Journal of Theoretical and Applied Information Technology
30th September 2022. Vol.100. No 18

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MODELS AND ALGORITHMS FOR OPTIMIZING THE RESERVE OF EQUIPMENT TO ENSURE THE CYBERSECURITY OF THE INFORMATION EDUCATIONAL ENVIRONMENT OF THE UNIVERSITY

[1]AKHMETOV B.S., [1]ABUOVA A.K., [1]IZBASOVA N.B., [2]ZHILKISHBAYEV A.A., [3]GERASYMCHUK N, [4]MATOVKA T., [4]RIZAK V.

[1]Abai Kazakh National Pedagogical University, Kazakhstan
[2]Yessenov University, Aktau, Kazakhstan
[3]Poltava State Agrarian University, Kyiv, Ukraine
[4]Uzhhorod National University, Kyiv, Ukraine

E-mail: [1]bakhytzhan.akhmetov.54@ gmail.com, [1]valss6412@gmail.com, [2]nurgul.izbassova@gmail.com, [2]askhat.zhilkishbayeva@yu.edu.kz, [3]nataliia.herasymchuk@pdaa.edu.ua, [4]rtanyusha17@gmail.com, [4]vrizak@uzhnu.edu.ua

ABSTRACT

The article proposes to apply a system of sufficiency indicators in the process of solving the optimization problem of assessing the effectiveness of choosing the composition of the backup equipment (CBE) for the information and educational environment of the university (IEEU), including information security systems (ISS). Also, a model, algorithms and corresponding software (SW) have been developed for solving the optimization problem of choosing CBE for IEEU. The proposed solutions will help to ensure the smooth operation of the IEEU. This is true both in terms of technological failures and in terms of destructive interference in the work of IEEU by hackers. The proposed solutions help to reduce the cost of creating a CBE for IEEU by 14–18%. For the practical implementation of the developed algorithms, a neural network analyzer (NNA) was developed and tested as part of a decision support system (DSS) for the selection of CBE for IEEU.

Keywords: *Information And Educational System Of The University, Information Security System, Equipment Reserve, Algorithm, Optimization*

1. INTRODUCTION

One of the criteria for evaluating a post-industrial society in a developed state is the existence of a system of continuous education. This criterion characterizes the role and importance of continuous human learning in accordance with the concept of rapid knowledge updating. In developed countries, there is an increasing opportunity to use advanced educational environments, platforms and new educational technologies in the process of teaching students at universities. Information technology (IT) has long been an integral part of the education of the world's leaders in the US, the EU, China and other countries. The modern information and educational environment of universities (hereinafter referred to as IEEU) today is a form of functioning of an educational institution in the electronic space, access to which is provided using information technologies and communications. Moreover, both for stationary and for distance learning (DL), Internet technologies, popular web services, etc. are widely used.

Most specialists in the field of digitalization of education consider computer equipment and telecommunication technologies as fairly reliable systems. And they expect to radically improve the quality of education with their help. However, as noted in [1-3], the weak link of the IEEU is its cyber security (hereinafter CS), what has become especially noticeable in the context of the global pandemic associated with COVID-19. Insufficient security of the IEEU manifested itself in the conditions of an increase in the number and complexity of destructive interventions in the operation of information systems (IS) of the IEEU [4, 5]. Note that the tasks of providing information and CS of IEEU are quite close to similar tasks

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

related to the protection of information resources in other areas of human activity. Moreover, for many information systems (IS), for example, in banks and industrial enterprises, the relevant legislative and regulatory framework in CS issues has already been developed and successfully tested. There are also specific, well-proven organizational and technical solutions [6, 7].

As world practice shows, in the process of operation of complex systems, to which, in our opinion, IEEU can be attributed, complications or emergency situations inevitably arise. Partially, these complications or emergencies arise as a result of a violation of the technologies for operating IEEU equipment. However, in recent years, many violations of the performance of IEEU [8, 9] are caused by the destructive intervention of computer intruders (hackers).

IEEU hardware should be considered as a complex technical system. In this system there are a large number of interconnected elements and components. For example, servers, information systems, telecommunications equipment, etc. During the operation of the constituent elements and components of the IEEU, it is necessary to timely identify and fend off potential failures of many hardware systems, for example, sensors, video surveillance cameras, network equipment, etc. As a rule, even at the stage of development of such complex systems, designers lay in their design the possibilities for automatic restoration of the operability of many elements. However, this is not always possible in practice [3]. The possibilities of restoring the operability of IEEU components are determined by a number of factors. For example, such factors include the availability of resources: 1) technical support systems; 2) employees of the repair departments of the university; 3) transport; 4) other. The topology of the IEEU is also important. This is especially true for large universities, where academic buildings, laboratories and campuses can be geographically distant from each other.

In [1-3], it was noted that IEEUs often became the targets of targeted cyberattacks. Moreover, the list of cyber threats is constantly growing [11]. The growing cyber threats and the corresponding risks for the IEEU have led to the fact that the risk of failure, for example, of the server of the university's DL system, may adversely affect the financial and reputational losses of the university. Many risks in the field of CS of IEEU are related to the fact that the digital and physical infrastructure of IEEU inevitably intersect. Any IS involved in university management tasks can be subjected to major cyberattacks. For example, a system for recording personnel, a contingent of students, etc. And these systems, as a rule, are inextricably linked.

