survey. A feature of the formation of arrays of factors is the inclusion in each cluster of a factor that reflects the passive behavior of the user to negative factors. Thus, the model introduces the probability of rejection of negative factors and the probability of ideal behavior for the formation of the appropriate class of threats. It is proposed to determine the average weights of the factors of the level of influence on the cybersecurity of the information system on the basis of the weighted average indicator. A method of estimating weights based on the equally probable distribution of negative factors within the cluster is proposed. The proposed technique does not depend on the number of factors in the cluster.

Keywords: cybersecurity of the information system; security state clusters; severity of consequences; the average weight of the cluster.

INTRODUCTION

In relation to the information system, its cybersecurity (CS) in the general sense can be defined as a state of security of the information space of the system, in which it is impossible to damage the properties of the object in relation to information and system`s infrastructure [1].

The level of security of the information system today is carried out mainly by risk-based analysis in accordance with ISO / IEC 27001 [2]. Cybersecurity of the information system, as a rule, is carried out according to the methods of assessment of organizational, technological and technical risks, aimed at assessing the threats and vulnerabilities of the system. This practically does not take into account the problems of analysis of a set of factors associated with human-machine interaction - the culture of cybersecurity (CSC) of the information system.

Problem statement. One of the urgent tasks that are solved by administrators of cybersecurity management systems is to assess the effectiveness of the implemented measures to ensure the basic functions of the information system. Thus information on results of the carried-out actions can have not only quantitative, but also qualitative character. Assessment of the culture of cybersecurity of information systems of enterprises, organizations, etc. is currently poorly formalized and conducted, mainly through risk assessments. It should also be noted that the main focus on cybersecurity of organizations and their information systems is paid separately to technical and organizational aspects. In addition, the analysis of research in the field of cybersecurity of information systems showed that there is a problem of formalizing the assessment of the level of CSC, assessment of its components, assessment of the dynamics of the overall level of CSC and its individual components and more.

Therefore, it is important to formalize the processes of CSC assessment based on the development of a comprehensive model taking into account the technical and organizational parameters of the information system and the risks associated with them.

Analysis of recent research and publications. In [3] the definition of the concept of cybersecurity in relation to the objects of critical infrastructure in nuclear energy is given. It covers the hardware and technological components of cybersecurity of the system, as well as a set of parameters that characterize the impact on the CSC of the human factor in the process of internal and external activities. The basis of the CSC analysis is based on the identification of individual components of system security risks and aggregate risk. At the same time the weights of separate components are not allocated, the estimation of action of administrative decisions on them, dynamics of the general indicator and its components is not carried out.

Information security culture models presented in [4] identified 16 CSC measurement tools. But the authors point out that there is no proven and generally accepted tool that could be used in different industries and organizations. Most of the considered tools use only the quantitative method; however, the security culture includes very different domains and therefore a mixed approach should be used.

An attempt to generalize approaches to determining the level of CSC is proposed in [5]. The paper proposes the development of standards for determining CSC factors, assessing their risks, etc. But did not propose a single model for estimating CSC based on them.

In [6] a fuzzy model of complex assessment of the level of information security culture of the organization was developed taking into account the peculiarities of human-machine interaction. The model makes it possible to assess the CSC only the current state of the system, based on models of fuzzy logic, in which sets of rules are formed subjectively, depending on the requests and needs of experts or decision makers.

Thus, there is a problem of creating a generalized mathematical model for determining the complex indicator of the CSC, taking into account arrays of factors / threats, assessing their contribution to the overall indicator and assessing the dynamics after the implementation of appropriate management decisions.

The purpose of the article, given the lack of research in this area is to build a model for evaluating the effectiveness of implemented measures to improve the culture of cybersecurity in the information system.

FORMALIZED CYBER SECURITY CULTURE ASSESSMENT MODEL

One of the urgent tasks facing administrators of management systems is to assess the state of security, its dynamics and the dynamics of its components, as well as the effectiveness of the

ISSN 2663 - 4023

implemented measures. In this case, information about the results of the assessment and changes in the state of cybersecurity of the system can be not only quantitative but also qualitative [7]. Consider an information system at some point in time $t \in [0, T]$. Suppose that at a given moment in time we observe *N* clusters of characteristics of the states of the security system $Q_1(t), Q_2(t), \dots, Q_N(t)$, where *N>2*.

