Applied Mathematics and Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/190318

Using the Object Perimeters in MGA Algorithms for the Best Choice of Cybernetic Security Means

Berik Akhmetov[1], *Lyazzat Atymtayeva*[2], *Valery Lakhno*[3], *Bakhytzhan Akhmetov*[4], *and Bagdat Yagaliyeva* [5,*]

[1] Department of Computer Science, Yessenov University, 130000 Aktau, Kazakhstan
[2] Department of Information Systems, SDU University, 040000 Kaskelen, Kazakhstan
[3] Department of Computer Systems and Networks, National University of Life and Environmental Sciences of Ukraine, 03041 Kyiv, Ukraine
[4] Department of Informatics and Informatization of Education, Abay University, Almaty 050010, Kazakhstan
[5] Department of Cybersecurity, Information Processing and Storage, Satbayev University, Almaty 050000, Kazakhstan

Received: 2 Dec. 2024, Revised: 22 Feb. 2025, Accepted: 10 Mar. 2025
Published online: 1 May 2025

Abstract: Often, we encounter with the difficulties when constructing multi-circuit integrated information security systems (IISS). The reason is necessity to formalize the procedure for selecting the optimal configuration of information security (IS) hardware and software devices (HSD) in the purposes for protection the informatization object (OBI). The list of problems to be solved also includes the procedure for generating an optimality criterion in the course of choosing a specific information security tool (IST) in the OBI security contours. The selected IST must be adequate in relation to the general design goals of the IISS for IOB. The task of choosing the optimal design alternative with the available set of acceptable options also has its own difficulties, for example, according to the technical and economic indicators of the IST. This paper introduces the author's vision of the process for generating the optimality criterion when choosing specific IST for the OBI multi-circuit protection system. In contrast to the existing solutions, we propose the implementation of the information security options ranking by individual indicators. For making decision we use the generalized evaluation function. It is obtained as a result of the summation of the ranks for the considered IST. We propose a modified genetic algorithm (MGA), that allows flexible changes in the search procedure for suitable IST, depending on the history of search. This provides a compromise between the speed of the locally optimal solution and its quality. We describe a software product for the implementation of the proposed model and the MGA for the choice of IST.

Keywords: distributed computing system, information security, optimization, genetic algorithm

1 Introduction

The constant increase in the list of tasks that information security tools (IST) have to solve as a part of multi-circuit systems of information security (MCIS) causes a high complexity of the task design. It becomes complicative due to the increase of the requirements imposed on them in the context of the growing complexity of cyberattack scenarios. This complexity is associated with the need to work out in detail and subsequently optimize the composition for all components of the integrated information security system (IISS) on the corresponding informatization object (OBI).

The set of different factors such as the heterogeneity of the physical principles on the basis of which the majority of hardware and software devices (HSD) as a parts of IISS, have been implemented, a large number of possible options for implementing the structures of each individual IST, the multivariance of methods for combining means and measures to protect information into a holistic multifunctional IISS, leads to the fact that that the problem analysis in a given subject area can be attributed to a rather laborious design task.

The problem of high dimension in relation to the design problem of the IISS concerns the entire set of considered alternatives in the design process. This, in particular, can be attributed the following: many ways and

* Corresponding author e-mail: bagdat.yagaliyeva@gmail.com

means by which the tasks of ensuring IS of OBI are solved; many economic, technological, technical and other restrictions that affect the choice of certain measures and means of protection.

Implemented in many specific situations, a modular approach to the creation of IISS for large OBI based on the combination of sets of IS compatible HSD, significantly increases the number of possible options for analysis.

We can distinguish the following basic approaches with regard to the selection and application of specific analytical methods in the process of solving optimization problems in the construction of MCIS. The first group is based on exact methods for solving optimization problems. For example, cutting-off methods are widely used. The second group includes methods of partial enumeration. Finally, the third group contains of the methods for global random search. The latter group also includes genetic algorithms (GA), which can speed up the procedure for solving a problem.

This paper describes an integrated approach used by the authors in the process of problem solving for the formation a set of information security tools for MCIS.

The proposed approach is based on a combination of techniques for the formation of admissible IST option sets for the OBI distributed computing system, including the principles of heuristic optimization. At the same time, heuristic optimization is performed on the basis of evolutionary programming with help of GA algorithms, that allows us to provide an acceptable time and quality of the task solution.

