www.czasopisma.pan.pl PAN www.journals.pan.pl

jet INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2022, VOL. 68, NO. 3, PP. 549-555
Manuscript received December 17, 2021; revised August, 2022. DOI: 10.24425/ijet.2022.141273

Automation of Information Security Risk Assessment

Berik Akhmetov, Valerii Lakhno, Vitalyi Chubaievskyi, Serhii Kaminskyi, Saltanat Adilzhanova, and Moldir Ydyryshbayeva

***Abstract*—An information security audit method (ISA) for a distributed computer network (DCN) of an informatization object (OBI) has been developed. Proposed method is based on the ISA procedures automation by using Bayesian networks (BN) and artificial neural networks (ANN) to assess the risks. It was shown that such a combination of BN and ANN makes it possible to quickly determine the actual risks for OBI information security (IS). At the same time, data from sensors of various hardware and software information security means (ISM) in the OBI DCS segments are used as the initial information. It was shown that the automation of ISA procedures based on the use of BN and ANN allows the DCN IS administrator to respond dynamically to threats in a real time manner, to promptly select effective countermeasures to protect the DCS.**

***Keywords*—information security; audit; Bayesian network; artificial neural networks**

I. Introduction

With the growth of cyber-attacks rate, increase in attack scenarios complexity, the problem of reliable information security (IS) for many objects of informatization (OBI) has become more relevant than ever.

Note that in comparison to the 80s-90s of the last century the loudest cyber-attacks were associated with the selfish motives of the attackers, and the question in many cases concerned the theft of funds from bank cards or industrial espionage by hacking the information systems of competitors, then at the beginning of the 20th century, the situation changed dramatically.

Without going into a detailed analysis of well-known and technically difficult to implement cyberattacks, for example, Stuxnet [1] or "Moonlight Labyrinth" [2], etc., it was noted that nowadays the selfish motives of the attackers are fading into the background. In the context of the global information confrontation between the leading world states, globalization and fierce competition, the issues of providing information security for OBI of any scale have become a priority task for many companies. Nowadays, leading companies build their business processes based on the widespread use of information technology (IT) and information systems. They take into account the existing landscape of cyber threats.

The problem of providing IS OBI of any scale is complex. Such an integrated approach includes a fairly large list of necessary measures aimed at ensuring IS OBI. For example, it includes activities aimed at:

1) *search for the optimal strategy for investing into information security means (ISM);*
2) *formation of the optimal composition of the information security system along the contours of the information security OBI;*
3) *risk assessment for OBI information assets;*
4) *etc.*

Many researchers [3, 4] include the organization of an effective IS audit (hereinafter ISA) for OBI in this list of activities. However, if the issues of technical security of information security OBI are currently well studied and many new approaches for ensuring information security are based on innovative technologies, then the processes of conducting ISA remain a new area for researchers. Indeed, modern technologies have brought to the field of information security approaches based on cognitive technologies [5, 6], neural networks [7, 8], evolutionary algorithms [9, 10], etc. At the same time, most research in the field of organization and conduction of ISA focuses primarily on the organizational side of the issue. At the same time, not enough attention, in our opinion, is paid precisely to the problems of developing new methods and models of ISA based on new technologies, for example, on the use of artificial neural networks (ANN) in ISA procedures.

All of the above has determined the relevance of research aimed at studying the prospects of using the ANN apparatus in ISA procedures. First of all, this concerns the ISA of distributed computing networks (DCN) OBI, which today have become the basis of many business processes of companies and organizations.

II. Literature Review

In works [11, 12] it was shown that the organization of an effective information security management system (ISMS) OBI should be focused on the priority of the problem of information security risk management.

In works [12-14] it was shown that the internal audit function (IAF) can play an important role in ensuring IS OBI. ISA procedures allow owners of information assets (IA) to better understand how they can improve the information security of their enterprise, company or organization. However, these works do not touch upon the practical aspects of the use of

The work was carried out within the framework of the grant study AP08855887-OT-20 "Development of an intelligent decision support system in the process of investing in cyber security systems."

Berik Akhmetov is with Yessenov University, Aktau, Kazakhstan (e-mail: berik.akhmetov@yu.edu.kz)

Valerii Lakhno is with National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine (e-mail: lva964@nubip.edu.ua)

Vitaliy Chubaievskyi and Serhii Kaminskyi are with Kyiv National University of Trade and Economics, Kyiv, Ukraine (e-mail: {chubaievsyi_vi, s.kaminskyj} @knute.edu.ua)

Saltanat Adilzhanova and Moldir Ydyryshbayeva are with Al-Farabi Kazakh National University, Almaty, Kazakhstan (e-mail: asaltanat81@gmail.com, moldir__ydyryshbaieva@mail.ru)

intelligent technologies in the issues of ISA OBI. In works [15, 16], the authors noted that for ISA OBI, as a rule, a unique data set is used, which has been studied by experts. After that, experts develop recommendations that can affect the effectiveness of IS organization at OBI. However, the authors do not make unequivocal conclusions about the advisability of using IT in ISA procedures. Works [17, 18] focus on the principles and objectives of ISA enterprises. However, in these works, the question of the potential of using new IT to increase the efficiency of ISA remains unclear.

