Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 215 (2022) 598–607

Procedia Computer Science

www.elsevier.com/locate/procedia

4th International Conference on Innovative Data Communication Technology and Application

Application of a Genetic Algorithm for the Selection of the Optimal Composition of Protection Tools of the Information and Educational System of the University

Akhmetov B.S.[a], Lakhno V.[b], Akhmetov B.B.[c], Zhilkishbayev A.[c], Izbasova N.[c], Kryvoruchko O.[d], Desiatko A.[d]*

[a]*Abai Kazakh National Pedagogical University, Kazakhstan*
[b]*National University of Life and Environmental Sciences of Ukraine, Ukraine*
[c]*Yessenov University, Kazakhstan*
[d]*State University of Trade and Economics, Ukraine*

Abstract

The article discusses the possibility of using a genetic algorithm (GA) in the search for the optimal composition of information security tools (IST) for the information and educational environment of the university (IEEU). In the process of research, there was developed an optimization model for choosing the structure and composition of the information security system for IEEU nodes. The model made it possible to refine the objective function based on minimizing the costs of creating an information security system (IS) of the IEEU. The corresponding computational experiments were carried out, which confirmed the efficiency of the model. The practical significance of the conducted research lies in the fact that the proposed approach significantly reduces the time for calculating the optimal composition of the information security system for IEEU. This, in turn, allows the protection side to quickly respond to the changing landscape of cyber threats for IEEU. The proposed approaches, in our opinion, will lead to an improvement in their technical and economic indicators of the IS of IEEU system, reduce time and labor costs for designing an effective IS system

* Corresponding author. Tel.: +38-067-5051194.
E-mail address: desyatko@gmail.com

10.1016/j.procs.2022.12.062

Keywords: Information security; information and educational system of the university; information security tools, optimization

1. . Introduction

Ensuring information security (IS) and protecting information, including intellectual property and confidential data, is a complex and costly task for any organization. This fully applies to modern universities, which in recent years have formed information and educational systems (hereinafter referred to as IEE of the University or IEEU) [1]. Modern IEEU are a form of functioning of an educational institution in the electronic space. Access to the IEEU is provided with the help of modern information technologies and means of communication. In our opinion, the weak link of the IEEU is still its cybernetic or information security (hereinafter, respectively, CS and IS). The insufficient level of IS of the IEEU manifested itself in the conditions of an increase in the number and complexity of destructive interventions in the IEEU operation. One of the reasons for such IEEU vulnerabilities is the insufficient amount of investment in the creation of effective information security systems of universities. CS and IS have never been set as priority tasks for educational institutions. As an exception, we can consider technological universities that take part in research related to the protection of a particular state. In addition to costly investments in IEEU, other contradictions and complexities need to be considered. Let's take a quick look at these contradictions:

1) between the availability of information resources (IR) of IEEU and the required degree of protection. This is especially true for distributed computing systems (DCS). DCS is the basis of IEEU;
2) an excessive increase in the composition of information security tools (IST), as practice shows, does not directly lead to an increase in the degree of security of the informatization object. In addition, with regard to IEEU, an excessive increase in the number of information security facilities at the defense lines leads to a decrease in the usability of IEEU;
3) contradiction of interests of the operator side of the information security system (it is focused on the predictability of the parameters of the IS system efficiency), and the companies developing the IS tools. Many of the IST developers actively advertise their innovativeness, which, accordingly, leads to an increase in their cost. As a result, users, a priori, overpay for excessive functionality. Or users are forced to constantly increase the performance of their computer systems so that they meet the requirements of IST development companies.

The growth in the scale and number of successful cyber-attacks [2], the development of computer crime, is becoming a global trend. This trend makes the task of finding new ways to solve multicriteria optimization problems related to the selection of the composition of the information security system for protected objects relevant. This fully applies to the task of forming the composition of information security tools for IEEU. An additional factor emphasizing the importance of research in this area is the fact that the protection often has to act in dynamically complex situations. That is, when the cyber threat landscape is changing rapidly. Accordingly, the variability of the scenarios used by the attacker is difficult to predict. In such dynamically changing situations, the protection side of the IEEU has to take non-trivial responses. These measures or solutions are characterized by the following features:

1) in order to maximize the information security metrics of the IEEU, the protection side needs to make many decisions. Moreover, this applies to both technical and organizational decisions, for example. And besides, not least difficult financial decisions have to be made, since information security requires corresponding costs for hardware and software components of information security.
2) all solutions are interconnected. Accordingly, they cannot be considered in isolation from one another. The connections are not always obvious. These links can be either direct or indirect. And in some situations they are stochastic in nature;
3) it is important to take into account the influence of the external environment on IS of IEEU. The external environment is not characterized by constant parameters. It can change under the influence of both external factors.