Increasingly complex scenarios for conducting cyber attacks on IEEU have led to the fact that their already rather complex architecture required to be supplemented with a variety of information security systems (ISS). This, in turn, gave rise to the need to determine the optimal composition of the backup equipment, including the information protection system for IEEU. Obviously, as the IEEU architectures become more complex, the computational complexity of finding the optimal composition of the backup equipment (CRE) has also increased. Even highly qualified experts are not always able to quickly analyze all the variables for this class of tasks and issue reasonable recommendations, justified by appropriate calculations on creating a reliable and secure IEEU architecture. First of all, from the point of view of information risks and CS of IEEU.

As practice shows, for any IEEU it is advisable to form technological reserves of equipment. For example, this reserve will be needed in case of failure of the IEEU equipment due to technological failures or cyber attacks. The failure of, for example, server equipment or a switching node will disable the entire IEEU.

The above arguments predetermined the relevance of the search for new models and methods for solving the problem of optimizing the composition of backup equipment for IEEU.

2. LITERATURE REVIEW

Failure of key IEEU components, for example, such important ones as server and communication equipment, uninterruptible power supplies, information security equipment, etc. even for a short time - a loss for the business processes of any university. When identifying pre-emergency situations, for example, caused by the destructive actions of the attacking side during the operation of the IEEU, the dimension of the feature space is quite large. Note that, as shown in [6], the boundaries between classes of different types of emergencies caused by cyberattacks are fuzzy in some cases. For example, most features of network cyberattacks are characterized by a set of features described in KDD 99. Quite a lot of works have been devoted to the issues of minimizing the dimension of the feature space when detecting pre-emergency conditions, for example, IS server equipment. So in [12-14], the authors showed that the use of models based on Bayesian classification and cluster analysis methods for solving the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

problem of recognizing potentially pre-emergency situations in IS (including IEEU) is inappropriate due to the inaccuracy of the findings. In [15, 16], the authors showed that it is better to use the apparatus of artificial neural networks (ANN) to solve this class of problems. As an ANN learning algorithm, the error backpropagation algorithm [17] can be used. In [18, 19], various mathematical models for ANN training were analyzed. In [20, 21] it is shown that, in comparison with other approaches, the potential of the ANN provides the universality of the learning algorithm.

It should be noted that the use of the error backpropagation algorithm for training a multilayer ANN gives reason to implement a specialized neural network analyzer (NNA). Such a NNA is adapted for a specific task - optimization of CBE for IEEU. Also, in parallel, with the help of the NNA, it is possible to perform the classification of pre-emergency situations in the IEEU. However, this is true for any objects of informatization. Such a classification is especially useful in situations of pre-emergency situations that arise as a result of the destructive effects of hackers. The hardware-software NNA will make it possible to reduce the time to eliminate emergency situations. It also becomes possible to reduce the cost of the CRE, which ensures the elimination of failures in the IEEU.

The purpose of the study is to develop algorithms for the NNA to improve the efficiency of forming the composition of the backup equipment for the IEEU.

Thus, the problem of the present study can be formulated as follows - the development of a methodology for solving optimization problems in the course of evaluating the effectiveness of choosing a composition of backup equipment (CBE) for the informational and educational environment of the university (IEEU), including information security systems (ISS). related software.

To achieve the goal of the study, it is necessary to solve the following tasks:

to develop new algorithms for emergency situations arising from the destructive actions of the attacking side;

to conduct computational experiments to study the degree of influence of the number of NNA outputs on the efficiency of choosing the composition of the backup equipment for the IEEU.

The need to solve the problem is related to the tendency of a constant increase in the number of destructive impacts on the informational and educational environment of universities (IEEU) from computer intruders' side.

3. METHODS AND MODELS.

Let's represent IEEU in the form of several functional circuits. The main circuits that need to protect their information resources are shown in Figure 1. These circuits primarily depend on the uninterrupted operation of the IEEU server and network equipment. Note that the circuits, as a rule, function as a single hardware-software complex. However, based on the topology of the IEEU, some of them can function independently. For example, the information arrays of the accounting circuit may not contain joint data with the circuit intended for issuing information about the progress of students' to parents.

Journal of Theoretical and Applied Information Technology
30th September 2022. Vol.100. No 18

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

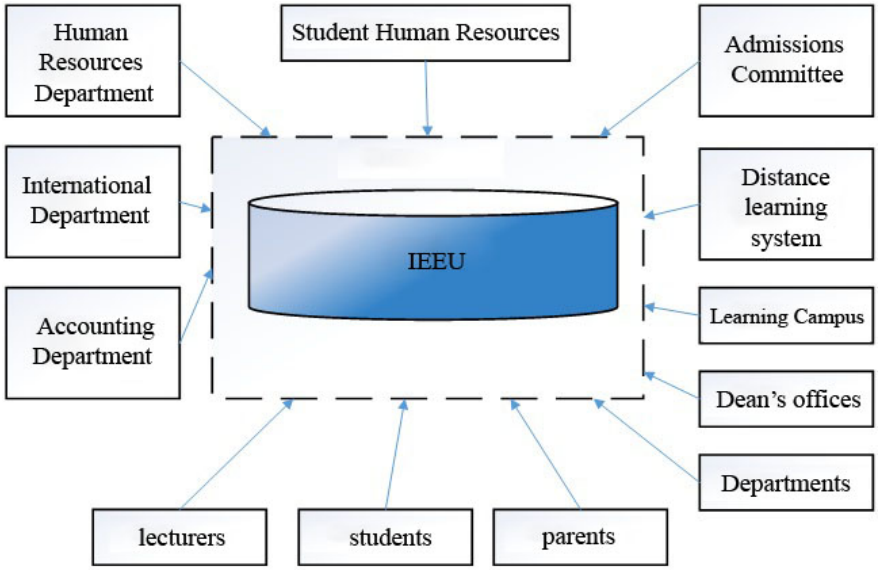

Figure 1: Scheme of IEEU elements

Let us introduce the following notations:

$W_{ij}-$ specific increment of reserve elements of the $i-$th type for the $j-$th IEEU circuit; $m-$ number of elements for a given type of IEEU equipment; t_r- the time it takes to resume the work of the IEEU after an emergency caused by the destructive interference of attackers; t_d- the time spent on the delivery of the CBE to a certain circuit of the IEEU; t_p- time spent repairing or backing up; t_i- time spent on replenishment of CBE for elements of the $i-$th type; $R-$ quantitative characteristics of the CBE for the restoration of the work of the IEEU; $C-$ CBE cost; C_d- the cost of delivery of the CBE to the warehouses of the university; C^0- cost of a serial sample of equipment for the IEEU circuit; $k-$ step number in the process of finding the optimal CBE; $\delta_{ij}-$ increment of reserve elements of the $i-$th type for the $j-$th IEEU circuit.

The problem of substantiating the quantitative CBE to ensure the current repairs of the IEEU has not been given due attention. Meanwhile, an integral part of the effective operation of the IEEU is, among other things, ensuring the restoration of its performance. This fully applies to the restoration of performance after the destructive effects of the attackers, both individual circuits and the IEEU as a whole. The task of optimizing the composition of CREs can, for example, be considered if we take the minimum cost of CREs as a basic criterion.

We write the analytical dependence for solving the direct optimization problem for determining the CBE as follows:

$$C^0_{\sum CPO} = \sum_{i=1}^{N} C_i \cdot R_i^{opt} = \min_{(R_i,...R_N)} \sum_{i=1}^{N} C_i \cdot R_i \quad (1)$$

under restrictions $SP(R_1,...R_N) \geq SP^0$,

where $N-$ number of types of spare parts (SP) for IEEU;

$C_1,...,C_N-$ SP cost vector;

$R_1,...,R_N-$ optimal SP set;

SP^0- normative value of the SP sufficiency criterion for IEEU.

Let us apply the hierarchical principle in the course of developing the methodology for

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

determining the optimal CBE for IEEU. Then, to restore the operability of one IEEU circuit, two approaches can be considered.

The first is the local location of the backup equipment. For example, for an IS used for distance learning, it is advisable to place the backup equipment directly in the information center of the distance learning. Indeed, it does not take much time to, for example, replace RAM sticks or a hard disk on a server of the DL system. This will allow to quickly eliminate the consequences of emergencies caused by the destructive interference of attackers. And, accordingly, this approach will ensure a quick replacement of the failed IEEU equipment.

The second approach is the storage of group stocks of CBEs in a warehouse. If the IEEU circuits operate the same type of network components, for example, switches, routers, video surveillance cameras, etc., then you can create a group reserve of CBEs. This group reserve will be available to all IEEU circuits without exception, although territorially each of these circuits can be located quite far, see fig. 2.

Accordingly, it is possible to restore the operability of the IEEU using the first or second approach. Their combination is also possible.

In our model, the optimization of the CBE system for IEEU is performed based on the following condition. In accordance with this condition, the reduced contribution of each element of the CBE to the average time spent on restoring the IEEU performance was taken as the basis.

In the course of research, appropriate algorithms were developed, see fig. 3–5. These algorithms can subsequently be used in the computational core of the decision support system (DSS), which will automate the search for the optimal CBEs. The individual main components of these algorithms are described below.

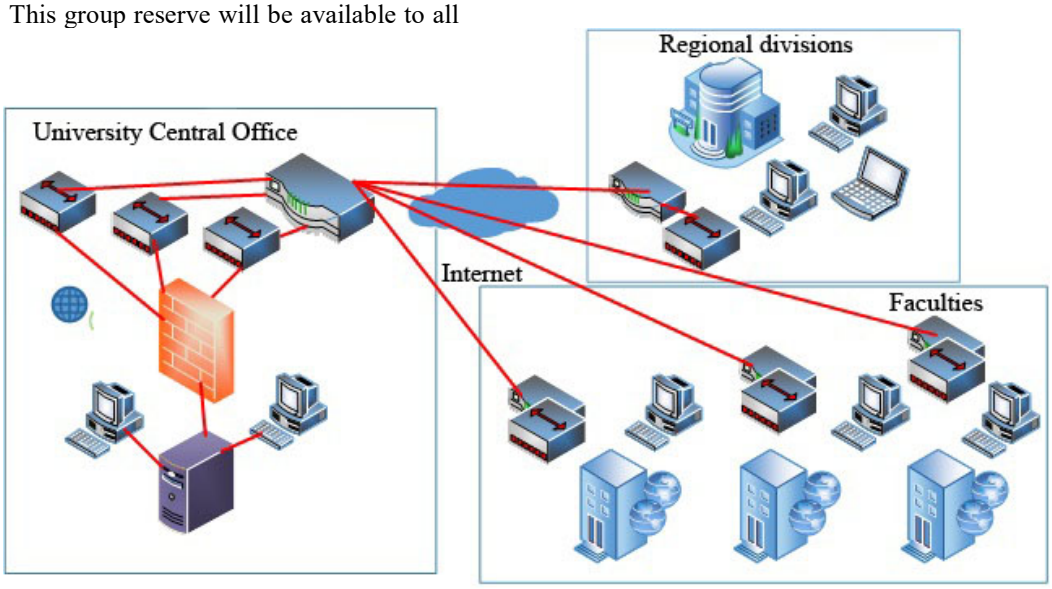

Figure 2: Scheme of IEEU elements for the territorially remote architecture of the university departments

In the first case, see Figure 4, an approximate solution of the above optimization problem is found. For the case when restrictions on the CBE cost for IEEU are set.