In works [19, 20], a model for assessing the risks of violation of the IS policy (hereinafter PIS) OBI, based on the use of fuzzy cognitive maps, is proposed. However, this approach, although it makes it possible to take into account many IS threats, remains difficult to be algorithmic. This shifts all the main work to the expert, and, therefore, increases the likelihood of a subjective assessment of the results of ISA OBI.

In [21–23], practical aspects of the implementation of ISA based on ANN are considered. The issues of training the ANN and its testing in the course of the ISA of a specific OBI are also considered. However, many questions have not been disclosed in the work. For example, the work lacks a statistical assessment of the ANN learning outcomes. There is also no generalization of the ability developed by the ANN for the ISA tasks of different OBIs.

The possibility of automating ISA procedures by using various kinds of decision support systems (DSS) and other IT is considered in the works [24–26]. However, the authors noted that these studies have not yet been completed and it is still premature to talk about full-scale automation of the OBI ISA.

As shown in [23, 29, 30], an integral part of ISA procedures is the analysis and assessment of IS risks for OBI. Also, an IS risk assessment should be performed at the design stage of IS for OBI. To solve this problem, the authors of [29, 31] used the apparatus of fuzzy logic (FL) and ANN. However, the authors failed to provide convincing arguments for how the posteriori probabilities are estimated during the implementation of IS threats for OBI in a dynamic confrontation with the attacking side.

All of the above has determined the relevance of new research aimed at developing new models and developing the methodology for conducting ISA OBI. The research focuses on using the potential of ANNs and Bayesian networks (BNs) when conducting ISA.

III. The Purpose and Objectives of the Study.

The aim of the study is to increase the degree of reliability of the results obtained in the course of ISA by using ANN and BN in these procedures.

Research objectives:

1) build and train ANN to automate the ISA procedure and obtain the values of the risks of IS violation OBI.

2) test the developed ANN as an element of an intelligent system for automating ISA OBI procedures.

IV. Methods and Models

The dynamically changing landscape of cyber threats for OBI, especially critical computer systems (CCS), forces the defense side to actively develop models and methods of continuous ISA. In conditions of dynamic confrontation with the attacking side, one of the priority tasks of the ISA is the task associated with the analysis and forecasting of risks.

In works [21, 23, 27-30], devoted to the prospects of using ANN for the tasks of auditing information security risks, the emphasis is on the situation when auditors have sufficiently large data samples. Note that in the framework of our study, we do not touch upon the discussion of the general limitations of the ANN as a tool for auditing and assessing the risks of information security OBI. This analysis has been performed by many authors in the past.

In accordance with [32, 33], the size of the IS risk for OBI can be determined as follows:

$$R = f(A,T,V), \tag{1}$$

where A,T,V – parameters, respectively, characterize the value of the information asset (IA), the likelihood of threats and the likelihood of vulnerabilities.

As a rule, in the course of ISA, the values of the IS breach risks for OBI as a whole are calculated - R_{FR}.

To do this, you can use the following dependency:

$$R_{FR} = \sum_{n=1}^{N} R_{FR_{cu}}, \tag{2}$$

where N – the number of DCN segments, see Fig.1;

$R_{FR_{cu}}$ – IS level for a separate DCN segment.

The value can be determined using the following dependency:

$$R_{FR_{cu}} = \sum_{st=1}^{ST} P_{\Sigma}^{T} \cdot \left(\frac{IAV_{ST}}{IAV_{\Sigma}} \right), \tag{3}$$

where ST – is the number of IS threat sources for the OBI DCN segment;

P_{Σ}^{T} – the resulting value of the probability of the implementation of threats for the IS of the DCN segment;

IAV_{ST}, IAV_{Σ} – accordingly, the cost of the IA segment and OBI (DCN) as a whole.

The value P_{Σ}^{T} can be found like this:

$$P_{\Sigma}^{T} = 1 - \prod_{st} \left(1 - P_{ST}^{T}\right), \tag{3}$$

where P_{ST}^{T} – is the value of the probability of realizing a threat to IS within a specific DCN segment. These values are determined, for example, based on building a threat model for certain types of threats and classes of attacks.

When carrying out ISA, and, accordingly, risk analysis, an expert evaluates a priori probabilistic information about the possibility of a threat being realized. However, as new information is studied, the results obtained in the course of the ISA can both confirm and refute the a priori information.

In the proposed solution for assessing information security risks, it is proposed to use Bayesian trust networks (BN) at the first stage [34, 36-38].

For example, for the BN shown in Fig. 2, a priori conditional probabilities of occurrence of certain events were given. After that, the BS was trained on the basis of statistical data [35].

Data were taken based on information on the US National Vulnerability Database website.