Consider the idealized case of the state of the system. Namely, we will assume that these clusters do not intersect in pairs, are uncorrelated and make the same contribution to the overall assessment of cybersecurity of the information system. We will also assume that the *i*-th cluster contains m_i elements that can be observed according to the polynomial scheme of probability distribution $(p_{i1}(\tau), p_{i2}(\tau), \dots, p_{iM_i}(\tau))$ where $\tau \in [0, T]$. And $p_{i1}(\tau) + p_{i2}(\tau) + \cdots + p_{iM_i}(\tau) = 1$. It should also be noted that the probability distribution may change at discrete times τ. The change in the distribution of probabilities may occur due to the management of the enterprise organizational (including training) activities with the staff of the information system, which has access to critical resources (users, operators, service personnel, etc.).

There is a problem of quantitative assessment of the change (assessment of trend parameters) in the anthropogenic factor of the security system after the measures taken on the basis of clusters

We assume that the cluster of security characteristics is described by the identity:

$$Q_i(t) = \{\langle k_{ij}, p_{ij}(t)\rangle,\ j \in [1, M_i]\}, i \in [1, N] \quad (1)$$

where M_i –the number of elements in the set;

$p_{ij}(t)$ –the probability of manifestation of the factor *#j*, (for example, the factor *#j* may mean that a randomly selected employee always opens the application in an e-mail from an unknown sender);

k_{ij} - some coefficient proportional to the severity of the consequences for the cybersecurity of the system in the case of the manifestation of the factor *#j*. In this case, if the factor #j has more serious consequences for security than the factor #l, then we assume that there is a strict inequality $k_{ij} > k_{il}$.

For all clusters there is an expression:

$$k_{i1} + k_{i2} + \cdots . + k_{iM_i} = S, \forall\, i \in [1, N] \quad (2)$$

where *S*–integer, range of rating scale.

The function *W* of the average weight of the cluster in the general indicator of the level of threats to the information system can be defined as a linear additive function of the form:

$$W_i(t) = W\big(Q_i(t)\big) = \sum_{j=1}^{M_i} k_{ij} p_{ij}(t) \cdot M_i \quad (3)$$

or

$$W_i(t) = W\big(Q_i(t)\big) = \sqrt{\sum_{j=1}^{M_i} k_{ij} p_{ij}^2(t)} \cdot M_i \quad (4)$$

For the case of uniform distribution in the case of definition (3) we have

$$p_{i1} = p_{i2} = \cdots = p_{iM_i} = \frac{1}{M_i} \quad (5)$$

And then

$$W_i(t) = M_i \cdot \sum_{j=1}^{M_i} k_{ij} \frac{1}{M} = \sum_{j=1}^{M_i} k_{ij} = S \quad (6)$$

In the case of definition (4) we have

$$W_i(t) = M_i \cdot \left(\sum_{j=1}^{M_i} k_{ij} p_{ij}^2(t)\right)^{\frac{1}{2}} = M_i \cdot \frac{1}{M_i} \cdot \left(\sum k_{ij}\right)^{\frac{1}{2}} = \sqrt{S} \quad (7)$$

Thus, in both definitions at the points of maximum entropy [8] the values of the weight function do not depend on the different elements in the cluster.

RESULTS OF THE NUMERICAL EXPERIMENT

Approbation of the proposed theoretical model for assessing the level of cybersecurity was conducted as part of the audit of the information security management system at the Institute for Safety Problems of Nuclear Power Plants of the National Academy of Sciences of Ukraine (ISPNPP NASU) based on ISO / IEC 27001.

An integral part of the audit and analysis of the state of information security management was a survey of the culture of cybersecurity in the institution. In order to study the level of cyber security culture, a method of interviewing employees of the organization was used on the basis of questionnaires developed in the framework of NATO's project "Cyber Rapid Analysis for Defense Awareness of Real-time Situation (CyRADARS)" under grant G5286 [9]. More than 85% of the total number of ISPNPP employees took part in the survey. The sample is representative, according to [10] the sample size is defined by the expression:

$$n = \frac{Z^2 \cdot p \cdot q}{\Delta^2}, \quad (8)$$

where n - sample size;
Z - coefficient depending on the selected level of significance;
p - the share of respondents who have the studied factor;
q - the share of respondents who do not have the studied factor;
Δ - marginal sampling error.

A confidence level of 0.95 was set for the study, with the following parameter values selected: $Z = 1.96, p = q = 0.5, \Delta = 0.05$.

The initial survey found that 53.3% of respondents have access to information hosted in a closed corporate information system, 40% of employees do not have access to or work with the system, 6.7% of respondents have no idea about that the corporate information system is absent. Thus, more than half of the staff work with the information resources of the institution, including people who did not have special skills in cybersecurity.

The study provided an opportunity to develop a plan of measures aimed at, in particular, raising awareness of staff in the field of information security and cybersecurity, as well as creating conditions for improving the effectiveness of organizational and technical solutions to ensure the required level of overall security. After the implementation of the measures

ISSN 2663 - 4023

envisaged by the plan in order to determine the dynamics of the state of cybersecurity culture and its components, a re-audit of this institution was conducted.