Journal of Theoretical and Applied Information Technology
30th September 2022. Vol.100. No 18

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

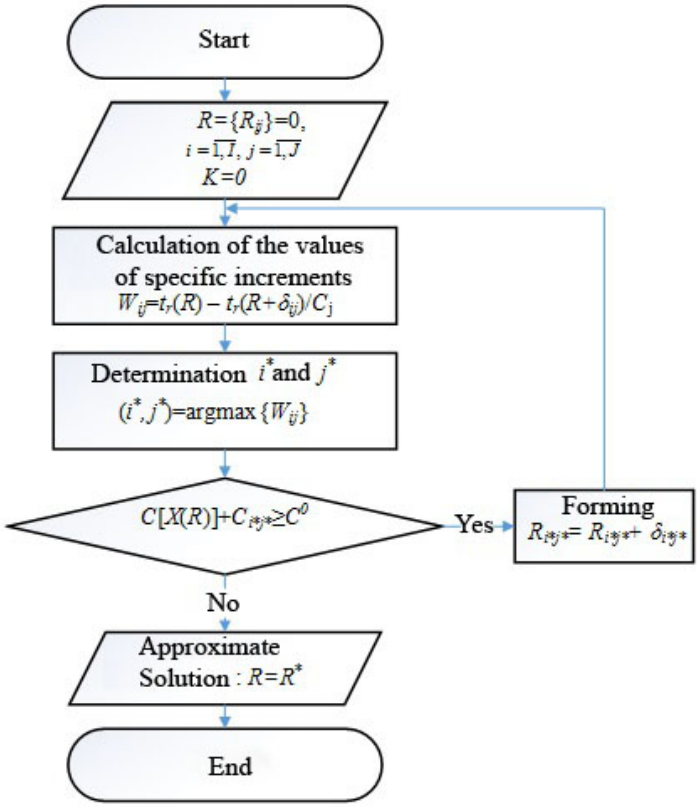

Figure 3: Block diagram of the algorithm for the formation of CBE for IEEU (variant 1)

In the second case, see Figure 4, we find a solution to the optimization problem for the variant when it is necessary to form an CBE warehouse for all IEEU circuits.

Journal of Theoretical and Applied Information Technology
30th September 2022. Vol.100. No 18

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

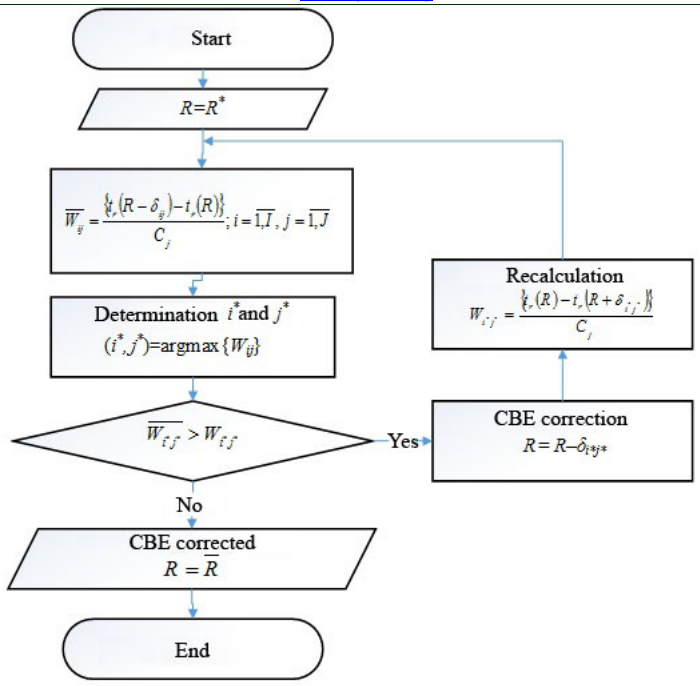

Figure 4: Block diagram of the algorithm for the formation of CBE for IEEU (variant 2)

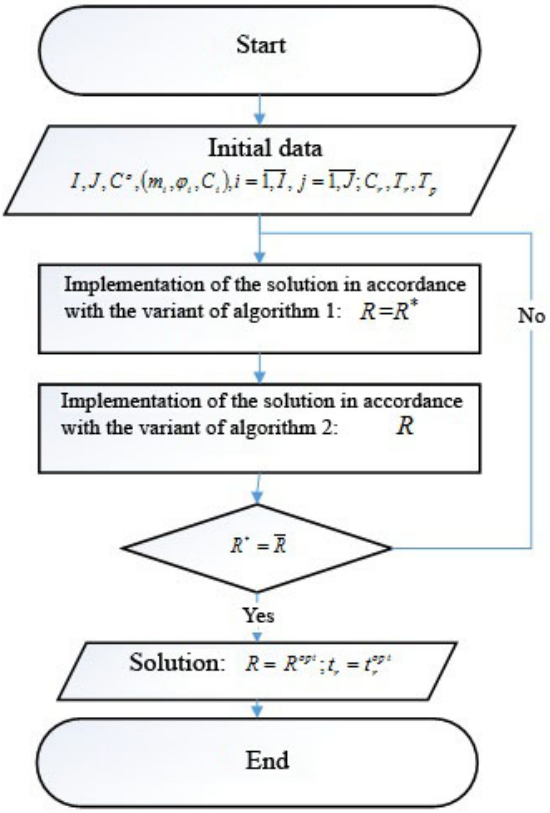

Figure 5: Block diagram of the CBE optimization algorithm for IEEU

Journal of Theoretical and Applied Information Technology
30th September 2022. Vol.100. No 18