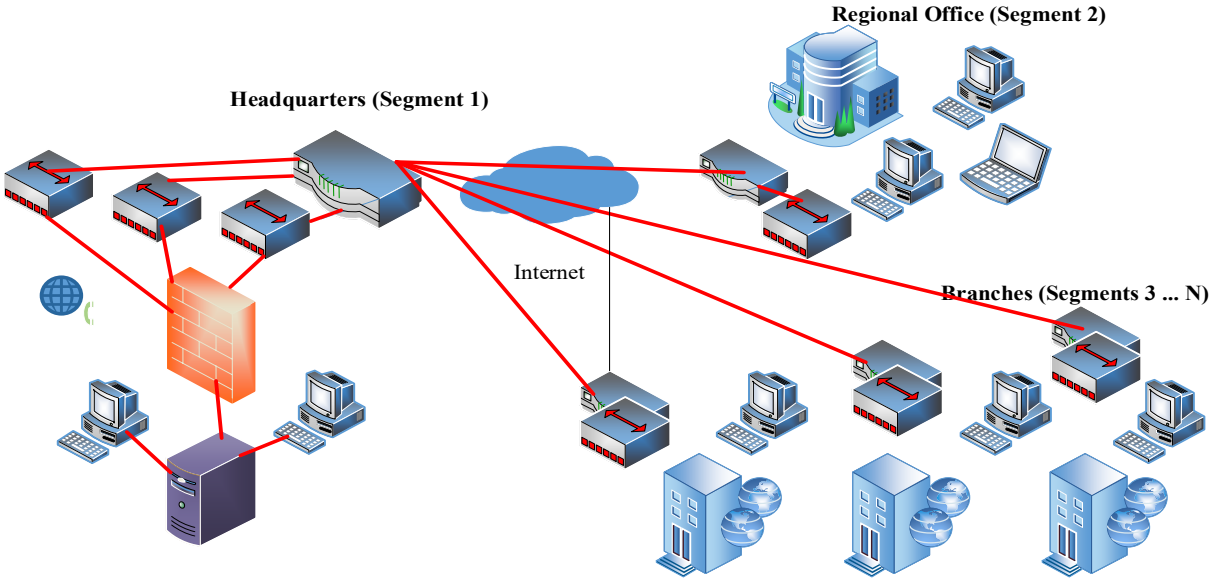

Fig. 1. DCN architecture for OBI (as an ISA object)

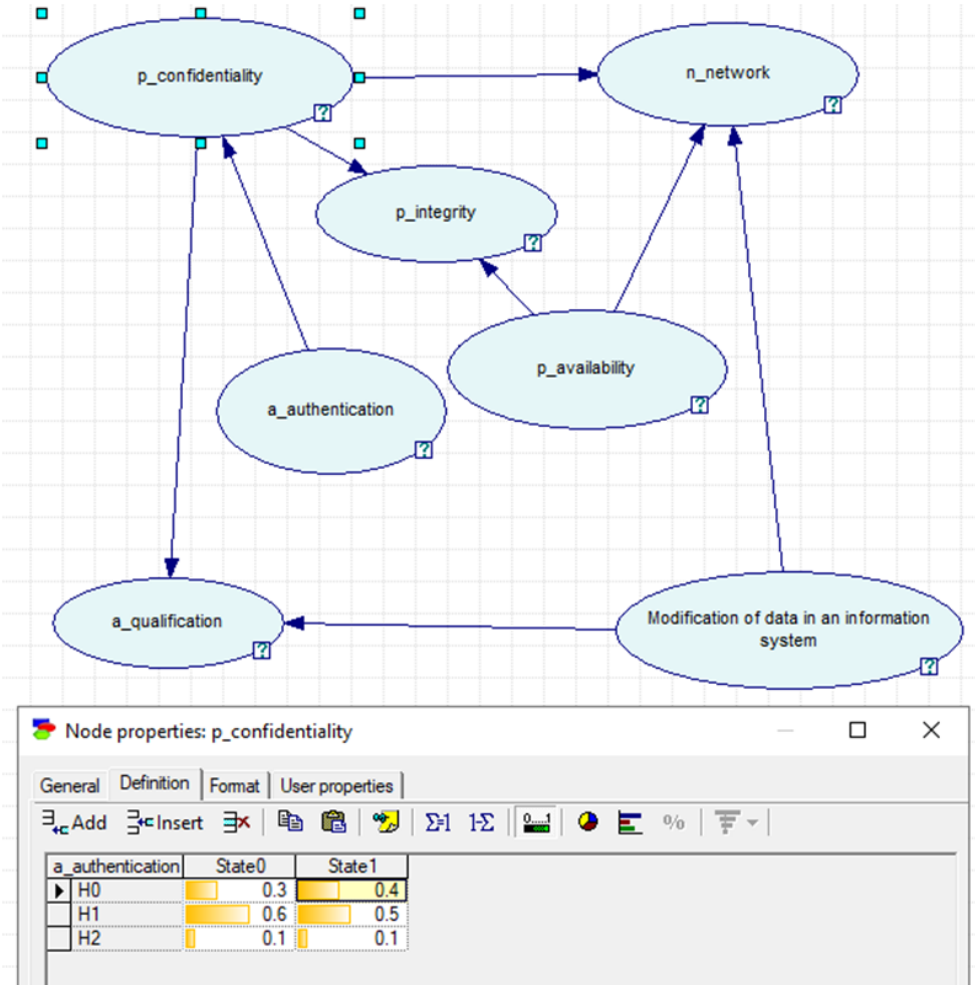

Fig. 2. Bayesian search and visualization of simulation results in the Genie package (v2.0)