2 Literature review

The problem to be solved belongs to multi-criteria and multi-extreme [1],[2]. That is why, to solve it, the possibility of applying GA is considered to be less laborious and fast in work. The latter circumstance is important if you are required to dynamically reconfigure information security tools along the information security contours, for example, when identifying targeted attacks on an informatization object. That is, just in a situation where it is required to concentrate fixed assets to protect critical information assets of IOB.

In works [3],[4], the use of GA to solve these problems is substantiated.

In works [5],[6], the features of using GA in the problem of choosing equipment for IOB cyber security circuits are analyzed in detail. However, the solution proposed by the authors is essentially a combination of GA and standard greedy algorithms.

It is quite difficult to unambiguously algorithmize the effectiveness of the selection of the IST for multi-circuit IOB. This complexity is primarily associated with the difficulties in describing the objective function. A priori, the objective function must be multivariable. This is because it is influenced by a large number of factors, including stochastic ones, for example, the timing of a cyberattack directed at IOB information assets by attackers.

In [7], [8] it was shown that the modeling of the IOB security indicators should be carried out in relation to the IST complexes along the IOB contours. Only after that, the impact evaluation of these contours on the integral security metrics for the entire protected object is carried out.

3 Methods and models

The goal of current research is to study the feasibility and possibility of using a modified adaptive genetic algorithm (MAGA) to organize a flexible search procedure for the suitable information security tools based on the security perimeters of an informatization object (OBI).

To achieve this goal, we are solving the following tasks:

- to develop a procedure for generating an optimality criterion when choosing specific IST for the OBI multi-circuit protection system;
- to modify the GA based on the need to achieve a compromise between the speed of a locally optimal solution and its quality when selecting IST for a specific circuit;
- to describe the software product for the implementation of the proposed MAGA, used in the selection of IST.

In the process of solving the problem, we will put in accordance with each variant the distribution of the IST analyzed for the IS contour. For example, for the centralized organization of information protection contours, see Fig. 1 and 2, the vector, looks as follows:

$$V_j = [v_k^j]_{1\times H}, \quad j = 1,2,\ldots,M, \quad inlengthH = \sum_{i=1}^{N} h_i \text{ bits.} \tag{1}$$

where m_i – IST in the corresponding $i-m$ circuits;

N-the number of IS circuits, depending on the architecture of the IOB distributed computing system;

M-the number of variants formed during the selection of the IS along the i-my circuit.

In Figure 1, numbers from 1 to 5 indicate the contours (perimeters of IS support OBI): 1 - the perimeter of information systems (IS). For example, for a distributed OBI architecture, each IS will have its own perimeter; 2 - OBI control perimeter; 3 - user access perimeter; 4 - perimeter of network equipment; 5 - OBI outer perimeter.

The distribution options are encoded based on a binary alphabet according to conditions (2):

$$v_k^j = \begin{cases} 1, & \text{if included in the IS circuit;} \\ 0, & \text{otherwise.} \end{cases} \tag{2}$$

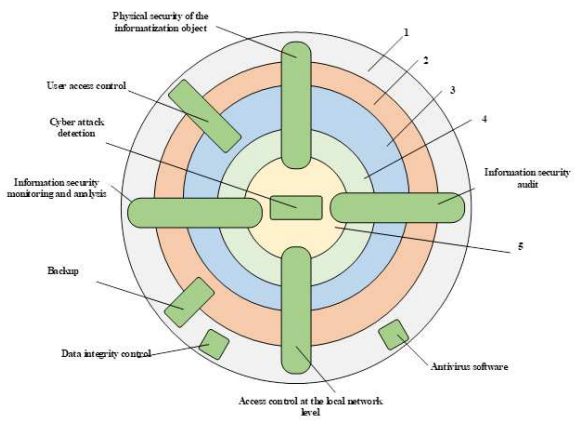

Fig. 1: Conceptual layout diagram of an information security tools for a centralized version of organizing information security of an informatization object

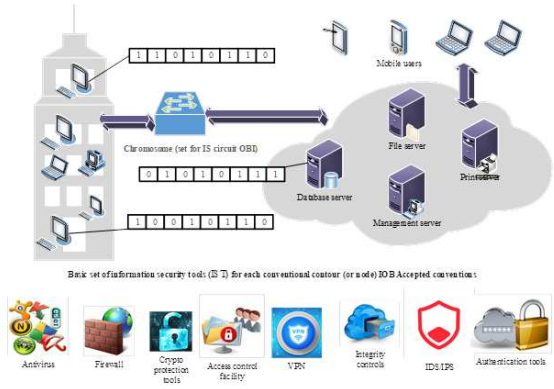

Fig. 2: The infrastructure of the IOB conditional contour from the point of view of ensuring information security

Limitation. It is assumed that in each fragment of the vector corresponding to the i- my contour of the IS, there must be one nonzero element.