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

During the study, the following assumption was put forward. It is possible to increase the efficiency of the DSS for the formation of an optimal CBE by using a neural network analyzer (NNA), see Fig. 6. Such a NNA will allow analyzing data on failures of IEEU equipment, for example, for individual circuits. Such information can later be used in the course of solving the optimization problem with respect to CBE for IEEU circuits. In fact, the NNA will become a source of additional data necessary to assess the performance of key IEEU equipment. The use of NNA allows to improve the strategies for the formation of CBEs and reduce the cost of maintaining the IEEU in working order even during targeted cyber attacks on the system. The following parameter is taken as an optimization criterion:

$$E = E_{ex} + E_{st} + E_s + E_{tr}, \tag{2}$$

where $E_{ex}, E_{st}, E_s, E_{tr} -$ respectively, the cost of operating IEEU equipment, downtime; storage of CBE in warehouses; CBE transportation.

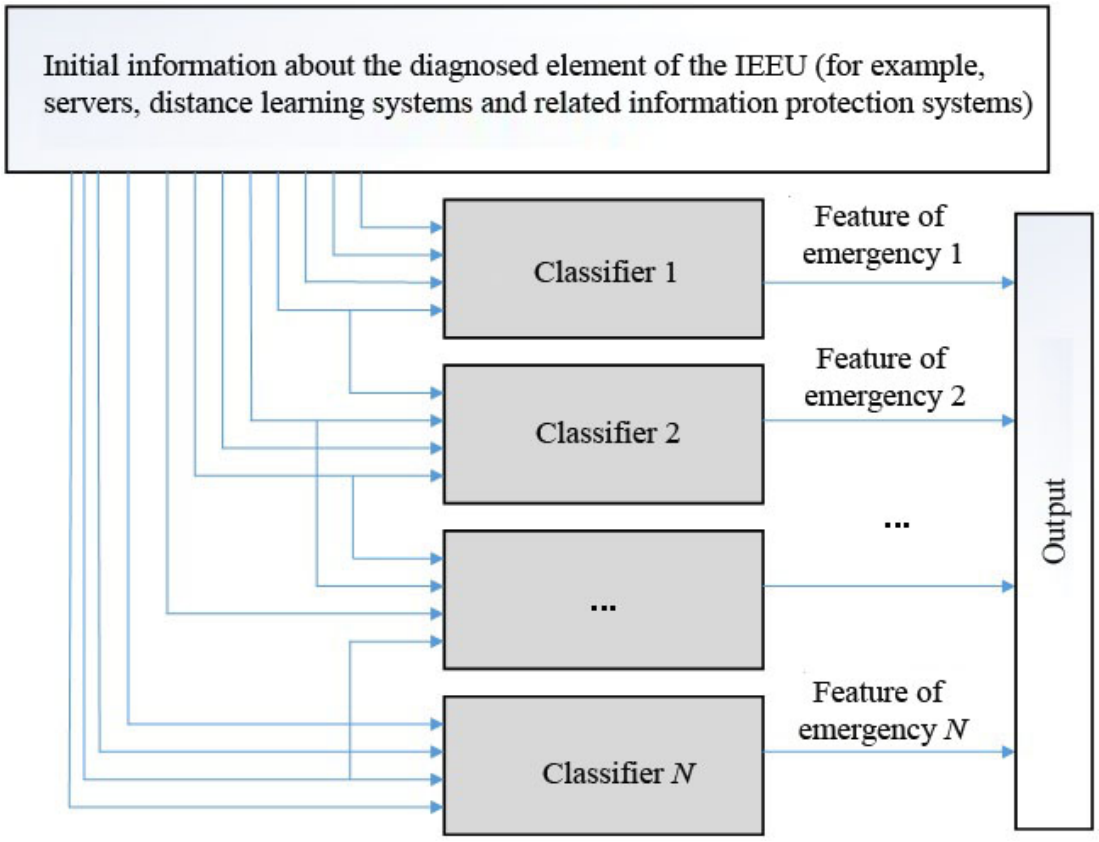

Figure 6: Schematic diagram of the NNA in the DSS for the selection of CBEs for IEEU

The developed models and the corresponding algorithms for the NNA used in solving the above optimization problem were implemented in the prototype of the DSS module, see Fig.7.

4. COMPUTATIONAL EXPERIMENT.

This prototype of the DSS module allows, in a user-friendly graphical interface for the IEEU administrator, to analyze the options for solving the problem depending on the list of pre-emergency

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

states identified by the NNA during the monitoring of the IEEU operation.