In such a BN, the target variables are potential threats to which the OBI DCN may be vulnerable. All the variables are shown in Fig. 2, discrete. Each variable (or threat) can take one of five values, each of which corresponds to the probability of its realization: trivial, low, medium, high, critical (respectively, insignificant, low, medium, high, critical). The rest of the variables in the BN are characteristics. A set of these characteristics makes it possible to identify a threat and determine its likelihood. These variables are divided into categories that classify information security threats or describe different types of computer intruders. For example, consider a BN for the threat of unauthorized access (UAA) to information resources in the DCN OBI: 1) The purpose of the UAA. Violation of confidentiality (p_confidentiality), integrity (p_integrity), or availability (p_availability) of information resources of the DCN OBI is considered; 2) Position of the tamper source (n_network). Three source categories were accepted: intra-segment, intersegment, external; 3) the need for authentication to implement the threat (a_ authentication); 4) Attacker's qualification (a_qualification): high, medium, low.

Table 1 shows an example of a piece of data for describing the conditional probabilities for the threat "Data modification in the information system" OBI.

Similar tables of conditional probabilities were constructed in the course of the study for other classes of information security threats.

At the next stage of ISA automation, ANN is used.

In the process of developing a method for conducting ISA, which would be based on obtaining numerical assessments of the risks of IS violation using ANN, it is necessary to generate data for a training sample. Next, the ANN structure is selected.

An example of a developed ANN for ISA automation is shown in Fig. 3.

TABLE I
AN EXAMPLE OF A PART OF THE TABLE OF CONDITIONAL PROBABILITIES FOR THE THREAT "DATA MODIFICATION IN THE INFORMATION SYSTEM"

Factors	*p_availability*	Full					
	p_integrity	Full					
	p_confidentiality	Full					
	n_network	Intersegment					
	a_authentication	Missing		Weak			
	a_qualification	Low	Middle	High	Low	Middle	High
Threat level	*trivial*	0,00059	0,00059	0,025	0,0074	0,0074	0,025
	low	0,00059	0,00059	0,025	0,0074	0,0074	0,025
	medium	0,00059	0,00059	0,9	0,0074	0,0074	0,9
	high	0,998	0,998	0,025	0,97	0,97	0,025
	critical	0,00059	0,00059	0,025	0,0074	0,0074	0,025

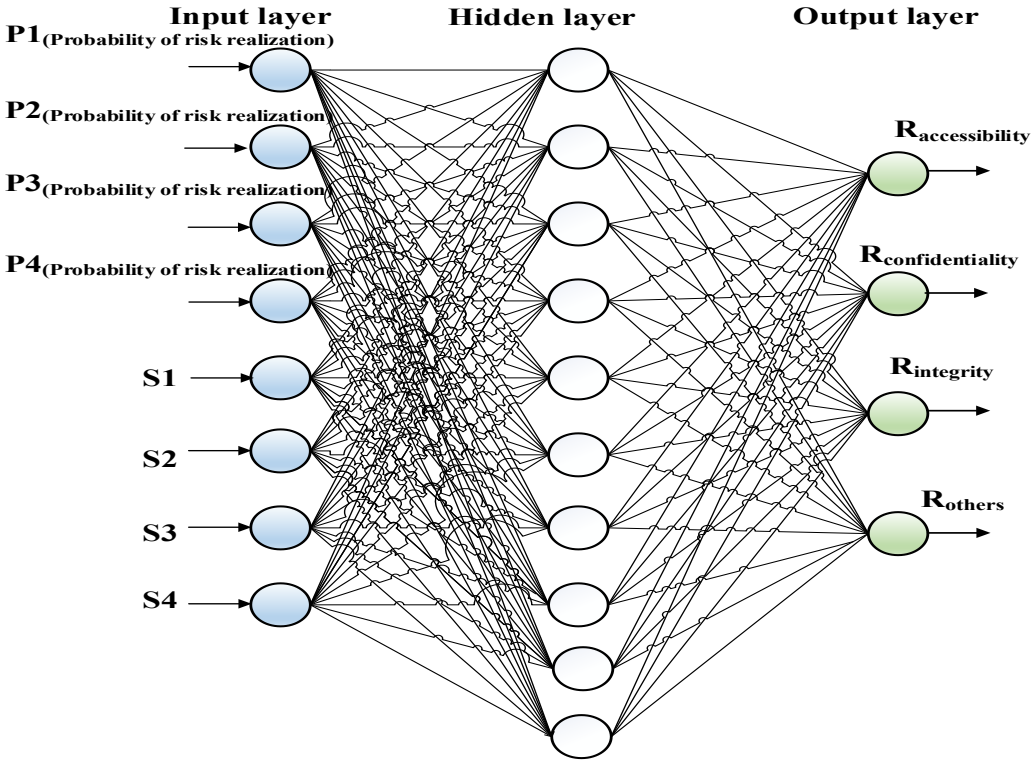

Fig. 3. ANN topology for ISA automation

An example of a training sample fragment for the network topology shown in Fig. 4 is shown in Table 2.