Based on the results of the sets of possible option formation, we can select the optimal composition of the IST for the OBI IS contour. At the same time, we used a generalized criterion of effectiveness as an integral criterion for selection. It includes indicators characterizing the functionality of each selected IST, for example, as shown in Table 1.

The process of creating a functional and reliable IISS for a multicircuit OBI, among others, includes the following interrelated tasks:

1. to generate an optimality criterion (which should be adequate in relation to the design goals);
2. to choose the optimal design alternative from the set of admissible options.

Table 1: Initial data for solving the optimization problem for the IS circuit OBI

IST number	**1**	**2**	**3**	**4**	**5**	**6**
IST type	IC	CP	ID	CA	AC	VPN
Cost (units)	5.0	7.0	8.0	6.0	4.0	1.0
Integral indicator (based on www.anti-malware.ru)	2	3	4	3	2	1
The following reductions in information security tools have been adopted: CP - cryptographic protection; AC - access control; CA - authentication; IC - integrity control; ID - Intrusion Detection.						

When solving such a multi-criteria optimization problem, the final goal leaves its imprint on the selection principles - building a reliable and functional IISS.

At the same time, we need to consider the designing of IISS on the base of a sufficiently large number of private indicators or information security metrics. These particular indicators allow using all the signs that adequately reflect the results obtained in the design of OBI for multi-circuit IS system.

In addition, it is necessary to ensure the ranking of the selected options for IS contours. This can be done, for example, by taking as a basis the degree of preference for one or another information security system. And then we can make it correspondent to a specific quantitative measure of efficiency. For antivirus software, this may be the percentage (in %) of malware detected.

It should be noted that the application of assessment based on the vector criterion (1) is subjective. Indeed, some of the ISS options analyzed during the design process for a multi-circuit IS system (or IISS) may turn out to be more preferable if some indicators are taken as estimates (for example, software for managing and accessing IS risks) and less preferable for others (for example, hardware - software tools for tracking vulnerabilities).

In the works [9,10], the application of the main axiom for evaluating the information security system for OBI multi-circuit IS systems is substantiated by several indicators. Moreover, in [9, 11] authors proved that it is impossible to show mathematically the existence of the most preferable option. And, therefore, any option from the list of less preferred can be recognized as the most preferable for specific conditions.

In order to accept the resulting estimates as reasonable in the design of a multi-circuit IS system, it is necessary to develop a decision rule. Moreover, this rule should facilitate selection in relation to the volume of reliable data characterizing the properties of the evaluation functions.

Also, the analysis of previous studies suggests that this rule defines the least subjective approach to the selection of IST for the analyzed IS circuit. The options should be ranked for each of the considered characteristics of the IST included in the IS circuit OBI. Then the scoring function can be defined as a sum of all the ranks. For example, let's consider this rule for three local indicators of the IST:

1.the cost of acquisition, installation and operation – (ST);
2.the type of IST (indicates the principles of operation of elements of IST, for example, a frequency scanner) – (TYPE);
3.the expert assessment of work efficiency – (EXP).

All values can be accepted in points.

Then the resulting characteristics for each IST option considered as a "candidate" for the OBI IS contour will be determined as a sum (SUM) of indicators (ST), (TYPE) and (EXP) for the next option

$$\text{SUM\_ST}_j = \sum_{k=1}^{H^2} ST_k \times v_k^{j^2} \mid v_k^j \in V_j; \quad (3)$$

$$\text{SUM\_TYPE}_j = \sum_{k=1}^{H^2} TYPE_k \times v_k^{j^2} \mid v_k^j \in V_j; \quad (4)$$

$$\text{SUM\_EX}_j = \sum_{k=1}^{H^2} EX_k \times v_k^{j^2} \mid v_k^j \in V_j; \quad (5)$$

Further, in accordance with the obtained values SUM_ST_j, SUM_TYPE_j, and SUM_EX_j for each variant of the set of SIS contour, we assign a rank to it. The rank is assigned as a natural number; for example, as shown in Table 2.