The developed module allows to view the received diagnostic messages to determine the CBE for the IEEU, as well as basic recommendations and ways to eliminate them, see Fig. 7

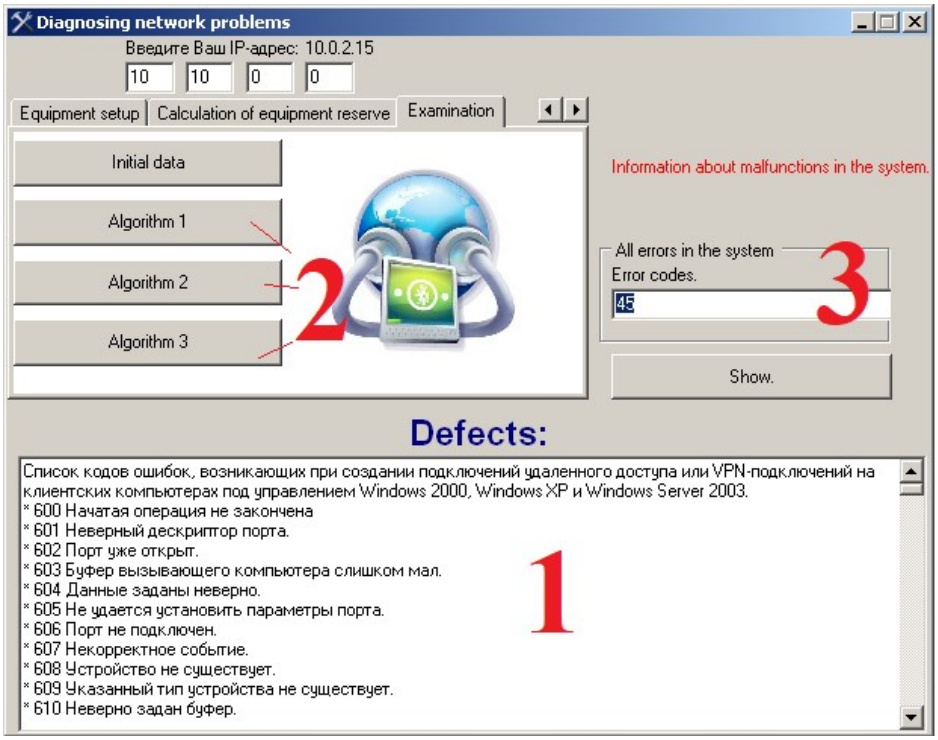

Figure 7: An Example Of The Operation Of The DSS Module With The NNA For Diagnosing The Equipment Of The IEEU Circuits (On The Example Of Network Equipment)

The numbers indicate: 1 - The area of messages about detected errors and pre-emergency situations identified during the diagnostics of the IEEU circuits; 2 - Selection of an algorithm for solving the problem of optimizing the CBE; 3 - Selection of the error code in the course of diagnosing the equipment of the IEEU circuits.

An experimental study of the developed DSS module was carried out for the IEEU equipment of the Abai University (Republic of Kazakhstan) and Esenov University (Republic of Kazakhstan). These educational institutions were chosen as the bases of the pilot study because they are actively developing Smart technologies in education.

Computational experiments for evaluating the effectiveness of the combined use of the NNA and the DSS module were carried out for different strategies for operating the equipment of the IEEU circuits. The corresponding results are shown in Figures 8, 9.

Figure 8 shows the calculated dependencies of the reduced costs for the hardware and software components of the information security system for different strategies for IEEU operating.

At the same time, during the computational experiment, a different number of neurons in the output layer were involved.

Figure 9 shows data on the number of iterations in the learning process of the NNA on the number of neurons and the number of layers.

Journal of Theoretical and Applied Information Technology
30th September 2022. Vol.100. No 18

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

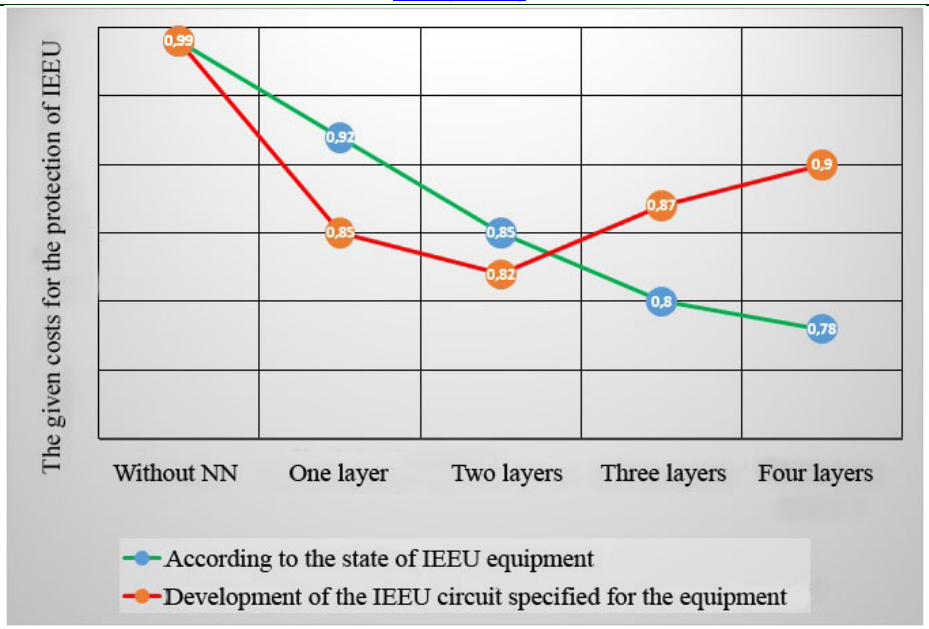

Figure 8: The Reduced Costs For The Hardware And Software Components Of The Information Security System For Different Strategies For The Operation Of The CBE For The IEEU And The Number Of Layers In The NNA