To implement the proposed model, 4 clusters of characteristics of the security system were formed:

$Q_1(t)$ - factors of vulnerability to methods of social engineering;

$Q_2(t)$ -; the state of information security culture in professional activities;

$Q_3(t)$ - the level of organizational culture of information security;

$Q_4(t)$ - the level of personal information security culture.

In cluster $Q_1(t)$ $m_1 = 3$ factors of vulnerability to methods of social engineering are allocated; in ciuster $Q_2(t)$ $m_2 = 4$ factors of a condition of culture of information security in professional activity are allocated; in ciuster $Q_3(t)$ $m_3 = 5$ level of organizational culture of information security is allocated; in cluster $Q_4(t)$ $m_4 = 6$ elements for assessment of level of personal culture of information security are allocated. Characteristics of the elements of the clusters are given in table.1

Table 1

Characteristics of cluster elements for assessing the level of cybersecurity of the information system of the ISP NPP of the NAS of Ukraine

Cluster	Number of elements	Characteristics of elements (factors)
$Q_1(t)$	$m_1 = 3$	$X_{1,0}$ Cluster factors not taken into account and factors that do not affect CS $X_{1,1}$ Types of responses to emails from an unknown recipient $X_{1,2}$ Degree of trust in links in letters and messages $X_{1,3}$ Degree of trust in social networks
$Q_2(t)$	$m_2 = 4$	$X_{2,0}$ Cluster factors not taken into account and factors that do not affect CS $X_{2,1}$ Availability of knowledge in the field of CS $X_{2,2}$ Personal influence on the information security of the organization $X_{2,3}$ Possibilities of remote work $X_{2,4}$ Interaction with internal and external information environments
$Q_3(t)$	$m_3 = 5$	$X_{3,0}$ Cluster factors not taken into account and factors that do not affect CS $X_{3,1}$ Use of devices for work and own needs $X_{3,2}$ Formalization of CS culture in the organization $X_{3,3}$ Climate in the team $X_{3,4}$ Information support for safety in the workplace $X_{3,5}$ Using online banking
$Q_4(t)$	$m_4 = 6$	$X_{4,0}$ Cluster factors not taken into account and factors that do not affect CS $X_{4,1}$ Types of accounts in the OS $X_{4,2}$ Use of shared accounts and gadgets $X_{4,3}$ Activity in social networks $X_{4,4}$ OS and software updates $X_{4,5}$ System scan with antivirus tools $X_{4,6}$ Technology of creating and storing passwords

At the first stage of research for approbation of the proposed model by expert methods with the involvement of specialists of the information department of ISPNPP NASU, responsible executors of CyRADARS project and laboratory of cybersecurity research Institute of Mathematical Machines and Systems Problems of the NASU, were established probability distributions $p_{ij}(t_1)$ for each system of factors k_{ij} (table 2)

ISSN 2663 - 4023

Table 2

Parameters of clusters for the initial assessment of cluster weights in the cybersecurity indicator of the information system of the ISPNPP NPP of the NAS of Ukraine

Cluster	Number of elements	Probabilities of manifestation of factors for the initial state of the system (t_1)	Coefficients of severity of consequences of manifestation of factors
$Q_1(t)$	$m_1 = 3$	$p_{1,0} = 0{,}10$ $p_{1,1} = 0{,}40$ $p_{1,2} = 0{,}30$ $p_{1,3} = 0{,}20$	$k_{1,1} = 0{,}50$ $k_{1,2} = 0{,}30$ $k_{1,3} = 0{,}20$
$Q_2(t)$	$m_2 = 4$	$p_{2,0} = 0{,}10$ $p_{2,1} = 0{,}30$ $p_{2,2} = 0{,}20$ $p_{2,3} = 0{,}20$ $p_{2,4} = 0{,}20$	$k_{2,1} = 0{,}40$ $k_{2,2} = 0{,}30$ $k_{2,3} = 0{,}20$ $k_{2,4} = 0{,}10$
$Q_3(t)$	$m_3 = 5$	$p_{3,0} = 0{,}10$ $p_{3,1} = 0{,}20$ $p_{3,2} = 0{,}15$ $p_{3,3} = 0{,}20$ $p_{3,4} = 0{,}15$ $p_{3,5} = 0{,}20$	$k_{3,1} = 0{,}30$ $k_{3,2} = 0{,}20$ $k_{3,3} = 0{,}20$ $k_{3,4} = 0{,}20$ $k_{3,5} = 0{,}10$
$Q_4(t)$	$m_4 = 6$	$p_{4,0} = 0{,}10$ $p_{4,1} = 0{,}15$ $p_{4,2} = 0{,}20$ $p_{4,3} = 0{,}20$ $p_{4,4} = 0{,}15$ $p_{4,5} = 0{,}10$ $p_{4,6} = 0{,}10$	$k_{4,1} = 0{,}20$ $k_{4,2} = 0{,}20$ $k_{4,3} = 0{,}20$ $k_{4,4} = 0{,}20$ $k_{4,5} = 0{,}10$ $k_{4,6} = 0{,}10$