All of the above, in fact, determines the complexity of finding methods acceptable for the protection side for solving a multi-criteria optimization problem for selecting information security tools (IST) for IEEU. All of the above has determined the relevance of the problem to be solved in this study.

2. Literature review

Many theorists in the field of information security theory in their works focus on the need to use the potential of intelligent information systems, for example, decision support systems (hereinafter DSS) to solve such optimization problems. In the process of solving such optimization problems, for example, modular [2, 3] or cluster [4] DSS were used. Examples of solving a similar class of problems in relation to optimizing the composition of the IS tools for various optimization objects are known. Moreover, it was shown in [5, 6, 7] that such a problem is complex. In [8], the authors note that the probability of losses that occur with an incorrectly chosen strategy for investing financial resources (FR) of companies in information security can be large. It is noted that the sphere of information security, by its nature, is not in all situations conducive to excessive innovation. With the help of DSS, a decision maker (DM), for example, for an information security administrator of a university, during a predictive assessment, it is easier to determine which particular set of information protection tools available on the market [8, 9] is a higher priority for investing their financial resources (FR). These reasons necessitated the search for rational strategies for investing in information security complex informatization objects, which certainly include IEEU. In these works, attention is also focused on the fact that it is difficult to manage without appropriate computer support for making such risky decisions. In [10], the authors noted that not all innovations have a beneficial effect on the investment market in the development of information security hardware and software. Such innovations often generate controversy among experts who argue about their appropriateness. In [11], it is rightly stated that investment projects in the field of information security should be considered comprehensively. That is, as a system of interrelated goals and programs for IS of the corresponding informatization object. However, this assertion was not further developed in the work. There is also no clear algorithm that allows finding a solution regarding the optimal composition of the information security system for the protected object. As the authors of [12] note, the achievement of a given level of information security of a protection object depends on the successful solution of a number of interrelated tasks: technical and technological, financial, organizational, etc. The authors of this study do not evaluate the advantages of using DSS in similar tasks related to the sphere of information security. The Gordon L. A. & Loeb M. P. models proposed in [13, 14] (hereinafter referred to as the GL models) have become one of the main ones for evaluating investments in information security. However, it should be noted that both the basic GL model and its numerous modifications, for example, [15], are characterized by certain disadvantages. In particular, it is shown in [16] that the formally approximate method of constructing a model does not make it possible to take into account the real mechanisms for ensuring the information security of the protected object, as well as the interests of investors. This limits the practical aspects of the application of the GL model and the objectivity of the findings. The authors of [17], [18] believe that the development of such an area of applied research as mathematical decision support in the course of choosing a rational strategy for investing in IS should be accompanied by a synthesis of new models and methods. The software implementation of the models presented in the works is not described.

In [18], it is noted that, in relation to this class of problems, the most adequate approach in the process of finding a solution can be models based on the application of game theory. It is noted in [19] that the category of software products such as DSS helps to simplify the task of finding rational strategies for investors in the field of IS. This, among other things, is also relevant when solving such a subtask as the formation of the optimal composition of the IS system for specific informatization objects. Moreover, optimization is performed based on the ratio of the cost of the information security system and their effectiveness. In [20], various approaches are considered in sufficient detail from the point of view of the mathematical apparatus used in such models. However, the software implementation of the proposed model is not given. The authors of [21] describe the application of classical economic and mathematical models. However, most of the analyzed models do not take into account many investing parameters in complex projects in the field of IS. As the analysis of works [22, 23, 24, 25, 26] showed, most of the models and algorithms given in the works analyzed above do not contain real recommendations for investors in the field of information security. The main disadvantage of such models is the low information content of the results obtained. In particular, it is quite difficult to assess the prospects of investment projects and options for investors in the field of information security. The papers [26, 27, 28, 29] consider the possibilities of using genetic algorithms (GA) to solve problems related to the choice of an investor's strategy. In these publications, the GA maintains a population (a group of chromosomes) that is a contender for the optimal solution. Using probabilistic operators, the authors of these studies sought to obtain populations that are most suitable for the conditions set for a particular problem. However, these GAs were actually simple operations for the exchange and copying of parts of chromosomes. This approach is not always suitable for such a subject area as the procedure for investing in complex information security projects.

The main disadvantage of the GA [29] can be considered as the possibility of its convergence to the local optimum. Based on the size of the binary solution vector and the selected set of IEEU cybersecurity frontiers), the dimension of the problem is calculated, i.e. the number of options for a set of solutions is determined. The choice of the optimization method depends on the resulting dimension of the problem. However, with an increase in the dimension of the problem, the requirements for resource intensity increase sharply. Accordingly, the efficiency of solving the problem worsens. Therefore, to search for the optimal composition of the information security system for distributed computing systems on which most of the IEEU are built, in our opinion, it is advisable to use GA. The foregoing determined the problem associated with the need to develop a GA-based model for solving an optimization problem to determine the optimal composition of the information security tools for IEEU, which is built based on a distributed computing network.