The highest rank is assigned to the best IST, based on the evaluation function results. The last column of **Table 2** contains the total rank (SUM_RANG) for the IST option.

Table 2: General view of the table with the sum of the ranks by the indicators of the IST for the IS circuit

# SIS	SUM_ST_j	SUM_TYPE_j	SUM_EX_j	SUM_RANG
1	meaning	meaning	meaning	meaning
...	...	...	...	...

By evaluating the different solutions of the problem we discovered the fact that generalized ranks, which are involved in the process of choosing the IST for the OBI IS contours , allow us going directly to the procedures for selecting the optimal alternatives to IST project.

For making a search of optimal variant we propose the implementation of the modified adaptive genetic algorithm (MAGA) . This imparting of adaptability properties to the genetic algorithm (GA) allows us increasing the efficiency of the procedures implementation for finding a solution.

First, this can be achieved due to the properties of self-learning and adaptation. Moreover, the adaptability of the GA allows to eliminate some GA contradictions. The contradiction is that as the GA convergence rate increases, the probability of obtaining a local optimal solution also increases [7]. The introduction of adaptability properties into the GA allows more flexible adjusting the GA parameters. This setting helps to ensure the optimal convergence rate. And this, in turn, guarantees the acceptable quality of the resulting solution.

Let us consider the variant of GA (MAGA) adaptation to solve the problem of finding the optimal composition of the IST for the OBI IS circuits or, in other words, on the formation of OBI IST as a whole.

At each step, the Genetic Algorithm (GA) analyzes the population, which consists of a set of chromosomes (vectors V_j). Thus, the population can be written as follows:

$$\text{Gen}(p) = \{V_1(p), V_2(p), \ldots, V_M(p)\} \quad (6)$$

The function of suitability (FS) can be the total rank for each of the considered options of the OBI IST for the IS circuit (or IISS).

Note that the FS values for the same variants of different populations differ. This is due to the following circumstance. The value of the objective function of the corresponding option will be determined not only by its own elements of the IST set for the contour, but also by the IST sets in adjacent contours, see Fig. 1. And besides, the evaluation functions for the analyzed IST can also have an impact.

The composition of the initial population Gen(0) was formed on the basis of a stochastic sample. In this case, we take into account the following. Not all possible chromosome variants are valid for a population. The admissibility is determined based on the fact that in each section of the bit string (which corresponds to the selected IST for the contour), there is only one element other than "0". In the composition of each option, we include no more than one IST from the same type of hardware and software devices of the IS or measures to protect information.

We can form the subsequent populations on the basis that during transitions between populations, the average value of its constituent chromosomes (vectors V_j) is increasing. For that, it is necessary to implement the so-called *Elite selection*. Namely, for each new population $\text{Gen}(p+1)$, we place a "representative" of the population $\text{Gen}(p)$. Moreover, this "representative" must have the maximum rank. This corresponds to an operation like this:

$$\text{insert}\Big(\text{Gen}_{ev}(p+1), S_j \mid \text{SUM\_RANG}_j = \max(SUM\_RANG_j)\Big) \quad (7)$$

Note that the ratio of the stored vectors from the past population and new vectors that are formed during the involvement of genetic operators is regulated by the so-called *novelty coefficient* $-\mu$.

The following values are valid for the novelty coefficient:

$$\mu = \begin{cases} < 1, & \text{Overlapping: Elite Gen}(p) \text{ preserved;} \\ = 1, & \text{Non-overlapping: Fully renewed.} \end{cases} \quad (8)$$

In relation to those representatives of the population who remained after the previous screening by the coefficient of novelty, we carry out the operations of crossing over and mutation. Crossover will enable the adaptation of the GA parameters to be used. At the same time, as it was mentioned earlier, for GA it is important to achieve a compromise between the rate of convergence of the algorithm and the quality of the solution (for the situation of a locally optimal solution).

