Journal of Theoretical and Applied Information Technology
15th April 2022. Vol.100. No 7


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

# MULTİ-CRİTERİAL OPTİMİZATİON COMPOSİTİON OF CYBER SECURİTY CİRCUİTS BASED ON GENETİC ALGORİTHM

**LAKHNO V.[1], AKHMETOV B.[2], MOHYLNYI H.[3], BLOZVA A.[4], CHUBAIEVSKYI V.[5], KRYVORUCHKO O.[6], DESIATKO A.[7]**

[1,4] National University of Life and Environmental Sciences of Ukraine
[2]Caspian University of Technology and Engineering named after Sh.Yessenov, Aktau, Republic of Kazakhstan
[3] Luhansk Taras Shevchenko National University, Starobilsk, Ukraine
[5,6,7] Kyiv National University of Trade and Economics, Department of Software Engineering and Cybersecurity, Kyiv, Ukraine

E-mail: [1]lva964@gmail.com, [2]lim4best@gmail.com, [3]g.mogilniy@gmail.com, [4]andriy.blozva@nubip.edu.ua, [5]chubaievskyi_vi@knute.edu.ua, [6]kryvoruchko_ev@knute.edu.ua, [7]desyatko@gmail.com

**ABSTRACT**

The article proposes a method of multicriteria optimization (MCO) of costs for an information security system (SIS) of an informatization object (OBI). The technique is based on the use of the genetic algorithm (hereinafter GA) VEGA (Vector Evaluated Genetic Algorithm). The modified algorithm for solving the problem of multicriteria optimization of the parameters of the OBI multi-loop SIS allows substantiating the rational characteristics of the DSS components, taking into account the priority cybersecurity metrics of the OBI selected by the expert. Unlike the existing classical VEGA algorithm, the modified algorithm additionally applies the Pareto principle, as well as a new selection mechanism.

**Keywords:** *İnformation Protection, Cybersecurity, Protection Circuits, Multi-Criteria Optimization, Genetic Algorithm*

## 1. INTRODUCTION

As soon as scenarios of cyberattacks on objects of informatization (OBI) become more complex, the organization of the functioning of multi-circuit information security systems (ISS) requires synchronization of the operations of all components that makes up both the entire security system as a whole and its individual components at each of the defense lines. The solution of such a complex problem requires development of new and improvement of existing algorithms describing the change in the situation with the protection of OBI, as the current situation changes.

## 2. THE PURPOSE OF THE STUDY

The purpose of the study is to develop a methodology for minimizing the costs of building a multi-circuit information security system by selecting the optimal parameters of individual cybersecurity components.

Research objectives:

1. To develop a methodology for multi-criteria optimization of costs for OBI DSS based on a genetic algorithm.
2. Adaptation of the multicriteria genetic algorithm VEGA to find the optimal values of the target functions of the information security system. We believe that the target functions of the ISS determine the relationship between the probabilistic input actions on the individual components of the OBI protection and its output parameters.

## 3. LITERATURE REVIEW

The increasing number and complexity of successfully implemented cyberattacks on various OBIs [1, 2] give rise to the need for qualitatively new procedures for forming the composition of ISS and cybersecurity (CS) complexes for all protection circuits of OBI information arrays. The problem of formation of effective contours of information security (IS) and CB OBI, which does not lose its relevance, has generated a lot of theoretical researches devoted to the optimization of the composition of the information security system and CS [3, 4, 24-28].

In such tasks, it is necessary to find admissible Pareto-optimal solutions for ISS complexes. The solution of such a problem is an integral part of the procedure for constructing multi-circuit ISS in the face of an increase in the number of attempts at destructive impacts on OBI of various scales. And the solution of such problems is carried out based on not only classical procedures of multicriteria optimization (MCO) but also on more universal methods. In particular, these methods include various variations of the genetic algorithm (GA), which has proven its effectiveness in solving a wide range of complex problems [5], [6].