3. The purpose of the work

The purpose of the work is to develop a model for solving an optimization problem to determine the optimal composition of information security tools for the information and educational system of the university, which is built on the basis of a distributed computer network. To solve this problem, it is proposed to use a genetic algorithm.

4. Methods and models

There can be several criteria for evaluating the effectiveness of investing in IS systems for IEEU. These are also technical criteria that primarily evaluate the information security metrics of the protected object. In this case, we understand the object of protection as IEEU. You can also talk about economic criteria. After all, the management of IEEU is primarily interested in how effective the FR investments in the creation of the information security system of the IEEU will be. A decisive influence on the optimal solution is provided by forecasts of changes in the landscape of cyber threats for IEEU during the period of IEEU operation. It is difficult to accurately predict these threats. After all, even external factors, such as the COVID-19 pandemic, have influenced the change in the landscape of cyber threats, shifting the focus to network attacks against servers of the distance learning system. In view of the foregoing, as an optimization criterion when determining the composition of the IEEU information security system based on a distributed computer network, it is proposed to use the minimum cost for commissioning and subsequent operation of the IEEU information security system. That is, in fact, the annual reduced costs for the protection of IEEU. When some basic protection tools, for example, such as anti-virus software, firewalls, access control tools are already included in the basic distributed network, the problem of optimal planning of their operation modes arises. As well as the addition of more advanced components to the IEEU protection tools, for example, an intrusion detection system or cryptographic information protection. At the same time, we believe that the total costs of operating the entire IEEU information security complex should have been minimal.

The solution of the problem of optimizing the composition of the protection tools of the IEEU has a number of specific features. One of these features is integer. This is due to the fact that specific information security tools are selected based on the platforms and characteristics of both the server equipment of the distributed computing network of the IEEU, and for specific workstations and other types of information and communication equipment used in the educational process. Another feature of this problem is its large dimension. This is due to the fact that when searching for the minimum of the objective function, we have to go through many combinations of protection tools on the key nodes of the IEEU (for example, servers, routers, switches, workstations, individual audiences, etc.). The objective function in such problems can be characterized by several local minima. Accordingly, this complicates the use of the mathematical apparatus inherent in classical optimization methods. Given the above, in order to solve the optimization problem in the process of research, it is proposed to apply the GA method. This will allow to take into account the discreteness and integrality of the variables. In addition, GAs have proven themselves well in solving optimization problems characterized by large data dimensions. Also, GA is less sensitive to local extremes in comparison with other methods for solving optimization problems. To solve the problem of choosing the number of information security tools, their technical parameters based on integrated IS metrics, for the DCS of IEEU, the annual reduced costs are taken as the target function (TF) (TF or fitness functions in terms of GA):

$$C = p \cdot \sum_{i=1}^{n} CE_i + \sum_{i=1}^{m} OC_i, \tag{1}$$

where $p -$ coefficient characterizing the comparative efficiency of capital investments in information security of the university (IEEU), CE_i, $OC_i -$ respectively, the i-th cost items of capital and operational costs for IS of IEEU; $n, m -$ the number of components of capital and operating costs for IS of IEEU, respectively.

For the purpose of some simplification of the model, we will take the annual reduced costs for IS of the IEEU as the main optimization criterion in the task of evaluating the effectiveness of investing in the IS system. This simplification will demonstrate the overall performance of the model. And the simplicity of the calculation formula for the TF allows simplifying the analysis of the results for the adequacy of the model and the proposed GA to determine the optimal composition of the IST for IEEU. It is convenient to represent the components of capital costs for IS of IEEU in the context of the problem being solved analytically. It is possible, for example, to describe the costs of acquiring specific information security tools (within a specific class) for IS of IEEU as a function of the form:

$$CE_{1u} = a_1 + a_2 \cdot IPI, \tag{2}$$

where $IPI -$ an integral indicator of the effectiveness of a protection tool of a certain class (for example, a firewall or an intrusion detection system, etc.); $a_1, a_2 -$ a1, a2 – coefficients for linear approximation.

Similarly, it is possible to express the capital costs associated with the acquisition of other classes of information security tools, installation, connection to a distributed computer network of the university. Operating costs and limitations can be expressed in a similar way. Although, as was shown in [30, 31], the approximation expressions will not always be linear. In some cases, for example, when describing the costs of acquiring external services (protection of cloud services, VPN, protection against DDoS attacks, etc.), the function can change in steps [28].