The essence of the adaptation mechanism proposed in this paper can be expressed as follows. The probability of selecting $p(V_i)$ individuals must be flexible. Flexibility depends on the history of finding a locally optimal solution. For this, we apply the normal law of the probability distribution of selection. The mathematical expectation was determined as follows:

$$MO = \max\left(\text{SUM\_RUNG}_j\right) \quad (9)$$

If the best chromosome changes in the next generation, then the variance value will be maximum. This allows us to expand the search range for the problem solution. If we have a situation when for several generations the preferred chromosome does not appear, then the value of the variance will be decreased. In the simplest situation, the following expression may happen:

$$D = D_{\max} \quad (10)$$

where ψ is the coefficient that determines the rate of convergence of the GA; w is the number of "unsuccessful" generations. The implementation of the crossover operation involves the selection of parent individuals $V_{C1}(p) = \text{GET}(\text{Gen}(p))$ and $V_{C2}(p) = \text{GET}(\text{Gen}(p))$. After that, we find the resulting chromosome:

$$V_C(p) = \text{Cross}\left(V_{C1}(p), V_{C2}(p)\right) \quad (11)$$

The specificity for this optimization problem affects the ways of implementing crossing over.

In order to provide the functionality of the IST set in the OBI IS circuit and to preserve the composition of the equipment characteristic of a number of specific functions (for example, monitoring of all processes in OBI information systems), it is necessary to fulfill the following condition.

A break in parental chromosomes can be made only at the points of their division into genes. And the genes should be corresponded to different types of IST along the OBI contours.

Accepted condition.

However, a more flexible option would be the selection of multiple interruption points and then implementation of multipoint crossover operation. The number of multipoint crossover cycles can affect the range of the solution search. And since a priori the diversity of chromosomes will be increased, then, accordingly, it is possible to find more perfect options for the compatibility of different types of IST along the IISS OBI contours, even if the search procedure will be delayed. And this is not always acceptable in a dynamic confrontation with the side of the OBI attacking .

After crossover, we apply the mutation operator to the remaining chromosomes. In this task, it is unacceptable to use the classical mutation scheme. Due to this factor, we perform the mutation operation for the entire gene, and not with respect to a single bit. The gene contains more extensive information regarding the IST in each circuit. The chromosomes of descendants obtained after crossover and mutation will be randomly selected for the next generation. Chromosomes are selected from the expanded population. This population was previously replenished with new representatives at the last step of the algorithm. These new representatives were descendants, which were formed as a result of the implementation of crossover operations, and mutated chromosomes.

Initially, all members of the extended populations are recalculated for the fitness function. Next, adaptive selection is performed according to the expression (12):

$$\text{insert}\left(\text{Gen}_{ev}(p+1), V_C, V_H\right) \quad (12)$$

All new offspring are checked for the condition of avoiding the situation, so that the same individuals appear in the new population:

$$\text{insert}\big(\text{Gen}_{ev}(p+1), V_C, V_H \mid V_C, V_H \neq V_j, \; V_j \in \text{Gen}_{ev}(p+1)\big) \quad (13)$$

The adaptation mechanism used in the modified GA (MGA) allows us substantiating logically the criterion for stopping the search. Thus, the search will be terminated if the value (variance) decreases to a certain value. As such a threshold value for stopping the search, we can take a value of the probability of change according to the best of the found IST options for the corresponding contour. (see Fig. 1). Thus, this probability should be negligible.

Based on the assumption that the fitness function takes only integer values, it will be fair to assume that as a result of the selection, the best version of the IST for the OBI IS circuit will be formed. Then the search for a solution ceases to be random. It makes no sense to continue further work of the MAGA.

After all the procedures related to the optimization of the OBI contours are completed, the bits of the resulting chromosome will contain encoded data on the optimal version of the IST set for a particular IISS circuit.

4 Computational experiments

To check the main provisions outlined in the framework of this study, we developed a console application that implements the proposed modified adaptive GA for selecting an IST for OBI IS loops. Thus, for the formation of the OBI IISS, we created the console application in the algorithmic language C# using the Visual Studio 2019 programming environment (see Fig. 3).