Note that the efficiency of GAs depends on careful tuning and control of their parameters. The expediency of using GA is dictated by a situation in which, in addition to the traditional MCO task of choosing the composition of the information security system for OBI, various metrics are also considered for evaluating the effectiveness of the use of individual components of information protection tools along the cybersecurity contours of OBI. And besides, it is still necessary to take into account the magnitude of the risks, the cost indicators of the selected information security tools, based on the specifics of specific information assets - databases, knowledge bases, mail, website, etc.

It is shown in [7] that GAs which can be used in solving MCO problems are variations of evolutionary search methods. So, in [8], for example, a model is considered, following which a population of SZI elements (individuals) is created. To find the best solution, the authors used the target function. However, this study did not indicate how the proposed solutions are used in practice.

In [9], [10], GAs were investigated, which can be attributed to two groups. Binary coding is discussed in detail in [10], [11]. Real coding is considered in works [12], [13]. In particular, in [12], it was shown that in the first group it is possible to achieve a higher efficiency of searching for the extreme value on the set of feasible solutions.

It was shown in [14] that constant mutation of objects is used in most GA implementations. In this case, the variation of the variables will be more flexible. This makes it possible to find initial solutions already at fairly early stages of the GA operation, without a large number of its runs. However, in [12], [13], [14], the GA software implementation was not presented.

It was shown in [15], [16] that variable mutation looks preferable from the point of view of searching for the global optimum. These works also do not contain a description of the software implementation. In [17], [18], the features of using a modified GA (MGA) in MCO problems are analyzed. The difference between the MGA is that here, during the operation of the algorithm, not the sum of the ESS efficiencies was used as a fitness function, but the sum of the ratios of the efficiencies to the limiting characteristics of the ESS was used. This MGA is nothing more than a disjunction of the standard GA and the greedy algorithm.

The works [19], [20] consider the possibility of reducing the number of tunable GA parameters. The solutions proposed by the authors, in contrast to the standard ones, do not contain the crossing operator. The solution was obtained based on statistical information about the search space.

It is shown in [17], [20] that standard and modified GAs are quite effective for solving most complex optimization problems [21], [22] and are promising for further study and improvement.

All of the above has determined the relevance of our research.

## 4. MODELS AND METHODS

To solve the formulated problem, it is proposed to use a genetic algorithm.

The solution is based on the general evolutionary algorithm and its components of multicriteria GA. The main method was VEGA - Vector Evaluated Genetic Algorithm [1], [2]. The research plan in this article provides for the expansion of traditional GA. This method provides for the expansion of the traditional GA, which is implemented by using vector estimates of the degree of suitability of specimens (individuals), as well as the ability to simultaneously evaluate populations for each of the criteria separately, for example, for each of the components of the information security system, it can be - efficiency, scalability, cost, technical support. Thus, it is possible to implement the simultaneous optimization of all protection contours of the object of informatization following the specified target functions. At the initial stage of MGA operation, there are two parental chromosomes. At two randomly selected locations, gaps are made between gene positions. In Figure 1, the gaps are shown with a dash-and-dot red line. Further, there is an exchange of parts between chromosomes. As a result, two children are formed. One descendant is randomly selected from the descendants, which is passed as the result of the crossing operator. Next, we turn to the mutation operator - a random change in all descendants of the population. The purpose of the mutation is to make the individuals (specimens) analyzed in the course of solving the problem more diverse. In the course of a mutation, the scheme of which is shown in Figure 2, the genes of each specimen mutate with a certain predetermined probability. The mutated genes are

Journal of Theoretical and Applied Information Technology
15th April 2022. Vol.100. No 7

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

shown in Figure 2 as cells with light green shading. That is, during the mutation, the value of a bit in a cell changed to the opposite. So in the first cell from "0" to "1". In the second, from "1" to "0". Next, we form a new generation from an array of parents and educated descendants. During the formation of the new generation, both parents and descendants were used, already known [19], [21] values of the fitness function, see fig. 3.