We introduce a set of key private criteria that will be necessary to detail the description of the information security system for IEEU:

$$CR = \{CR_1, CR_2, CR_3, CR_4, CR_5\}, \tag{3}$$

where $CR_1 -$ cost of IST related to a certain class; $CR_2 -$ the number of threat classes for IS of IEEU, which will be blocked by the corresponding IST; $CR_3 -$ the size of leveled risk, which is reduced due to one or another class of IST; $CR_4 -$ availability of IS certificates for the relevant information security tools; $CR_5 -$ indicator of compatibility of a separate IST in the general protection complex and IS of IEEU.

Each of the private criteria specified above can vary in the range from 0 to 1. For example, for CR_5, if a specific IST is compatible with the rest in the group of tools located on the protected node, then the value $CR_5 = 1$. Otherwise $CR_5 = 0.$ For the criterion CR_1, , the interpretation can be as follows:

$$CR_1 = \begin{cases} 1, \quad if \quad C_{ist} < C_{ist}^{\max}; \\ 0{,}5 \quad if \quad 0{,}5 \cdot C_{ist}^{\max} \le C_{ist} \le C_{ist}^{\max}; \\ 0 \quad if \quad C_{ist} > C_{ist}^{\max}, \end{cases} \tag{4}$$

where $C_{ist}, C_{ist}^{\max}$ – average cost of IST within the analyzed class (for example, anti-virus software, firewalls, differentiation tools, intrusion detection systems, etc.) and the maximum cost.

For the criterion CR_2, the interpretation can be as follows [30]:

$$CR_2 = \begin{cases} 1, \quad if \quad \sum_{i=1}^{n} m_{ISR_{ii}}^{ist_k} = |IST|; \\ 0{,}5 \quad if \quad 0{,}5 \cdot |IST| \le \sum_{i=1}^{n} m_{ISR_{ii}}^{ist_k} \le |IST|; \\ 0{,}25 \quad if \quad 0 < \sum_{i=1}^{n} m_{ISR_{ii}}^{ist_k} \le 0{,}5 \cdot |IST|; \\ 0 \quad if \quad \sum_{i=1}^{n} m_{ISR_{ii}}^{ist_k} = 0, \end{cases} \tag{5}$$

where IST – many cyber threats to IEEU (the value is not constant and depends on external factors); n – the number of actual cyber threats for a specific IEEU; $m_{ISR_{ii}}^{ist_k}$ – matrix of overlapping actual cyber threats by existing and planned protection tools and IS of IEEU.

For the criterion CR_3, the interpretation can be as follows [30]:

$$CR_3 = \begin{cases} 1, \quad if \quad \sum_{i=1}^{n} R_{ISR} \cdot m_{ISR_{ii}}^{ist_k} < R_a; \\ 0{,}5 \quad if \quad R_a \le \sum_{i=1}^{n} R_{ISR} \cdot m_{ISR_{ii}}^{ist_k} \le 0{,}5 \cdot R_{cr}; \\ 0{,}25 \quad if \quad 0{,}5 \cdot R_{cr} \le \sum_{i=1}^{n} R_{ISR} \cdot m_{ISR_{ii}}^{ist_k} \le R_{cr}; \\ 0 \quad if \quad \sum_{i=1}^{n} R_{ISR} \cdot m_{ISR_{ii}}^{ist_k} \ge R_{cr}, \end{cases} \tag{6}$$

where R_a, R_{cr} – respectively, acceptable and critical levels of information security risk for information resources of the IEEU; n – the number of actual cyber threats for a specific IEEU; $m_{ISR_{ii}}^{ist_k}$ – matrix of overlapping actual cyber threats, by the existing and planned protection tools and IS of IEEU.

Similar calculations for partial criteria are repeatedly described in the scientific literature, for example [30, 31].

Then, using the proposed partial criteria, it is possible to represent the efficiency (EF) of the entire IS system for IEEU as a vector of the following form:

$$EF = \{1, 1, 1, 1, 1\}. \tag{7}$$

Actually, in this form, we have reference indicators of partial criteria that describe the effectiveness of the IST in the IS IEEU circuits (however, this is also true for other informatization objects)

It seems to be quite reasonable to use GA for ranking IST and their selection for IEEU nodes, based on generalized performance indicators. This will make it possible to form a rational composition of the IST by selecting specific funds from the existing list. Moreover, it is precisely those IST that are characterized by optimal adaptability indicators and fall under the specified cost restrictions are selected. The scheme of GA operation is shown on Figure 1, where changes during evolution occur in chromosomes. For the task under consideration, the chromosome encodes information about the integrated indicators of the efficiency of the IST, their number at the key nodes of the IEEU. Without retelling all the stages of GA, let's pay attention to the fact that in a distributed computer network of a university with its own IS system, the role of an individual is played by a certain possible composition of the IST for a node. Such an individual will be characterized by its own fitness function in the form of a TF. In the described problem, chromosomes are represented in binary code. Then the bits of the binary code in the GA are considered as separate genes.