The matrix of coefficients of severity of the consequences of the manifestation of factors (8) is also determined on the basis of expert studies:

$$K = \|k_{ij}\| = \begin{Vmatrix} 0.50 & 0.30 & 0.20 & 0.00 & 0.00 & 0.00 \\ 0.40 & 0.30 & 0.20 & 0.10 & 0.00 & 0.00 \\ 0.30 & 0.20 & 0.20 & 0.20 & 0.10 & 0.00 \\ 0.20 & 0.20 & 0.20 & 0.20 & 0.10 & 0.10 \end{Vmatrix} \quad (8)$$

For the studied information system, within the proposed model for estimating the weights of clusters, we will consider the components of the matrix (constant for all studies at times t_1, t_2, t_3)

Based on (3) for the initial state of the system (for the moment of study t_1)) the average weights of the clusters are determined as they affect the overall risk for the information system:

$$\begin{cases} W_1(t_1) = 3 \cdot (0.50 \cdot 0.40 + 0.30 \cdot 0.30 + 0.20 \cdot 0.20) = 0.99 \\ W_2(t_1) = 4 \cdot (0.40 \cdot 0.30 + 0.30 \cdot 0.20 + 0.20 \cdot 0.20 + 0.10 \cdot 0.20) = 0.96 \\ W_3(t_1) = 5 \cdot (0.30 \cdot 0.20 + 0.20 \cdot 0.15 + 0.20 \cdot 0.20 + 0.20 \cdot 0.15 + 0{,}20 \cdot 0{,}20) = 1{,}00 \\ W_4(t_1) = 6 \cdot (0.20 \cdot 0.15 + 0.20 \cdot 0.20 + 0.20 \cdot 0.20 + 0.20 \cdot 0.15 + 0{,}10 \cdot 0{,}10 + 0{,}10 \cdot 0{,}10) = 0{,}96 \end{cases}$$

The results obtained by (4) are somewhat larger, but similarly reflect the state of the cybersecurity culture of the information system in the respective clusters.

ISSN 2663 - 4023

$$\begin{cases} W_1(t_1) = 3 \cdot \sqrt{(0.50 \cdot 0.40^2 + 0.30 \cdot 0.30^2 + 0.20 \cdot 0.20^2)} = 1{,}02 \\ W_2(t_1) = 4 \cdot \sqrt{(0.40 \cdot 0.30^2 + 0.30 \cdot 0.20^2 + 0.20 \cdot 0.20^2 + 0.10 \cdot 0.20^2)} = 0{,}98 \\ W_3(t_1) = 5 \cdot \sqrt{(0.30 \cdot 0.20^2 + 0.20 \cdot 0.15^2 + 0.20 \cdot 0.20^2 + 0.20 \cdot 0.15^2 + 0{,}20 \cdot 0{,}20^2)} = 0{,}91 \\ W_4(t_1) = 6 \cdot \sqrt{(0.20 \cdot 0.15^2 + 0.20 \cdot 0.20^2 + 0.20 \cdot 0.20^2 + 0.20 \cdot 0.15^2 + 0{,}10 \cdot 0{,}10^2 + 0{,}10 \cdot 0{,}10^2)} = 0{,}99 \end{cases}$$

It should be noted that the working formulas do not include probabilistic characteristics of unaccounted for cluster factors and factors that do not affect the CS.

Re-assessment of the state of cybersecurity of the information system of the NPP NPP was carried out after the implementation of organizational and technical measures related to the results of primary research [11], in periods 13.07.2021 to 15.07.2021 pp. (t_2) and 14.09.2021p to 16.09.2021p. (t_3).

The results of estimates of cluster weights in the General indicator are given in table 3.