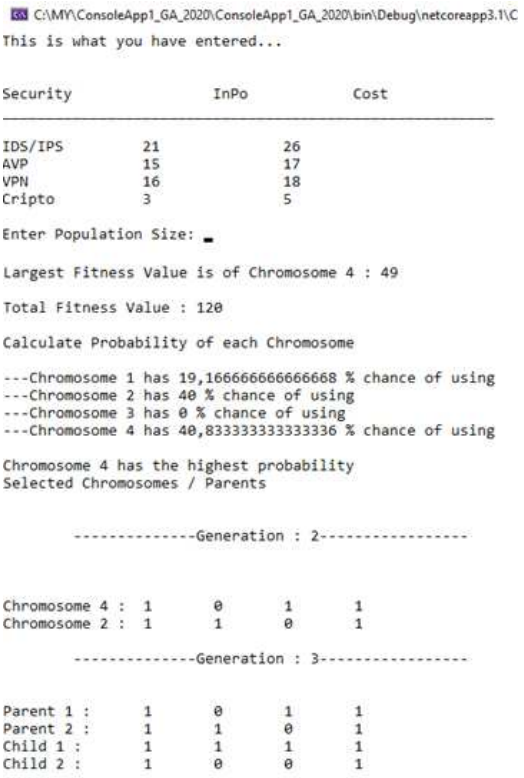

Fig. 3: General view of the console application for the modified adaptive GA, which implements the selection of the IST for the IS IOB contours

With the help of this console application we investigated the expedient number of cycles during the crossover operation. See Fig. 4 for results. We also provided a study to determine the number of generations required in order to complete the search for the optimal options for IST for the analyzed circuit (see Fig. 5).

5 Discussion of the results of computational experiments

Thus, in the process of computational experiments, we confirmed the following:

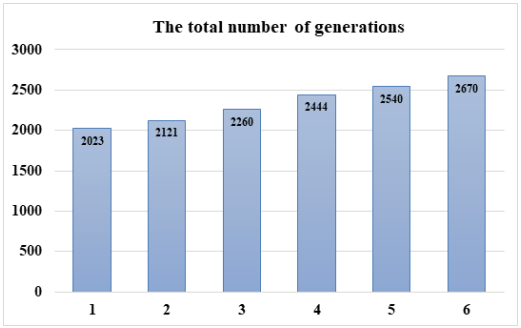

Fig. 4: The results of the study of the appropriate number of cycles during the crossover operation

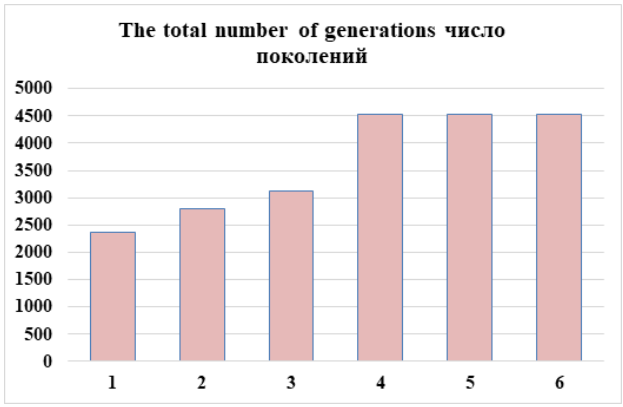

Fig. 5: Results of a study to determine the number of generations required in order to complete the search for optimal options for IST for the analyzed circuit

1.in relation to this optimization problem, to achieve a solution, the crossover operation should be performed once, see Fig. 4.
2.The best results were obtained for single mutations in relation to each generation, see Fig. 5.

Taking into account the previous studies [4–6, 12–19], the analysis of the requirements, which are usually drawn up by the customer when forming the technical specifications for the OBI IISS, allows you to generate a variety of acceptable IST options for protection contours. Accordingly, for each of the contours of the conceptual layout diagram of the information security system for the centralized version of the IOB IS organization, it is possible to quickly select compatible hardware and software protection means.

As a disadvantage of the approach considered within the framework of this article, it can be noted that the creation of IISS gives rise to a number of difficulties. These difficulties are associated, first of all, with the need to clearly formalize the procedure for selecting IST for a circuit, based on the criticality of information arrays that are actually subject to protection.

Also, a number of these difficulties can be attributed to the complexity of formalizing the procedure for generating the optimality criterion.

However, the approach outlined in this work, due to the ranking of options for each of the indicators of the IST, allows us to somehow solve these issues. First, this becomes possible if we take the value of the sum of ranks as a generalized evaluation function. The second, we make a choice of the specific IST for a specific circuit strictly in accordance with the available reliable information about the properties of the estimated functions involved in the GA.