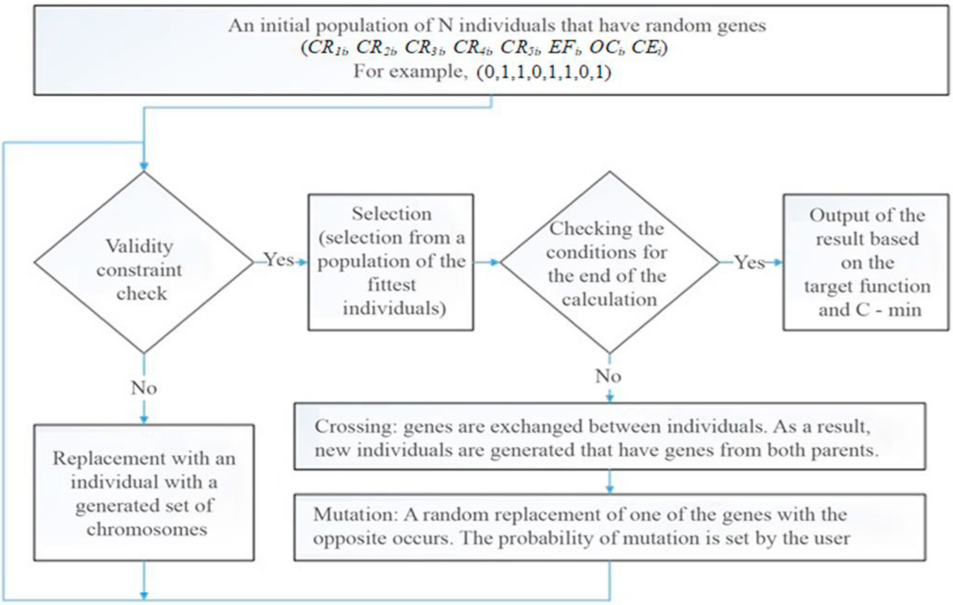

An initial population of N individuals that have random genes
$(CR_{1i}, CR_{2i}, CR_{3i}, CR_{4i}, CR_{5i}, EF_i, OC_i, CE_i)$
For example, (0,1,1,0,1,1,0,1)
Validity constraint check
Yes
Selection (selection from a population of the fittest individuals)
Checking the conditions for the end of the calculation
Yes
Output of the result based on the target function and C - min
No
No
Replacement with an individual with a generated set of chromosomes
Crossing: genes are exchanged between individuals. As a result, new individuals are generated that have genes from both parents.
Mutation: A random replacement of one of the genes with the opposite occurs. The probability of mutation is set by the user

Fig. 1. Generalized GA scheme

At the first stage of the GA operation, each of the individuals is subjected to a check for compliance with the restrictions. If a discrepancy is found, for example, the IS metrics for the IEEU node are low, then another individual is generated. At the next stage, individuals are selected from the population that are characterized by the lowest TF value. Then these selected individuals are crossed. As a result of crossing, descendants appear. At the same time, the higher the adaptability parameters of parental individuals, the greater the chances of their crossing. Since when crossing individuals exchange genes, new individuals bear the characteristics of parental individuals. Similarly, in GA, the most optimal solution is achieved. And although a number of individuals mutate, this fact helps the GA to implement the choice from local optima.

5. Computational experiment

The efficiency of the GA functioning is largely determined by its settings. The settings must be selected individually in each situation. It is advisable to select specific settings for the proposed model and the corresponding GA after a series of computational experiments. This will optimize the operation of the algorithm specifically for the task of selecting the optimal composition of the IST for IEEU. As a criterion in the computational experiments, the stop criterion (Sj) is set. This criterion corresponds to a given number of failed generations. The number of such failed generations ranged from $1000 < Sj < 30000$. For each value, the computational experiment was repeated 10 times. This is done in order to detect the average trend. The results of the calculations were summarized in Table 1. The table shows the average values of the objective function or the adaptability function (see expression (1), and also took into account the specifications of specific IST for IEEU, after which the values are reduced to the dimension of conventional units (to avoid binding to specific currencies) Values of IST specifications were taken according to the data of manufacturers or publications [27, 30, 32]. The results of the computations were summarized in Table 1. The table shows the average values of the objective function (see expression (1). Figures 2–4 show the results of the computational experiments

Table 1. Generalized results of computational experiments when testing GA.