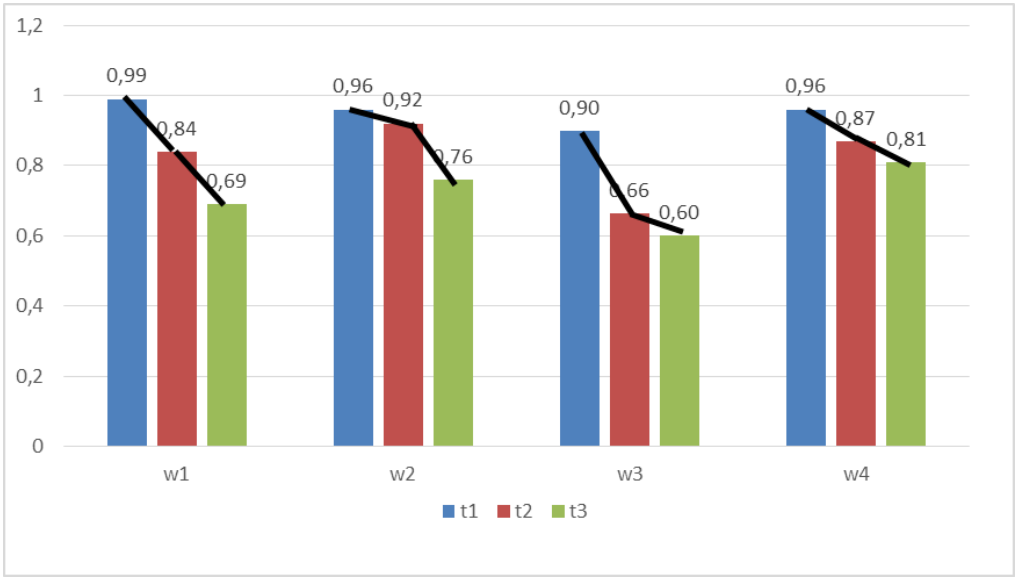
Table 3

Cluster parameters for re-estimating cluster weights in the information system cybersecurity indicator of the ISPNPP NPP of the NAS of Ukraine