DCN was conditionally divided into 4 segments - Each segment corresponds to the network of the head office and separate structural divisions.

ANN includes 10 neurons in the hidden layer and four neurons in the output layer. When training a multilayer perceptron, an error backpropagation algorithm was applied.

The value of information assets (IA) can be set by the owner. The owner of the IA determines their value based on their usefulness for their business processes. And also considering the importance of the IA and the potential losses in the event of their loss.

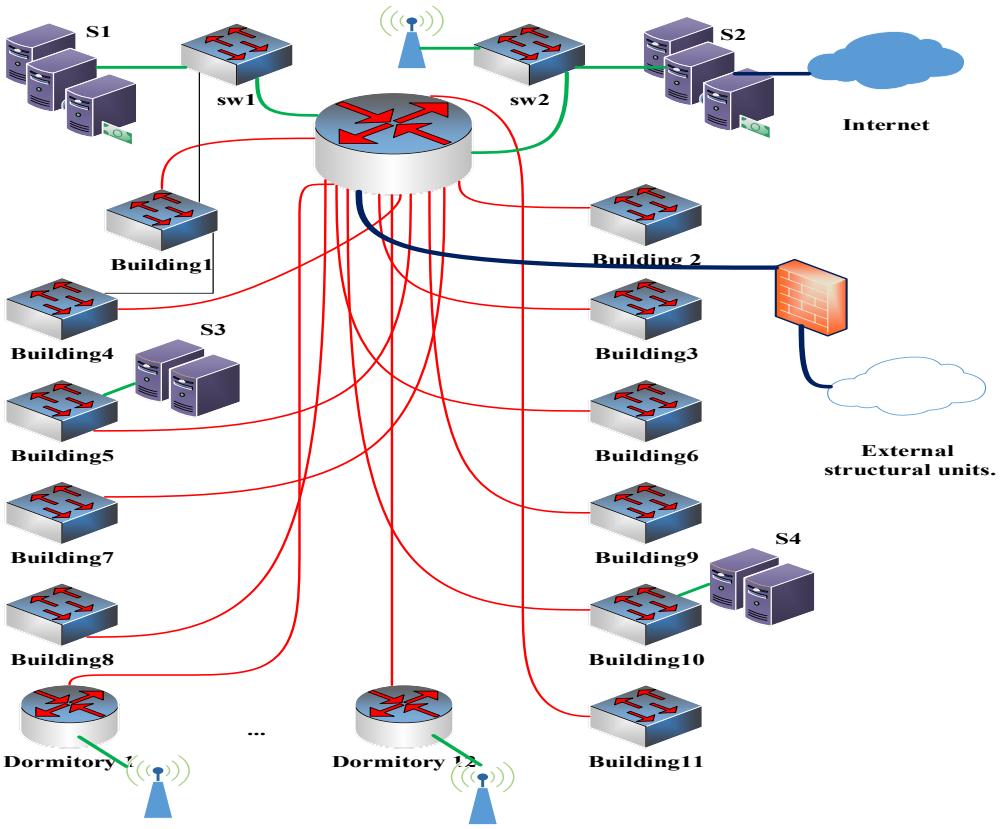

Fig. 4. OBI network architecture

TABLE II
FRAGMENT OF THE TRAINING SET FOR ANN

Probabilities of Threats Realization				DCN OBI segments				Information security risks
P1	*P2*	*P3*	*P*	*S1*	*S2*	*S3*	*S4*	
0	0	0	0	0	0	0	0	0
0	0	0	1	0	0,1	0,3	0,4	0
…	…	…	…	…	…	…	…	
1	1	1	1	0,6	0,1	0,4	0,2	0,21

Note that when developing the ANN, the specificity of the training sample was taken into account. The input of such an ANN is data obtained, for example, from antivirus software, firewalls, intrusion detection systems, etc. These data, respectively, act as a source of information when assessing the overall network activity and load, and also show the level of potentially dangerous activity.

V. COMPUTATIONAL EXPERIMENT

Computational experiments were carried out on the basis of the DCN of two universities - the National University of Life and Environmental Sciences of Ukraine (or NUBIP of Ukraine, Kyiv) and Yessenov University (Aktau, Kazakhstan).

The topology of the DCN of NUBIP Ukraine is shown in Fig.4.

Computational experiments for the designed ANN were performed using the Neural Network Toolbox for MATLAB

package. The training sample included from 1000 to 1500 samples. Test sample from 500 to 1000 samples. A graph illustrating the learning process of a neural network is shown in Fig. 5.

As a result, graphs of surfaces are obtained, for example, as in Figure 6.