KO, generation failures	Target function, conventional units	Calculation time Ta, min	The maximum value of the objective function, conventional unit	Time value of calculation time Ta, min	Average compliance of the result to the reference $Shmax$,%	Minimum compliance of the result to the reference $Shmin$,%
$1\cdot10^3$	55.1	45	56.9	59	97,62	94.36
$5\cdot10^3$	53.7	165	53.8	192	99.996	99.96
$10\cdot10^3$	53.7	329	53.8	411	99.996	99.995
$15\cdot10^3$	53.7	389	53.8	462	100	99.995
$20\cdot10^3$	53.7	410	53.8	521	100	99.995
$25\cdot10^3$	53.7	537	53.8	643	100	100
$30\cdot10^3$	53.7	654	53.8	725	100	99.995

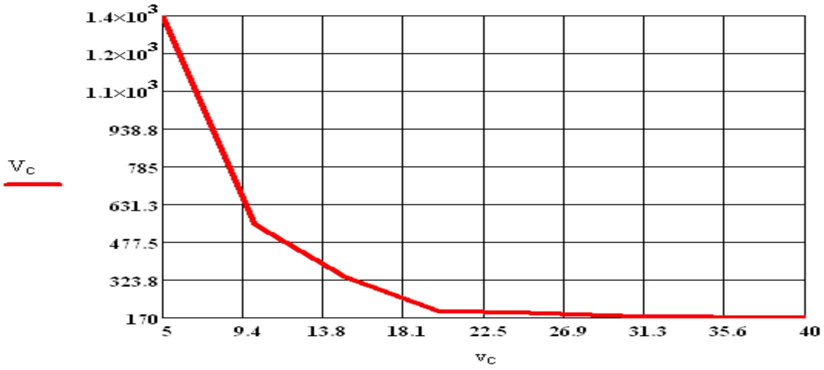
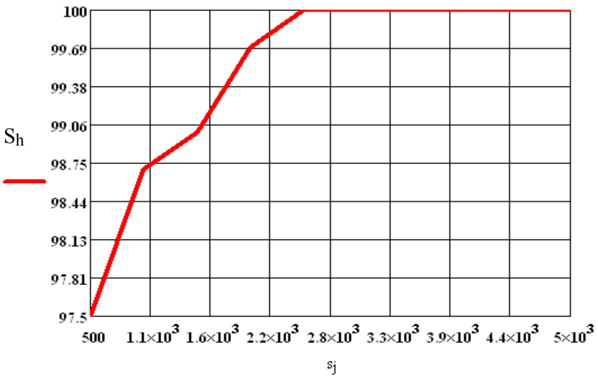


Fig. 2. Dependence of the accuracy of the result correspondence to the reference



S_j- GA stop criterion;

Sh- average correspondence of the result to the reference (%).

Fig. 3. Dependence of the average calculation time (T_a) on the probability of mutation (f_a)

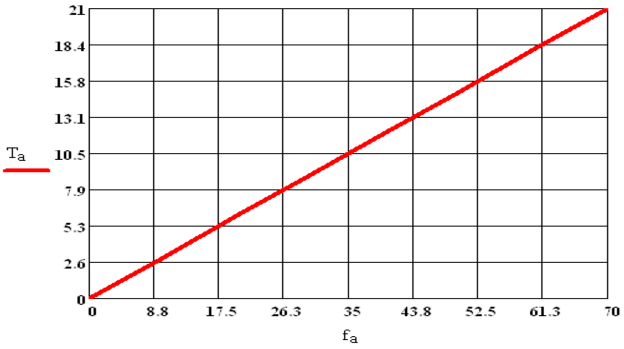


Fig. 4. Dependence of the average calculation time (V_c) on the size of the population (v_c)

6. Discussion of the results of the computational experiment

In the course of computational experiments, the following was established. A sufficient level of accuracy is achieved if the objective function values do not improve within approximately 20,000 generations. This is due to the fact that the population has already reached an absolute minimum, as illustrated in Figure 2. In the course of computational experiments, the following were changed programmatically: the probability of mutation (f_a), population size (v_c), the number of descendants, etc. As mentioned above, for each value, the calculation was carried out 10 times. Conclusions regarding a specific setting of the GA were made on the basis of the average value of the calculation time. Figure 3, respectively, shows the dependence of the average calculation time (T_a) on the probability of mutation (f_a). And figure 4 shows the dependence of the average calculation time (V_c) on the population size (v_c). During the experiments, it was also found that changing other settings does not have any significant effect on the patterns obtained and their stability. The optimization of the settings performed in the course of computational experiments made it possible to obtain the following results:

1) GA works stably when the probability of mutation is $f_a \approx 20\%$;

2) GA showed good results if the population size is about $v_c \approx 30$.