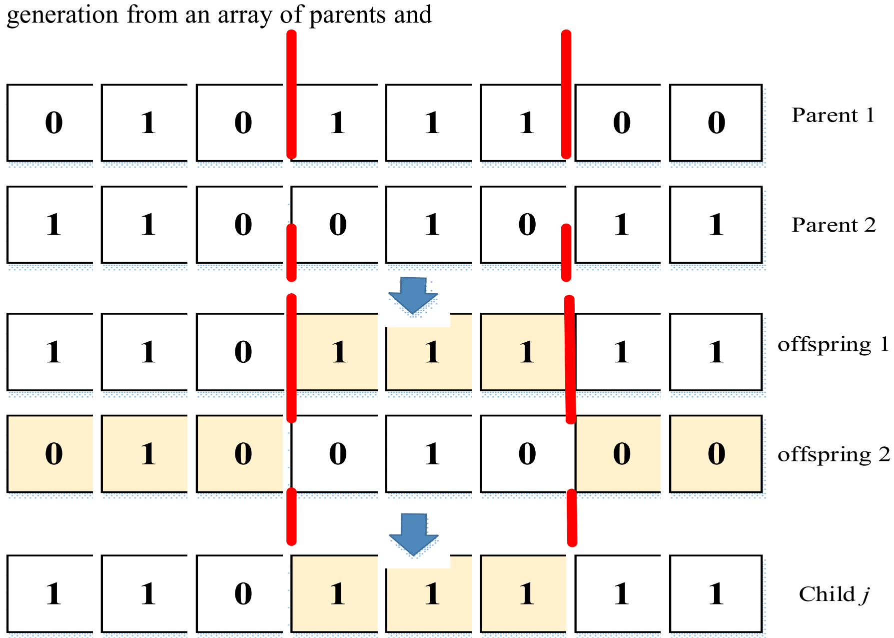



*Figure 1 – Scheme of Two-Point Crossing*

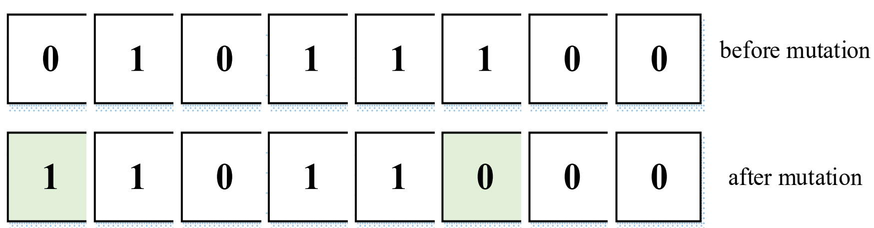
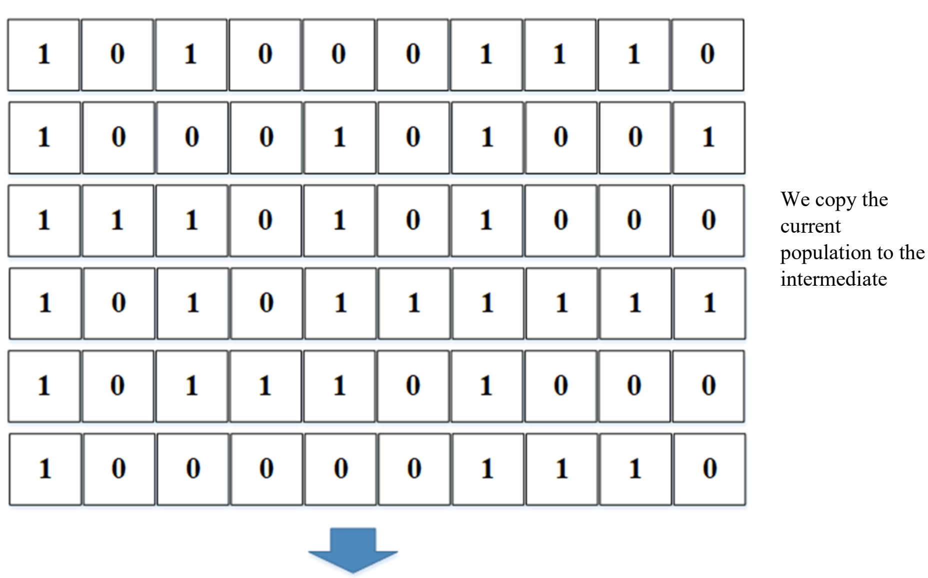