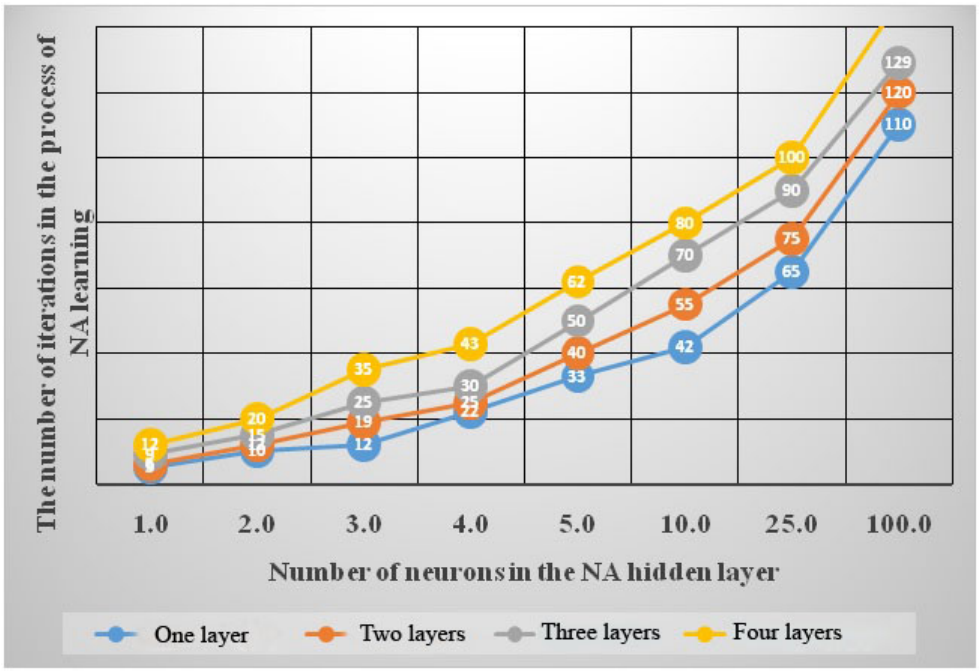

Figure 9: The Number Of Iterations In The Learning Process Of The NNA On The Number Of Neurons And The number of layers

Figure 9: The Probability Of The Accuracy Of Recognition Of Emergency Situations And The Correct Formation Of CBE For IEEU On The Number Of Neurons And The Number Of Layers In The NA
Figure 5: Block Diagram Of The CBE Optimization Algorithm For IEEU

5. DISCUSSION OF THE RESULTS OF A COMPUTATIONAL EXPERIMENT.

As can be seen from the obtained graphs 8 and 9, the best effect is achieved in the situation of applying the strategy for operating the equipment of the information protection system of the IEEU circuits until the specified number of hours is worked out. The developed DSS and NNA can be used to solve problems related to the choice of the optimal CBE. This contributes to the smooth operation of the IEEU. And as for the conditions of technological failures. The same is true for the conditions of destructive interference in the work of the IEEU by computer intruders attacking the IEEU. As experimental studies have shown, the proposed approaches help to reduce the cost of creating CBEs for the IEEU by 14–18% compared to the results of known calculation methods [22–27].

In the process of computational experiments, the following is shown. The optimal number of NNA outputs can be considered as 2–3. This number of outputs will ensure a reduction in the reduced costs of creating CBEs for the IEEU.

It has been established that for practical use it is better to use the NNA structure consisting of one hidden layer. The number of neurons in the hidden layer is assumed to be equal to the number of NNA inputs.

6. CONCLUSIONS.

It is proposed in the process of solving the problem of evaluating the effectiveness of choosing the composition of the backup equipment (CBE) for the information and educational environment of the university (IEEU), including information security systems (ISS), to apply a system of sufficiency indicators;

a model, algorithms and corresponding software have been developed for solving the optimization problem of choosing CBEs for the IEEU. The proposed solutions help to ensure the uninterrupted operation of the IEEU both in the conditions of technological failures and in the conditions of destructive interference in the work of the IEEU by hackers. The proposed solutions help to reduce the cost of creating CBEs for the IEEU by 14–18%;

various strategies for the operation of backup equipment for IEEU were considered;

it is shown that the optimal number of outputs of the neural network analyzer is 2–3.

This will ensure a reduction in the reduced costs for creating a backup of equipment for the IEEU circuits, including the ISS.

7. ACKNOWLEDGEMENTS.

The study is funded by the Kazakh National Pedagogical University named after Abay (contract No. PPS-DN-01 dated 12.02.2020)

REFERENCES:

[1] Lakhno, V., Blozva, A., Kasatkin, D., Chubaievskyi, V., Shestak, Y., Tyshchenko, D., Brzhanov, R. Experimental studies of the features of using WAF to protect internal services in the zero trust structure (2022) *Journal of Theoretical and Applied Information Technology*, 100 (3), pp. 705-721.

[2] Lakhno, V.A., Kasatkin, D.Y., Skliarenko, O.V., Kolodinska, Y.O. Modeling and Optimization of Discrete Evolutionary Systems of İnformation Security Management in a Random Environment, (2022) *Smart Innovation, Systems and Technologies*, 269, pp. 9-22.

[3] Akhmetov, B., Lakhno, V., Malyukov, V., Akhmetov, B., Yagaliyeva, B., Lakhno, M., Gulmira, Y. A Model for Managing the Procedure of Continuous Mutual Financial Investment in Cybersecurity for the Case with Fuzzy Information, (2022) *Lecture Notes on Data Engineering and Communications Technologies*, 93, pp. 539-553.

[4] Lakhno, V., Akhmetov, B., Chubaievskyi, V., Desiatko, A., Palaguta, K., Blozva, A., Chasnovskyi, Y., Information Security Audit Method Based on the Use of a Neuro-Fuzzy System, (2021) *Lecture Notes in Networks and Systems, 232 LNNS*, pp. 171-184.