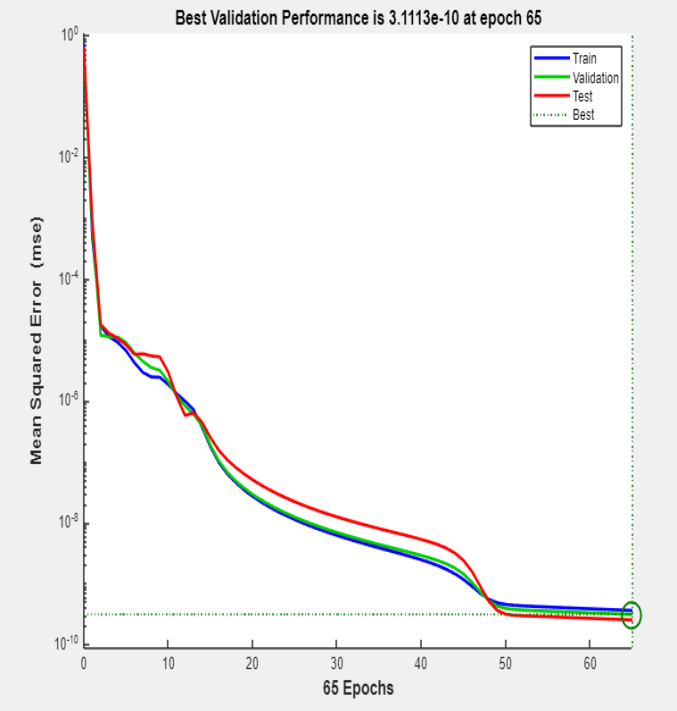

Fig. 5. Graph of the surface of the output values of IS risks

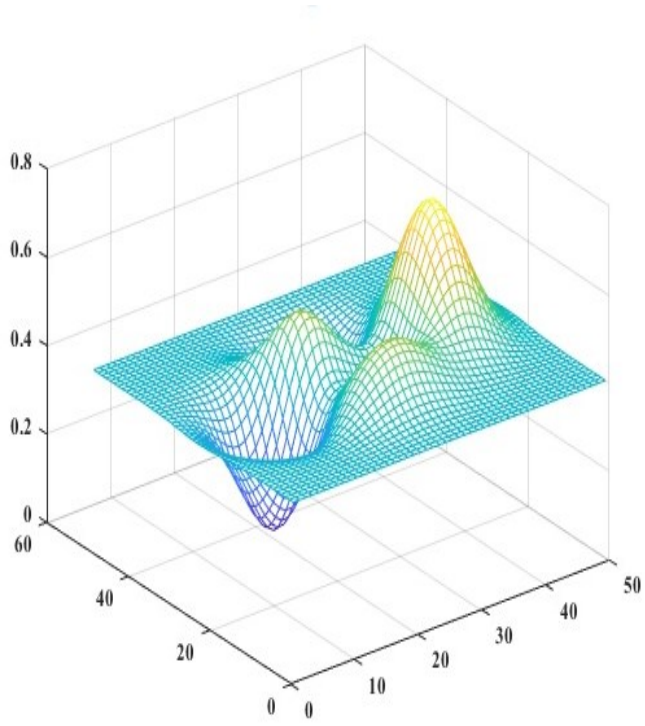

Fig. 6. Graph of the surface of the output values of IS risks

VI. Discussion of the results of the computational experiment

The results of computational experiments have shown that the initial dependences (1) - (4) can be fairly accurately approximated using artificial neural networks. It was found that with an increase in the number of neurons over 8, the complexity and degree of nonlinearity of the output display of the risk assessment parameters increases. When using artificial neural networks in ISA procedures, it is necessary to take into account the degree of expert's confidence in the previously formed training sample. If there is not enough data for training, or some of them are found unreliable, it is advisable to reduce the number of neurons. This allows you not to retrain the artificial neural networks.

Also, as a result of computational experiments in Genie and Matlab environments, it was shown that the proposed approach to assessing information security risks during an audit allows for a more accurate selection of information security tools for distributed computing networks circuits. Artificial neural networks used to assess and predict of information security risks during the audit not only allows you to effectively select countermeasures to protect OBI IS, but in general to build an effective ISMS adaptable to new threats. The cost reduction was at least 15% in comparison with the methods of risk assessment in the course of information security audit, which are described in the works [29, 32–34].

The prospect of research is the implementation of the developed artificial neural networks into the DSS, which can also be used in the course of ISA OBI. The task of the DSS will be to support options for solutions that will allow the administrator of the information security of the distributed computing networks to act proactively. For example, as such preventive measures, you can consider: stopping or restarting servers, restarting virtual machines, etc.

The combined use of the Bayesian networks apparatus and the artificial neural networks makes it possible to automate the information security audit procedures, including for rather complex scenarios of attacks on the distributed computing networks.

Conclusion

Within the framework of the studies carried out, the following main results were obtained:

The information security audit method was developed, based on the automation of audit procedures by using the Bayesian networks apparatus and the artificial neural networks to assess the of information security risks. It is shown that such a combination makes it possible to quickly determine the actual risks for information security OBI in the course of information security audit. At the same time, data from sensors / sensors of various hardware and software means of information protection in the OBI DCN segments are used as the initial information.