*Figure 2 – Scheme of Mutation*



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

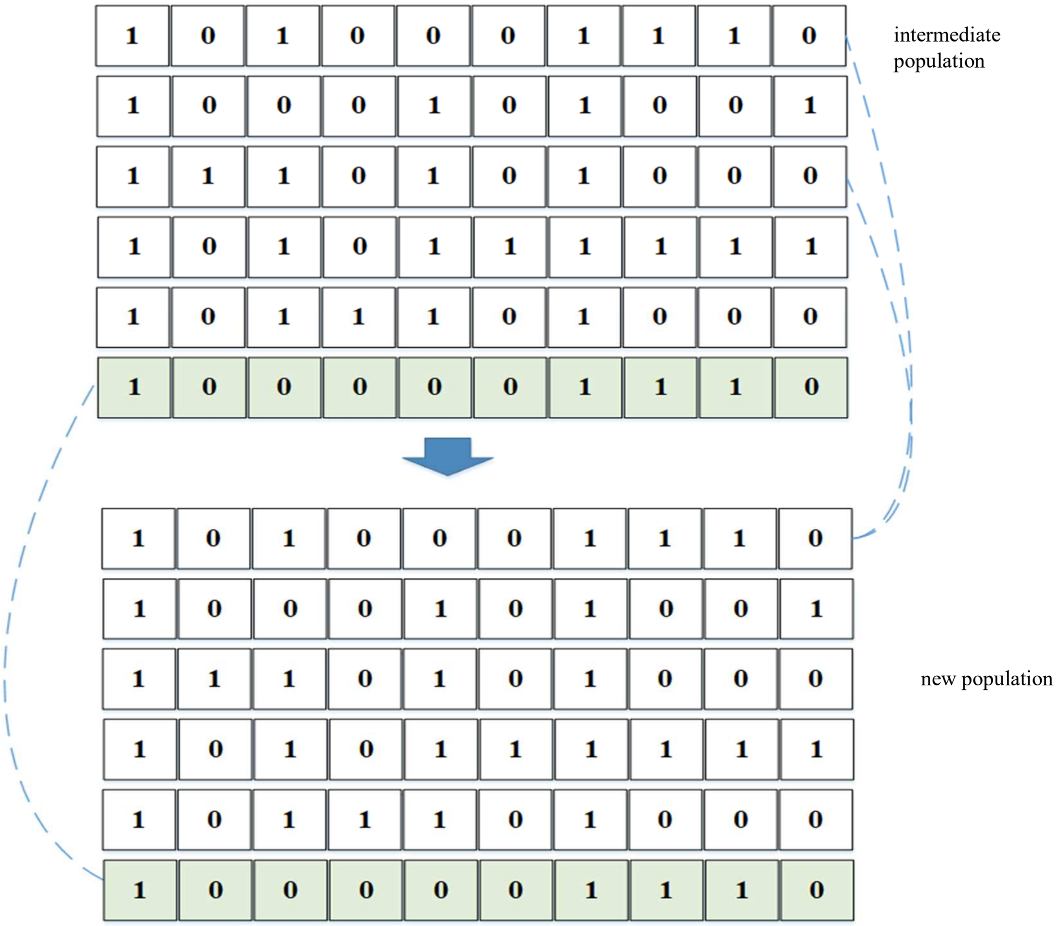



*Figure 3 – Scheme of the Formation of a New Population*

The procedure for working with the modified algorithm for solving the problem of multicriteria optimization of the parameters of a multi-circuit information system of an informatization object is as follows:

Step 1.

We select the domains of definition for all variables (OBI cybersecurity metrics), see table 1:

*Table 1 – Variables for GA*

| Bit number in the chromosome | Cybersecurity metrics for the analyzed object of informatization |
|---|---|
| 0 | The proportion of cybersecurity incidents (KB) on OBI (by type) |
| 1 | The proportion of incidents with design bureaus on OBI with observance of response times |
| 2 | The average duration of response time to incidents with KB (by severity level) |
| 3 | Percentage of OBI vulnerabilities that were fixed within a specified time frame |
| 4 | Average time spent on fixing OBI vulnerabilities |
| 5 | Share of risks for OBI information assets (unacceptable level for each asset) |
| 6 | The proportion of risks for CS OBI, for which appropriate measures were taken |
| 7 | Index of compliance with IS standard (s) |
| 8 | Effectiveness of training employees on measures to comply with CS rules |
| 9 | Indicators of the sufficiency of resources (financial, technical, organizational, etc.) to perform the tasks of IS and CS OBI |

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

Step 2.