[5] Akhmetov, B., Lakhno, V., Yagaliyeva, B., Kydyralina, L., Oshanova, N., Adilzhanova, S., Conceptual Diagram of An Intelligent Decision Support System in the Process of Investing in Cybersecurity Systems, (2021) *Journal of Theoretical and Applied Information Technology*, 99 (18), pp. 4297-4310.

[6] Lakhno, V., Adilzhanova, S., Kryvoruchko, O., Desiatko, A., Buriachok, V. Allocation of Organizational and Financial Resources of the Information Protection Side Using a Genetic Algorithm, (2021) *Lecture Notes in Networks and Systems*, 228, pp. 41-53.

[7] 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.

[8] Chapman, J., Chinnaswamy, A., & Garcia-Perez, A. (2018, January). The severity of cyber attacks on education and research institutions: a function of their security posture. *In Proceedings of ICCWS 2018 13th International Conference on Cyber Warfare and Security. Academic Conferences and Publishing Limited,* pp. 111-9.

[9] Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet*, 13(2), 39.

[10] Lakhno, V., Sahun, A., Khaidurov, V., Kasatkin, D., Liubytskyi, S., Model of operation system's incidents forecasting, (2021) *CEUR Workshop Proceedings, 2923*, pp. 289-294.

[11] Lakhno, V., Plyska, L., Analysis of Models for Selection of Investment Strategies, (2021) 2020 IEEE International Conference on Problems of Infocommunications *Science and Technology, PIC S and T 2020 - Proceedings*, № 9468024, pp. 43-46.

[12] Weber, P., & Jouffe, L. (2006). Complex system reliability modelling with dynamic object oriented Bayesian networks (DOOBN). *Reliability Engineering & System Safet*y, 91(2), 149-162.

[13] Cai, B., Liu, H., & Xie, M. (2016). A real-time fault diagnosis methodology of complex systems using object-oriented Bayesian networks. *Mechanical Systems and Signal Processing*, 80, 31-44.

[14] Lakhno, V.A., Kravchuk, P.U., Malyukov, V.P., Domrachev, V.N., Myrutenko, L.V., Piven, O.S., Developing of the cyber security system based on clustering and formation of control deviation signs, (2017) *Journal of Theoretical and Applied Information Technology*, 95 (21), pp. 5778-5786.

[15] Maździarz, A. Alarm Correlation in Mobile Telecommunications Networks based on k-means Cluster Analysis Method. Journal of telecommunications and information technology, 2, 2018, pp.95-102. https://doi.org/10.26636/jtit.2018.124518

[16] Bapiyev, I. M., Aitchanov, B. H., Tereikovskyi, I. A., Tereikovska, L. A., & Korchenko, A. A. (2017). *Deep neural networks in cyber attack detection systems. International Journal of Civil Engineering and Technology (IJCIET)*, 8(11), 1086-1092.

[17] Lakhno, V., Kryvoruchko, O., Desiatko, A., Blozva, A., Semidotska, V., Development strategy model of the informational management logistic system of a commercial enterprise by neural network apparatus, (2020) *CEUR Workshop Proceedings, 2746*, pp. 87-98.

[18] .Cilimkovic, M. (2015). Neural networks and back propagation algorithm. Institute of Technology Blanchardstown, Blanchardstown Road North Dublin, 15, 1-12.

[19] Wilamowski, B. M. (2009). Neural network architectures and learning algorithms. *IEEE Industrial Electronics Magazine*, 3(4), 56-63.

[20] Prechelt, L. (1996). A quantitative study of experimental evaluations of neural network learning algorithms: Current research practice. *Neural Networks*, 9(3), 457-462.

[21] Karayiannis, N. B., & Venetsanopoulos, A. N. (1993). Fast learning algorithms for neural networks. *In Artificial Neural Networks (pp. 141-193). Springer, Boston*, MA.

[22] Tamp, N. V., & Tamp, V. L. (2016). Programma raspoznavaniya sostoyanij informacionno-vychislitel'noj seti na osnove nejronnoj seti s obratnym rasprostraneniem oshibok. Svidetel'stvo o gosudarstvennoj registracii programmy dlya EVM Nomer svidetel'stva: RU 2016660599.

[23] CHEN, Mu-Chen; HSU, Chih-Ming; CHEN, Shih-Wei. Optimizing joint maintenance and stock provisioning policy for a multi-echelon spare part logistics network. *Journal of the Chinese Institute of Industrial Engineers*, 2006, 23.4: 289-302.

[24] MOURONTE-LÓPEZ, Mary Luz. Optimizing the spare parts management process in a communication network. *Journal of Network and Systems Management*, 2018, 26.1: 169-188.

[25] Lakhno V., Abuova A., Sagyndykova S., Alenova R., Lakhno Miroslav et al. Choosing an investment strategy for smart city projects based on a genetic algorithm, (2022) *Journal of Theoretical and Applied Information Technology*, 100(3), pp. 591-602.

[26] Lakhno, V., Akhmetov, B., Mohylnyi, H. ey al. A. Multi-criterial optimization Composition of cyber security circuits based on genetic algorithm (2022), *Journal of Theoretical and Applied Information Technology*, 100 (7), pp. 1996-2006.

[27] Lakhno, V., Bereke, M., et al. Genetic algorithm for solving the problem of scaling a cloud-oriented object of informatization (2022), Journal of *Theoretical and Applied Information Technology*, 100 (7), pp. 1693-1705.