6 Conclusion

The analysis of the typical requirements that customers impose on hardware and software security devices (HSD) included in integrated information security systems (IISS) has made it possible to systematize the process of forming a set of acceptable configurations for IISS in distributed computer systems of informatization objects (OBI). The study revealed that when designing multi-circuit IISS, significant difficulties arise due to the need to formalize the procedure for selecting the optimal HSD configuration from the available set of possible options. This complexity is driven by the fact that OBI protection must strictly comply with established security requirements while also considering technical, organizational, and economic factors that influence the effectiveness of the security system.

One of the key problems to be addressed is the development of a method for generating an optimality criterion when selecting a specific HSD for implementing security loops within OBI. Defining this criterion is challenging due to the diverse requirements imposed on IISS, as well as the need to consider multiple parameters, including reliability, performance, implementation costs, and operational characteristics of the chosen solution. Moreover, special attention must be given to ensuring that the selected security measures align with the overall design goals of the OBI information security system. This implies that the selection process should be highly adaptive and take into account both current and future security requirements.

Another significant challenge lies in selecting the best design alternative from a set of available options, which may differ in terms of technical and economic indicators. It is necessary to consider not only the basic characteristics of the HSD but also its potential effectiveness within a multi-level security system. Such an approach will enable the development of a balanced strategy for ensuring information security, taking into account potential threats, system resources, and regulatory requirements.

This paper presents the author's vision of the process of forming an optimality criterion when selecting specific HSDs for OBI multi-circuit protection systems. It is proposed to implement a ranking method for different IISS options based on individual performance indicators that characterize their effectiveness and compliance with established requirements. To facilitate decision-making, a generalized evaluation function is introduced, which is calculated by summing the ranks of the considered HSD options. This approach allows for a comprehensive analysis of available security solutions and helps select the most appropriate option based on a combination of criteria.

The research focuses on the use of modified adaptive genetic algorithms (MAGA), which provide a flexible approach to adjusting the search process for optimal solutions based on accumulated knowledge from previous search iterations. This methodology offers a balance between the speed of obtaining a locally optimal solution and its overall quality. By employing MAGA, the selection system for the optimal HSD configuration becomes more adaptive and efficient, ultimately enhancing the security level of distributed computer systems.

Thus, the proposed approach significantly improves the quality of the HSD selection process, making it more transparent, manageable, and aligned with current security requirements. The results of this study can be applied in the development of methodologies for IISS design, as well as in the creation of automated decision support systems for information security management.

7 Acknowledgement

The authors express their sincere gratitude to the Ministry of Education and Science of the Republic of Kazakhstan and Universities for their invaluable support. This research was made possible through funding from grant number AP08855887 – Development of an intelligent decision support system in the process of investing in cybernetic security systems. The financial assistance provided has greatly contributed to the advancement of this study, enabling an in-depth exploration of innovative approaches to information security. The authors deeply appreciate this support, which has played a crucial role in the successful completion of this research.

References

[1] Stepanov, L. V., Parinov, A. V., Korotkikh, L. P., & Koltsov, A. S., *Approach to estimation of level of information security at enterprise based on genetic algorithm,* In Journal of Physics: Conference Series, (2018, May) (Vol. 1015, No. 3, p. 032141). IOP Publishing.

[2] Pandey, H. M., *Performance evaluation of selection methods of genetic algorithm and network security concerns* Procedia Computer Science, (2016). 78, 13-18.

[3] Kumar, A., & Ghose, M. K., *Overview of information security using genetic algorithm and chaos,* Information