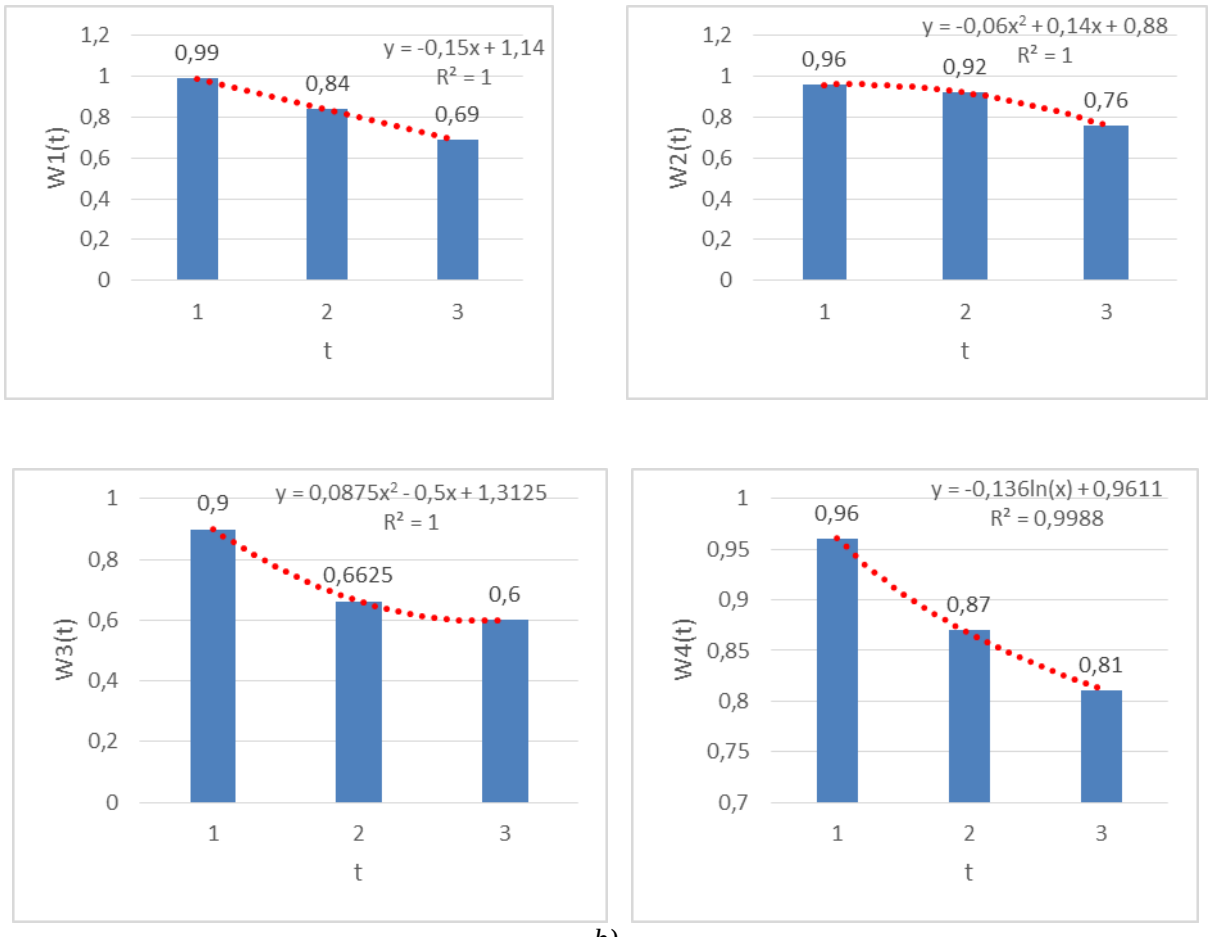
Cluster	Number of elements	Probabilities of manifestation of factors		The average weights of clusters in the overall hazard for the information system for (3) / for (4)	
		(t_2)	(t_3)	$W_i(t_2)$	$W_i(t_3)$
$Q_1(t)$	$m_1 = 3$	$p_{1,0} = 0{,}20$ $p_{1,1} = 0{,}30$ $p_{1,2} = 0{,}30$ $p_{1,3} = 0{,}20$	$p_{1,0} = 0{,}40$ $p_{1,1} = 0{,}30$ $p_{1,2} = 0{,}20$ $p_{1,3} = 0{,}10$	0,84/0,85	0,69/0,73
$Q_2(t)$	$m_2 = 4$	$p_{2,0} = 0{,}20$ $p_{2,1} = 0{,}30$ $p_{2,2} = 0{,}20$ $p_{2,3} = 0{,}20$ $p_{2,4} = 0{,}10$	$p_{2,0} = 0{,}30$ $p_{2,1} = 0{,}20$ $p_{2,2} = 0{,}20$ $p_{2,3} = 0{,}20$ $p_{2,4} = 0{,}10$	0,92/0,95	0,76/0,77
$Q_3(t)$	$m_3 = 5$	$p_{3,0} = 0{,}15$ $p_{3,1} = 0{,}20$ $p_{3,2} = 0{,}10$ $p_{3,3} = 0{,}20$ $p_{3,4} = 0{,}15$ $p_{3,5} = 0{,}20$	$p_{3,0} = 0{,}10$ $p_{3,1} = 0{,}20$ $p_{3,2} = 0{,}15$ $p_{3,3} = 0{,}20$ $p_{3,4} = 0{,}15$ $p_{3,5} = 0{,}20$	0,66/0,87	0,60/0,86
$Q_4(t)$	$m_4 = 6$	$p_{4,0} = 0{,}15$ $p_{4,1} = 0{,}15$ $p_{4,2} = 0{,}20$ $p_{4,3} = 0{,}15$ $p_{4,4} = 0{,}10$ $p_{4,5} = 0{,}15$ $p_{4,6} = 0{,}10$	$p_{4,0} = 0{,}20$ $p_{4,1} = 0{,}15$ $p_{4,2} = 0{,}15$ $p_{4,3} = 0{,}10$ $p_{4,4} = 0{,}15$ $p_{4,5} = 0{,}10$ $p_{4,6} = 0{,}15$	0,87/0,89	0,81/0,82

Figure 1 shows the dynamics of estimating the state of the system based on the analysis of the average weights of the clusters $W_i(t_i)$ in different periods of research (Fig.1a) and dynamics of weights after organizational measures (Fig. 1b).

ISSN 2663 - 4023



a)



b)

Fig. 1. Average values of cluster weights

a) weights of the clusters $W_i(t_i)$ in different periods of research
b) dynamics of weights $W_i(t_i)$ after organizational measures

As can be seen from Fig. 1, the model of estimation of cluster weights in the general structure of cybersecurity of information system depends on estimations of probabilities of occurrence of factors. In turn, such assessments should be based on an analysis of both the factors themselves and their structure. In fig. 1b shows the parameters of trends in changes in the weights of clusters as a result of changes in the probabilities of their components. That is - the results of organizational and technical activities.

Analysis of the factors that affect the overall level of weight of the cluster will allow on the basis of factor models $W_i\,(t_i) = f(X_i(t_i))$ to assess the impact of individual factors and their components. Construction of factor models of dynamics will allow to estimate force and a direction of influence of factors on the general level of weights. And this, in turn, will allow to form a set of the most effective management decisions to increase the level of cybersecurity of the object.

CONCLUSIONS AND PROSPECTS OF FURTHER RESEARCH

Thus, based on the proposed model for assessing the components of cybersecurity on the example of the information system of the ISP NPP NASU, an assessment of the impact of factors on the overall state of information security. The evaluation showed the effectiveness of the proposed model and the formation of organizational, technical and managerial decisions based on it.