The solution is based on the general evolutionary algorithm and its components of multicriteria GA. The main method was VEGA - Vector Evaluated Genetic Algorithm [1,2].

The input of GA parameters. We set: the size of the population; the number of generations (from 100 to 2000); the mutation type: number of runs.

Unlike the existing classical VEGA algorithm [5], [19], the modified algorithm additionally applies the Pareto principle.

Let's take the following variables:

$PO_t$ – current population;

$PO_m$ – intermediate population;

$S_{po}$ – population size;

$N_{PO_m}$ – the number of copies in the comparative set;

$D(I_1, I_2)$ – distance between instances.

The selection procedure uses ranking of specimens based on Pareto dominance [21]. The rank of a specimen, in relation to which none of the alternative specimens of the analyzed population has superior optimality criteria, is set equal to 1.

For the rest of the instances, we find the rank as follows:

$$rank(I_k) = 1 + N_{a_k}, \tag{1}$$

$N_{a_k}$ – the number of specimens of the current population, the characteristics of which are better than the current one.

The instantiation mechanism is provided when the following condition is met:

where $M(I)$ – is the function to display the instance $I \in CS_I$;

$CS$ – the space of criteria by which the selection of instances is carried out.

The rank of instances for which constraint (2) is violated is assigned depending on how these constraints are violated. The rank of each of the instances for which constraint (2) is violated will be greater than the rank of any of the instances for which this (2) holds.

We build the fitness function based on the expression:

$$\gamma(I) = 1 + \sum_{k=1}^{rank(I)-1} h(k), \tag{3}$$

where $h(k)$ – is the number of instances with rank $(k)$.

The fitness function can be written in another way:

$$f(I_1) = z(I_1) \cdot \gamma(I_1), \tag{4}$$

where $z(I_1)$ – the number of instances is calculated as follows:

$$z(I_1) = \sum_{I_k \in PO_t} Sh(d(I_1, I_k)), \tag{5}$$

where $Sh(d)$ – the split function is calculated like this:

$$Sh(d) = \begin{cases} 1 - \dfrac{d}{S_{po}}, & d < S_{po}, \\ 0, & d \geq S_{po}. \end{cases} \tag{6}$$

The Pareto principle applies to the best point. At this point, the solution, interpreted as the best, if there is an improvement in one of the cybersecurity metrics, and strictly no worse in the other metric (or metrics).

## 5. ACKNOWLEDGEMENTS

The GA described above was software implemented in the form of separate modules of the decision support system (DSS) for the problem of multi-criteria optimization of costs for the OBI ISS. The programming environment is Visual Studio. Below is the description of the DSS module "Genetic algorithm for multi-criteria cost optimization for OBI SIS. This algorithm and the corresponding module are part of the DSS expert subsystem. The block diagram of the entire algorithm of the expert system is shown in Fig. 4.

The expert subsystem provides the development and assessment of possible alternatives to the multicriteria optimization of costs for the OBI SIS based on the knowledge that was obtained from expert experts.

The expert subsystem consists of:

- knowledge bases (KB). KB is intended for storing initial and intermediate facts accumulated in the course of solving the problem of multi-criteria optimization of costs for OBI information security;
- block for solving problems associated with the choice of rational multicriteria cost optimization for OBI information security. This block will ensure the implementation

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

of a sequence of rules execution for solving a specific problem of multi-criteria cost optimization for OBI ISS;

- subsystem explanations. This subsystem will allow the decision-maker (DM) to understand the reason that is proposed by the expert DSS module;
- a module for generating rules. The module is used to add new rules to the knowledge base and/or modify them;
- dialogue interface.