The results obtained during the computational experiments allow us to conclude that the values obtained in the calculations based on the proposed GA model are fully consistent with the results that are determined in the process of direct enumeration of all variants of the information security system for a distributed computer network of the IEEU. At the same time, the time spent is much less. This is confirmed by the results of similar works in this direction, for example, [32]. As in any variation, the GA allows to find only an approximately optimal solution. This is achieved by consistently improving current results. To complete the calculations in accordance with the proposed GA, its operation may stop if the specified number of past generations is reached. Or, as an alternative, you can use the so-called failed generations, the latter, in fact, are "areas" for which the value of the objective function is not observed for a significant number of options for the composition of the IST.

7. Acknowledgements

The study is funded by the Kazakh National Pedagogical University named after Abai (contract No. PPS-DN-01 dated 12.02.2020) & AP08855887-OT-20 "Development of an intelligent decision support system in the process of investing in cyber security systems."

8. Conclusions

The following main results are obtained in this work. The effectiveness of GA application in the course of searching for the optimal composition of the IST for IEEU is shown. An optimization model for choosing the structure and composition of the IST for IEEU nodes has been developed. The model made it possible to refine the target function based on minimizing the costs of creating an information security system for IEEU. The corresponding computational experiments were carried out, which confirmed the efficiency of the model. The practical significance of the conducted research lies in the fact that the proposed approach significantly reduces the time for calculating the optimal composition of the IST for IEEU and allows to quickly respond to a changing landscape of cybernetic threats. This, in turn, will lead to an improvement in their technical and economic indicators of the IS IEEU, reduce time and labor costs for designing an effective IS system.

References

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

[2] Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. *South African Journal of Information Management*, *23*(1), 1-11.

[3] Yulianto S., Lim C., Soewito B. Information security maturity model: A best practice driven approach to PCI DSS compliance //2016 IEEE Region 10 Symposium (TENSYMP). – IEEE, 2016. – C. 65-70. (2016) DOI: 10.1109 / TENCONSpring.2016.7519379

[4] Akdeniz E., Bagriyanik M. A knowledge based decision support algorithm for power transmission system vulnerability impact reduction //International Journal of Electrical Power & Energy Systems. – 2016. – T. 78. – C. 436-444. (2016)

[5] Schneider, Fred B. "Cybersecurity education in universities." IEEE Security & Privacy 11.4 (2013): 3-4. DOI DOI: 10.1109/MSP.2013.84

[6] Kim A. C., Lee S. M., Lee D. H. Compliance risk assessment measures of financial information security using system dynamics //International Journal of Security and Its Applications. – 2012. – Т. 6. – №. 4. – С. 191-200. (2012)

[7] Fazlida M. R., Said J. Information security: Risk, governance and implementation setback //Procedia Economics and Finance. – 2015. – Т. 28. – С. 243-248. (2015) DOI https://doi.org/10.1016/S2212-5671(15)01106-5

[8] Joshi C., Singh U. K. Information security risks management framework–A step towards mitigating security risks in university network //Journal of Information Security and Applications. – 2017. – Т. 35. – С. 128-137. (2017) DOI https://doi.org/10.1016/j.jisa.2017.06.006

[9] Bergström E., Lundgren M., Ericson Å. M. Revisiting information security risk management challenges: a practice perspective //Information and Computer Security. – 2019. – Т. 27. – №. 3. – С. 358-372. (2019) DOI https://doi.org/10.1108/ICS-09-2018-0106

[10] Chhetri S. R. et al. Security trends and advances in manufacturing systems in the era of industry 4.0 //2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD). – IEEE, 2017. – С. 1039-1046. (2017) DOI: 10.1109 / ICCAD.2017.8203896

[11] Vaseashta A. Roadmapping the Future in Defense and Security: Innovations in Technology Using Multidisciplinary Convergence //Advanced Nanotechnologies for Detection and Defence against CBRN Agents. – Springer, Dordrecht, 2018. – С. 3-14. (2018) DOI https://doi.org/10.1007/978-94-024-1298-7_1

[12] Schatz D., Bashroush R. Economic valuation for information security investment: a systematic literature review //Information Systems Frontiers. – 2017. – Т. 19. – №. 5. – С. 1205-1228. (2017) DOI https://doi.org/10.1007/s10796-016-9648-8

[13] Filimonova L. A., Skvortsova N. K. On issue of algorithm forming for assessing investment attractiveness of region through its technospheric security //IOP Conference Series: Materials Science and Engineering. – IOP Publishing, 2017. – Т. 262. – №. 1. – С. 012196. (2017) DOI:10.1088/1757-899X/262/1/012196