Automation of ISA procedures based on the use of BN and ANN allows the information security administrator of the DCN to respond dynamically to threats in a timely manner.

References

[1] R. Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon," in IEEE Security & Privacy, vol. 9, no. 3, pp. 49-51, May-June 2011, https://doi.org/10.1109/MSP.2011.67

[2] Lyubchenko, A. A. (2019). The Information Society and the Threat of Cyberwar. In Derzhavin Readings (pp. 303-305).

[3] Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. information security technical report, 13(4), 247-255. https://doi.org/10.1016/j.istr.2008.10.010

[4] Kanatov, M., Atymtayeva, L., & Yagaliyeva, B. (2014, December). Expert systems for information security management and audit. Implementation phase issues. In 2014 Joint 7th International Conference on Soft Computing and Intelligent Systems (SCIS) and 15th International Symposium on Advanced Intelligent Systems (ISIS) (pp. 896-900). IEEE. https://doi.org/10.1109/SCIS-ISIS.2014.7044702

[5] Han, D., Dai, Y., Han, T., & Dai, X. (2015). Explore Awareness of Information Security: Insights from Cognitive Neuromechanism. Computational Intelligence and Neuroscience, 2015, 762403-762403. https://doi.org/10.1155/2015/762403

[6] Andrade, R., Torres, J., & Flores, P. (2018, January). Management of information security indicators under a cognitive security model. In 2018 IEEE 8th annual computing and communication workshop and conference (CCWC) (pp. 478-483). IEEE. https://doi.org/10.1109/CCWC.2018.8301745

[7] Grediaga, Á., Ibarra, F., García, F., Ledesma, B., & Brotóns, F. (2006, May). Application of neural networks in network control and information security. In International Symposium on Neural Networks (pp. 208-213). Springer, Berlin, Heidelberg. https://doi.org/10.1007/11760191_31

[8] Mukkamala, S., Janoski, G., & Sung, A. (2002, May). Intrusion detection using neural networks and support vector machines. In Proceedings of the 2002 International Joint Conference on Neural Networks. IJCNN'02 (Cat. No. 02CH37290) (Vol. 2, pp. 1702-1707). IEEE. https://doi.org/10.1109/IJCNN.2002.1007774

[9] Kirta, T., & Kivimaab, J. (2010). Optimizing it security costs by evolutionary algorithms. In Conference on Cyber Conflict Proceedings (pp. 145-160). https://ccdcoe.org/uploads/2018/10/Kirt-et-al-Optimizing-IT-security-costs-by-evolutionary-algorithms.pdf

[10] S. Lysenko, K. Bobrovnikova, R. Shchuka and O. Savenko, "A Cyberattacks Detection Technique Based on Evolutionary Algorithms," 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), 2020, pp. 127-132, https://doi.org/10.1109/DESSERT50317.2020.9125016

[11] Barankova I.I., Mikhailova U.V., Kalugina O.B. (2020) Analysis of the Problems of Industrial Enterprises Information Security Audit. In: Radionov A., Karandaev A. (eds) Advances in Automation. RusAutoCon 2019. Lecture Notes in Electrical Engineering, vol 641. Springer, Cham. https://doi.org/10.1007/978-3-030-39225-3_104

[12] Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. Accounting, Organizations and Society, 71, 15-29. https://doi.org/10.1016/j.aos.2018.04.005

[13] Mataracioglu, T., & Ozkan, S. (2011). Governing information security in conjunction with COBIT and ISO 27001. arXiv preprint arXiv:1108.2150.

[14] Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2012). The relationship between internal audit and information security: An exploratory investigation. International Journal of Accounting Information Systems, 13(3), 228-243. https://doi.org/10.1016/j.accinf.2012.06.007

[15] R. Montesino and S. Fenz, "Information Security Automation: How Far Can We Go?," 2011 Sixth International Conference on Availability, Reliability and Security, 2011, pp. 280-285, https://doi.org/10.1109/ARES.2011.48.

[16] Au, C. H., & Fung, W. S. (2019). Integrating Knowledge Management into Information Security: From Audit to Practice. International Journal of Knowledge Management (IJKM), 15(1), 37-52. https://doi.org/10.4018/IJKM.2019010103

[17] Stafford, T., Deitz, G., & Li, Y. (2018). The role of internal audit and user training in information security policy compliance. Managerial Auditing Journal, 33(4), 410-424. https://doi.org/10.1108/MAJ-07-2017-1596

[18] T. S. M. Pereira and H. Santos, "A Security Framework for Audit and Manage Information System Security," 2010 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology, 2010, pp. 29-32, https://doi.org/10.1109/WI-IAT.2010.244

[19] Mashkina I. V., Sentsova A. U. The methodology of expert audit in the cloud computing system // Information technology security, 2013. № 4. P. 63–70.

[20] Guzairov M. B., Mashkina, I. V., Stepanova E. S. The treats model development by fuzzy cognitive maps formation on the bases of security policy // Information technology security, 2011. № 2. P. 37–49.