It can be seen that the organizational measures have a positive impact on the overall state of information security, which can be seen in the reduction of threats by clusters compared to the initial state of information system assessment.

Areas of further research will focus on building assessment models within the clusters of significance of individual factors and study their structure [12] in order to form the most effective solutions that will improve the information security of the information system.

In addition, an important area of research is to assess both the individual values of the minimum acceptable levels of cluster weights and their ratio in the overall structure of the cybersecurity indicator.

ACKNOWLEDGMENTS

The author expresses gratitude to the responsible executors of the NATO project «Cyber Rapid Analysis for Defense Awareness of Real-Time Situation- CyRADARS» prof. Dorosh M.S., Ass.Prof. Trunova O.V., Ph.D. Wojciechowska M.M., Head of the Cyber Security Research Laboratory of the Institute of Problems of Mathematical Machines and Systems of the National Academy of Sciences of Ukraine, Doctor of Science Gulak G.M. for the provided research materials and expert assessments of the model parameters; management of the NPP NPP of the NAS of Ukraine for the opportunity to conduct research.

The work was performed within the framework of NATO's Science for Peace program, the Cyber Rapid Analysis for Defense Awareness of Real-Time Situation-CyRADARS project (grant agreement G5286).

REFERENCES

1 Про національну безпеку України, Закон України № 2469-VIII (2018, 1 липня) (Украина). *Відомості Верховної Ради України.*, *31*.

2 ДП «УкрНДНЦ». (2014). *Інформаційні технології. Методи безпеки. Системи менеджменту інформаційною безпекою. Вимоги* (ДСТУ ISO/IEC 27001:2013). Технічний комітет стандартизації «Інформаційні технології».

3 Baylon, C., Brunt, R., & Livingstone, D. (2015). *Cyber Security at Civil Nuclear Facilities Understanding the Risks* (Charity Registration No. 208223). The Royal Institute of International Affairs.

4 Sas, M., Hardyns, W., van Nunen, K., Reniers, G., & Ponnet, K. (2021). Measuring the security culture in organizations: a systematic overview of existing tools. *Security Journal*, (34), 340–357.

5 Seeba, M., Matulevi˘cius, R., & Toom, I. (2021). Development of the Information Security Management System Standard for Public Sector Organisationsin Estonia. У *24th International Conference on Business Information Systems (BIS2021)* (с. 355–366). Technische Informationsbibliothek.

6 Войцеховська, М. М. (2020). *Інформаційна технологія оцінювання рівня культури інформаційної безпеки організації* [Неопубл. дис. д-ра філософії в галузі техн. наук]. Національний університет «Чернігівська політехніка».

7 Solic, K., Ocevcic, H., & Golub, M. (2015). The information systems' security level assessment model based on an ontology and evidential reasoning approach. *Computers & Security*, *55*, 25–39.

8 Han, Q., & Yang, D. (2018). Hierarchical Information Entropy System Model for TWfMS. *Entropy*, *20*(10), 1–20.

9 *Cyber Rapid Analysis for Defense Awareness of Real-Time Situation*. https://www.cyradars.net/.

10 Cochran, W. G. (1977). *Sampling Techniques* (3-тє вид.). John Wiley & Sons, Inc. (Оригінал опубліковано 1953 р.)

11 Shkarlet, S., Dorosh, M., Druzhynin, O., Voitsekhovska, M., & Bohdan, I. (2021). Modeling of Information Security Management System in the Project. *Advances in Intelligent Systems and Computing*, *1265*, 364–376.

12 Скітер, І., & Вторнікова, Є. (2018). Розробка алгоритму вибору матричного матеріалу для іммобілізації трансуранових елементів на основі модифікованого методу аналізу ієрархій. *Ядерна та радіаційна безпека*, *2*(78), 36–42.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (13), 2021
ISSN 2663 - 4023

Ігор Семенович Скітер
Кандидат фізико-математичних наук, доцент,
старший науковий співробітник, Національна академія наук України,
Інститут проблем безпеки атомних електростанціs, м. Чорнобиль, Україна
ORCID ID 0000-0003-2334-2276
i.skiter@ispnpp.kiev.ua

Ворохоб Максим Віталійович
аспірант кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0001-5160-7134
m.vorokhob.asp@kubg.edu.ua