Security Journal: A Global Perspective. (2009), 18(6), 306-315.
[4] Tamjidyamcholo, A., & Al-Dabbagh, R. D., *Genetic algorithm approach for risk reduction of information security,* International Journal of Cyber-Security and Digital Forensics (IJCSDF), (2012). 1(1), 59-66.
[5] Banković, Z., Stepanović, D., Bojanić, S., and Nieto-Taladriz, O., *Improving network security using genetic algorithm approach,* Computers and Electrical Engineering, (2007). 33(5-6), 438-451.
[6] Gupta, M., Rees, J., Chaturvedi, A., and Chi, J., *Matching information security vulnerabilities to organizational security profiles: a genetic algorithm approach* Decision Support Systems, (2006). 41(3), 592-603.
[7] Leoshchenko, S., Oliinyk, A. O., Skrupsky, S., Subbotin, S., and Zaiko, T. *Parallel Method of Neural Network Synthesis Based on a Modified Genetic Algorithm Application,* (2019). In MoMLeT (pp. 11-23).
[8] Tamjidyamcholo, A., and Al-Dabbagh, R. D. *Genetic algorithm approach for risk reduction of information security* International Journal of Cyber-Security and Digital Forensics (IJCSDF), (2012). 1(1), 59-66.
[9] Marukhlenko, A. L., Plugatarev, A. V., & Bobyntsev, D. O., *Complex evaluation of information security of an object with the application of a mathematical model for calculation of risk indicators* In International Russian Automation Conference (pp. 771-778), (2019). Springer, Cham.
[10] Klyaus, T. K., & Gatchin, Y. A., *Mathematical model for information security system effectiveness evaluation against advanced persistent threat attacks* In 2020 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF), (2020). (pp. 1-5). IEEE.
[11] Korniyenko, B. Y., & Galata, L. P., *Design and research of mathematical model for information security system in computer network* Science-intensive technologies, (2017). (2), 114-118.
[12] Lakhno, V., Akhmetov, B., Adilzhanova, S., Blozva, A., Svitlana, R., Dmytro, R., *The use of a genetic algorithm in the problem of distribution of information security organizational and financial resources* , ATIT 2020 - Proceedings: 2020 2nd IEEE International Conference on Advanced Trends in Information Theory, (2020). article No. 9349310, pp. 251-254.
[13] 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* In: Silhavy R. (eds) Informatics and Cybernetics in Intelligent Systems. CSOC 2021. Lecture Notes in Networks and Systems, (2021). vol 228. Springer, Cham.
[14] Vakilinia, I., Louis, S. J., & Sengupta, S., *Evolving sharing strategies in cybersecurity information exchange framework* In Proceedings of the Genetic and Evolutionary Computation Conference Companion, (2017). (pp. 309-310).
[15] Stepanov, L. V., Koltsov, A. S., & Parinov, A. V., *Evaluating the Cybersecurity of an Enterprise Based on a Genetic Algorithm* In International Russian Automation Conference, (2020, September). (pp. 580-590). Springer, Cham.

Berik Akhmetov received the candidate of Technical Sciences degree in Technical and Computer Science at Al-Farabi National University, Kazakhstan. Now he is working as a professor in the department of Computer Science and President of Yessenov University. His research interests are information security, cybersecurity, decision support systems in the field of information security, game theory. He has over 100 publications, of which 34 are in highly rated peer-reviewed publications. Hirsch index in scientometric base Scopus - 8.

Lyazzat Atymtayeva received the Ph.D and Doctor of Science degree in Mechanics, Mathematics and Computer Science at Al-Farabi National University, Kazakhstan. Now she is working as associate professor in Information Systems at SDU University. Her research interests are in the areas of mechanics, applied mathematics and computer science including the numerical and rigorous mathematical methods and models for mechanical engineering and computer science, intelligent and expert systems in Information Security, Artificial Intelligence and Machine Learning, Project Management and Human-Computer Interaction. She has published research papers in reputed international journals of mathematical and computer sciences. She is a reviewer and an editor of international journals in mathematics and information sciences.

Bakhytzhan Akhmetov Doctor of Technical Sciences, Professor, Academician of the National Engineering Academy of the Republic of Kazakhstan, Academician of the International Engineering Academy, Academician of the International Informatization Academy. He works as a professor at the Department of Informatics and Informatization of Abay University. His research interests are information and communication technologies, artificial intelligence, information security, cyber security, biometric-neural network technologies for information protection. He has about 400+ articles.

Valery Lakhno Doctor of Technical Sciences, Professor, Department of Computer Systems, Networks and cybersecurity, National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine. His research interests are information protection, cybersecurity, expert systems and decision support systems in the field of information security, game theory. He has over 300 publications, of which 113 are in highly rated peer-reviewed publications. H-index in scientometric base Scopus is 11.

Bagdat Yagaliyeva received the Ph.D degree in Engineer Robotics at Satbayev Technical National University, Mathematics and Physics at Al-Farabi National University, Kazakhstan. Now she is working as associate professor in department of ”Cybersecurity, information processing and storage” at Institute of Automation and Information Technologies. Her research interests are in the areas of mechanics, applied mathematics and computer science including the numerical and rigorous mathematical methods and models for mechanical engineering and computer science, intelligent and expert systems in Information Security, Artificial Intelligence and Machine Learning. She has 60 publications, 10 of them in highly rated peer-reviewed publications.