[21] Sentsova, A.Yu., Mashkina, I.V. Automation of an expert audit of information security based on the use of an artificial neural network. Information technology security. National Research Nuclear University "MEPhI" VNIIPVTI, No2, 2014. p. 118-126.

[22] Makarevich, O., Mashkina, I., & Sentsova, A. (2013, November). The method of the information security risk assessment in cloud computing systems. In Proceedings of the 6th International Conference on Security of Information and Networks (pp. 446-447).

[23] Mashkina, I. V., & Sentsova, A. U. (2014). The Method of the Information Security Risk Assessment in Cloud Computing Systems. In Computer Science and Information Technologies (CSIT'2014). (pp. 86-91).

[24] Akhmetov, B., Lakhno, V., Akhmetov, B., & Alimseitova, Z. (2018, September). Development of sectoral intellectualized expert systems and decision making support systems in cybersecurity. In Proceedings of the Computational Methods in Systems and Software (pp. 162-171). Springer, Cham.

[25] Lois, P., Drogalas, G., Karagiorgos, A., Thrassou, A., & Vrontis, D. (2021). Internal auditing and cyber security: audit role and procedural contribution. International Journal of Managerial and Financial Accounting, 13(1), 25-47.

[26] Roldán-Molina, G., Almache-Cueva, M., Silva-Rabadão, C., Yevseyeva, I., & Basto-Fernandes, V. (2017, June). A decision support system for corporations cybersecurity management. In 2017 12th Iberian Conference on Information Systems and Technologies (CISTI) (pp. 1-6). IEEE. https://doi.org/10.23919/CISTI.2017.7975826

[27] Calderon, T. G., & Cheh, J. J. (2002). A roadmap for future neural networks research in auditing and risk assessment. International Journal of Accounting Information Systems, 3(4), 203-236. https://doi.org/10.1016/S1467-0895(02)00068-4

[28] Gaganis, C., Pasiouras, F., & Doumpos, M. (2007). Probabilistic neural networks for the identification of qualified audit opinions. Expert Systems with Applications, 32(1), 114-124. https://doi.org/10.1016/j.eswa.2005.11.003

[29] Atamanov, A.N. (2012). Methodology for dynamic iterative assessment of information security risks in automated systems. Global Science Potential, (3), 30-34.

[30] Markowski, A. S., & Mannan, M. S. (2009). Fuzzy logic for piping risk assessment (pfLOPA). Journal of loss prevention in the process industries, 22(6), 921-927. https://doi.org/10.1016/j.jlp.2009.06.011

[31] Grace, A. M., & Williams, S. O. (2016). Comparative analysis of neural network and fuzzy logic techniques in credit risk evaluation. International Journal of Intelligent Information Technologies (IJIIT), 12(1), 47-62. https://doi.org/10.4018/IJIIT.2016010103

[32] Mokhor, V., & Honchar, S. F. (2018). The Idea of the Construction of the Algebra of Risks on the Basis of the Theory of Complex Numbers. Electronic modeling, 40(4), 107-111. https://doi.org/10.15407/emodel.40.04.107

[33] Mokhor, V., Honchar, S., & Onyskova, A. (2020). Cybersecurity Risk Assessment of Information Systems of Critical Infrastructure Objects. In 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T). (pp. 19-22). IEEE. https://doi.org/10.1109/PICST51311.2020.9467957

[34] Akhmetov, B.S., Lakhno, V.A., Ydyryshbayeva, M.B., Yagaliyeva, B.E., Baiganova, A.V., Akhanova, M.B., Tashimova, A.K. Application of bayesian networks in the decision support system during the analysis of cyber threats (2021) Journal of Theoretical and Applied Information Technology, 99 (4), pp. 884-893.

[35] US National Vulnerability Database - https://nvd.nist.gov/

[36] Bebeshko, B., Khorolska, K., Kotenko, N., Kharchenko, O., & Zhyrova, T. (2021). Use of neural networks for predicting cyberattacks. Paper presented at the CEUR Workshop Proceedings, 2923 13-223. http://ceur-ws.org/Vol-2923/paper23.pdf

[37] Khorolska K., Lazorenko V., Bebeshko B., Desiatko A., Kharchenko O., Yaremych V. (2022) Usage of Clustering in Decision Support System. In: Raj J.S., Palanisamy R., Perikos I., Shi Y. (eds) Intelligent Sustainable Systems. Lecture Notes in Networks and Systems, vol 213. Springer, Singapore. https://doi.org/10.1007/978-981-16-2422-3_49

[38] Lakhno V., Akhmetov B., Ydyryshbayeva M., Bebeshko B., Desiatko A., Khorolska K. (2021) Models for Forming Knowledge Databases for Decision Support Systems for Recognizing Cyberattacks. In: Vasant P., Zelinka I., Weber GW. (eds) Intelligent Computing and Optimization. ICO 2020. Advances in Intelligent Systems and Computing, vol 1324. Springer, Cham. https://doi.org/10.1007/978-3-030-68154-8_42