МОДЕЛЬ ОЦІНКИ РІВНЯ КУЛЬТУРИ КІБЕРБЕЗПЕКИ В ІНФОРМАЦІЙНІЙ СИСТЕМІ

Анотація. В роботі поставлена задача формалізації процесів оцінки культури кібербезпеки інформаційної системи організації на основі розроблення комплексної моделі з врахуванням технічних та організаційних параметрів інформаційної системи та ризиків, пов'язаних з ними. Проводиться оцінка рівня культури безпеки інформаційної системи на основі побудови адитивної моделі, яка включає в себе характеристики кластерів станів системи. Кластери формуються на основі масивів факторів, які відповідають різним класам культури інформаційної безпеки. Їх вплив оцінюється за допомогою коефіцієнтів тяжкості наслідків для рівня кібербезпеки інформаційної системи. Крім того визначається ймовірність прояву даного фактору в конкретній інформаційній системі. Величина коефіцієнтів та ймовірнісних розподілів для кожного кластеру та набору факторів оцінюється експертними методами та на основі проведеного анкетування. Особливістю формування масивів факторів є включення до кожного кластеру фактору, який відображає пасивну поведінку користувача до негативних факторів. Таким чином у моделі вводиться ймовірність несприйняття негативних факторів та ймовірність ідеальної поведінки щодо формування відповідного класу загроз. Визначення усереднених ваг факторів рівня впливу на кібербезпеку інформаційної системи запропоновано проводити на основі середнього зваженого показника. Запропонована методика оцінки ваг на основі рівноймовірного розподілу негативних факторів в межах кластеру. Запропонована методика не залежить від кількості факторів у кластері.

Ключові слова Keywords: кібербезпека інформаційної системи; кластери станів безпеки; коефіцієнт тяжкості наслідків; усереднена вага кластеру.

REFERENCES

1 *Pro Nacionalnu bezpeku Ukrayiny. Zakon Ukraiyiny #2469-V111 (2018, 1 lypnua) (Ukrayina)* [On National Security of Ukraine, Law of Ukraine № 2469-VIII (2018, July 1) (Ukraine)]. *Відомості Верховної Ради України - Information of the Verkhovna Rada of Ukraine*, *31*. [In Ukraine]

2 Technical Committee for Standardization "Information Technology" (TC 20). (2014). Informatsiini tekhnolohii. Metody bezpeky. Systemy menedzhmentu informatsiinoiu bezpekoiu. Vymohy [Information Technology. Security methods. Information security of the management systems. Requirements] (DSTU ISO/IEC 27001:2013). DP «UkrNDNTs». [In Ukraine]

3 Baylon, C., Brunt, R., & Livingstone, D. (2015). *Cyber Security at Civil Nuclear Facilities Understanding the Risks* (Charity Registration No. 208223). The Royal Institute of International Affairs.

4 Sas, M., Hardyns, W., van Nunen, K., Reniers, G., & Ponnet, K. (2021). Measuring the security culture in organizations: a systematic overview of existing tools. *Security Journal*, (34), 340–357.

5 Seeba, M., Matulevi˘cius, R., & Toom, I. (2021). Development of the Information Security Management System Standard for Public Sector Organisationsin Estonia. У *24th International Conference on Business Information Systems (BIS2021)* (с. 355–366). Technische Informationsbibliothek.

6 Voitsekhovska, M. M. (2020). *Informatsiyna tehnologiya otsinuvannya rivnya kultury informatsiynoi bezeky organizaciy* [Information technology for assessing the level of information security culture of the organization] [Unpublished dis. Dr. of Philosophy in Tech. Science]. *Natsionalniy Universitet «Chernihivska Politechnika» - National University "Chernihiv Polytechnics"*.[In Ukraine]

7 Solic, K., Ocevcic, H., & Golub, M. (2015). The information systems' security level assessment model based on an ontology and evidential reasoning approach. *Computers & Security*, *55*, 25–39.

8 Han, Q., & Yang, D. (2018). Hierarchical Information Entropy System Model for TWfMS. *Entropy*, *20*(10), 1–20.

9 *Cyber Rapid Analysis for Defense Awareness of Real-Time Situation*. https://www.cyradars.net/.

10 Cochran, W. G. (1977). *Sampling Techniques* (3-d ed.). John Wiley & Sons, Inc. (The original has been published 1953 p.)

11 Shkarlet, S., Dorosh, M., Druzhynin, O., Voitsekhovska, M., & Bohdan, I. (2021). Modeling of Information Security Management System in the Project. *Advances in Intelligent Systems and Computing*, *1265*, 364–376.

12 Skiter, I. & Vtornikova, E. (2018). *Rozrobka algoritmu viboru matrichnogo materialu dlya immobilizacii transuranovih elementiv na osnovi modifikovanogo metodu analizu iyerarhiy*.[Development of an algorithm for selecting a matrix material for immobilization of transuranic elements based on a modified method of analysis of hierarchies] *Yaderna ta radiatsiyna bezpeka - Nuclear and radiation safety*, *2*(78), 36–42. [In Ukraine]