[14] Gordon L. A. et al. The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities //Journal of Accounting and Public Policy. – 2006. – Т. 25. – №. 5. – С. 503-530. (2006) DOI https://doi.org/10.1016/j.jaccpubpol.2006.07.005

[15] Gordon L. A., Loeb M. P., Lucyshyn W. Sharing information on computer systems security: An economic analysis //Journal of Accounting and Public Policy. – 2003. – Т. 22. – №. 6. – С. 461-485. (2003) DOI https://doi.org/10.1016/j.jaccpubpol.2003.09.001

[16] Qin W., Jianming Z. H. U. Research on the game of information security investment based on the Gordon-Loeb model //Journal on Communications. – 2018. – Т. 39. – №. 2. – С. 174. (2018) DOI: 10.11959 / j.issn.1000-436x.2018027

[17] Li X. Decision making of optimal investment in information security for complementary enterprises based on game theory //Technology Analysis & Strategic Management. – 2020. – С. 1-15. (2020) DOI https://doi.org/10.1080/09537325.2020.1841158

[18] Weishäupl E., Yasasin E., Schryen G. Information security investments: An exploratory multiple case study on decision-making, evaluation and learning //Computers & Security. – 2018. – Т. 77. – С. 807-823. (2016) DOI https://doi.org/10.1016/j.cose.2018.02.001

[19] Rees, Loren Paul, et al. "Decision support for cybersecurity risk planning." Decision Support Systems 51.3 (2011): 493-505.

[20] Fu Y., Zhu J., Gao S. CPS information security risk evaluation system based on Petri net //2017 IEEE Second International Conference on Data Science in Cyberspace (DSC). – IEEE, 2017. – С. 541-548. (2017) DOI: 10.1109 / DSC.2017.65

[21] Diesch R., Pfaff M., Krcmar H. A comprehensive model of information security factors for decision-makers //Computers & Security. – 2020. – Т. 92. – С. 101747. (2020) DOI https://doi.org/10.1016/j.cose.2020.101747

[22] Haqaf H., Koyuncu M. Understanding key skills for information security managers //International Journal of Information Management. – 2018. – Т. 43. – С. 165-172. (2018) DOI: 10.1016 / j.ijinfomgt.2018.07.013

[23] Silva M. M. et al. A multidimensional approach to information security risk management using FMEA and fuzzy theory //International Journal of Information Management. – 2014. – Т. 34. – №. 6. – С. 733-740. https://doi.org/10.1016/j.ijinfomgt.2014.07.005

[24] N. S., Von Solms R. An information security knowledge sharing model in organizations //Computers in Human Behavior. – 2016. – Т. 57. – С. 442-451. https://doi.org/10.1016/j.chb.2015.12.037

[25] Kosutic, Dejan, and Federico Pigni. "Cybersecurity: investing for competitive outcomes." Journal of Business Strategy 43.1 (2020): 28-36.

[26] Dor D., Elovici Y. A model of the information security investment decision-making process //Computers & security. – 2016. – Т. 63. – С. 1-13. (2016) DOI: 10.1016 / j.cos.2016.09.006

[27] Lakhno, V., Malyukov, V., Akhmetov, B., Kasatkin, D., & Plyska, L. (2021). Development of a model for choosing strategies for investing in information security. *Eastern-European Journal of Enterprise Technologies*, *2*(3), 110.

[28] Rahimunnisa, K. "Hybrdized genetic-simulated annealing algorithm for performance optimization in wireless adhoc network." Journal of Soft Computing Paradigm (JSCP) 1.01 (2019): 1-13.

[29] Viduto, Valentina, et al. "A multi-objective genetic algorithm for minimizing network security risk and cost." 2012 International Conference on High Performance Computing & Simulation (HPCS). IEEE, 2012. DOI: 10.1109/HPCSim.2012.6266959

[30] Olad'ko V.S. Model' vybora racional'nogo sostava sredstv zashchity v sisteme elektronnoj kommercii // Voprosy kiberbezopasnosti. 2016. № 1. S. 17–23.

[31] Prokushev, YA. E., Ponomarenko, S. V., & Ponomarenko, S. A. (2021). Modelirovanie processov proektirovaniya sistem zashchity informacii v gosudarstvennyh informacionnyh sistemah. Computational nanotechnology, (1), 26-37.

[32] Al-Matari, Osamah M., et al. "Cybersecurity tools for IS auditing." 2018 Sixth International Conference on Enterprise Systems (ES). IEEE, 2018. DOI: 10.1109/ES.2018.00040

[33] Vivekanandam, B. "Design an Adaptive Hybrid Approach for Genetic Algorithm to Detect Effective Malware Detection in Android Division." Journal of ubiquitous computing and communication technologies 3.2 (2021): 135-149. DOI 10.36548/jucct.2021.2.006