If there is no solution for the initial formulation of the problem, then a problem-oriented expert group is formed. Further, questions are sent to the experts, which will help in the future to form a new decision rule. Experts form a decision rule for choosing the best alternative and the corresponding DSS subsystem.

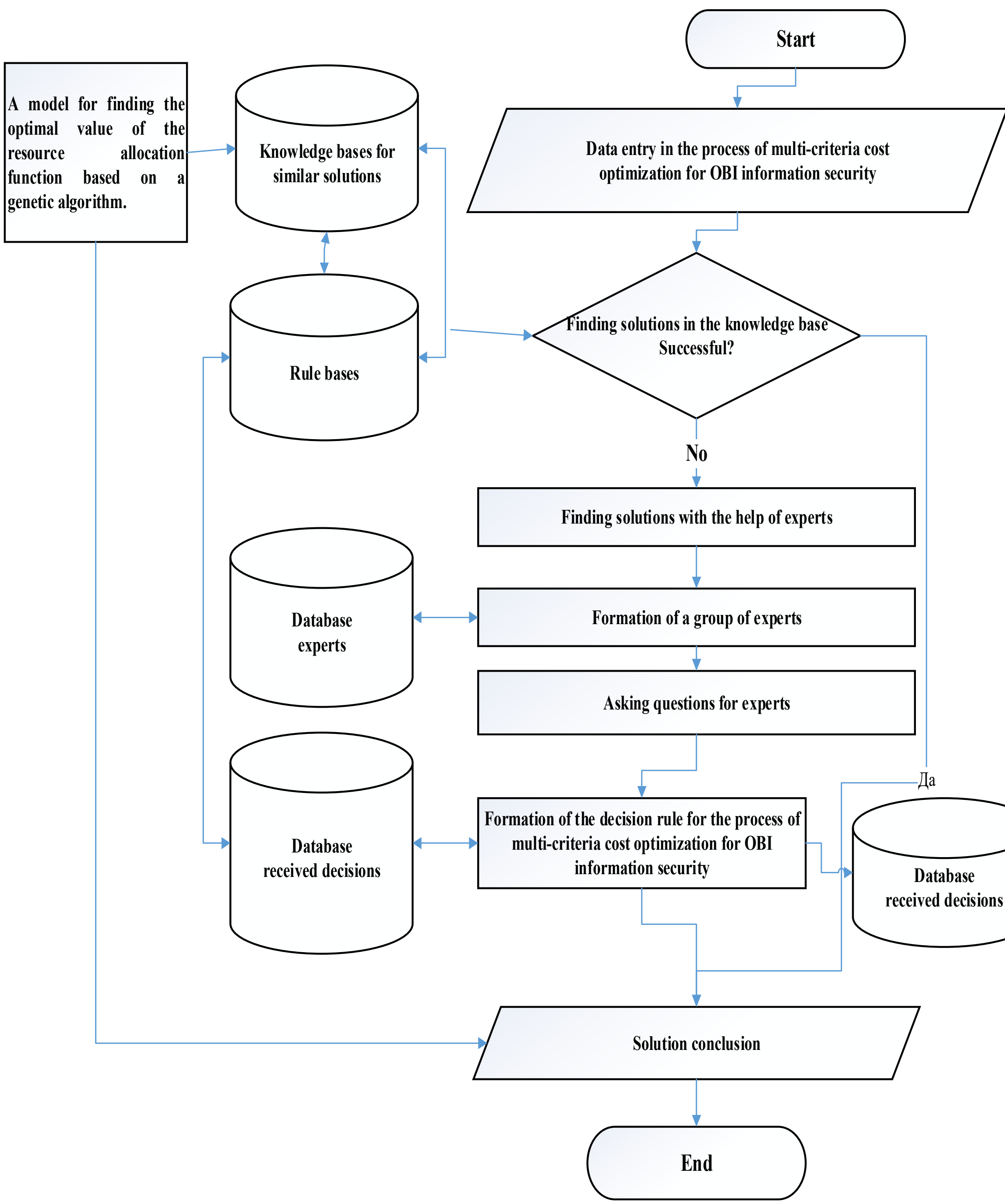
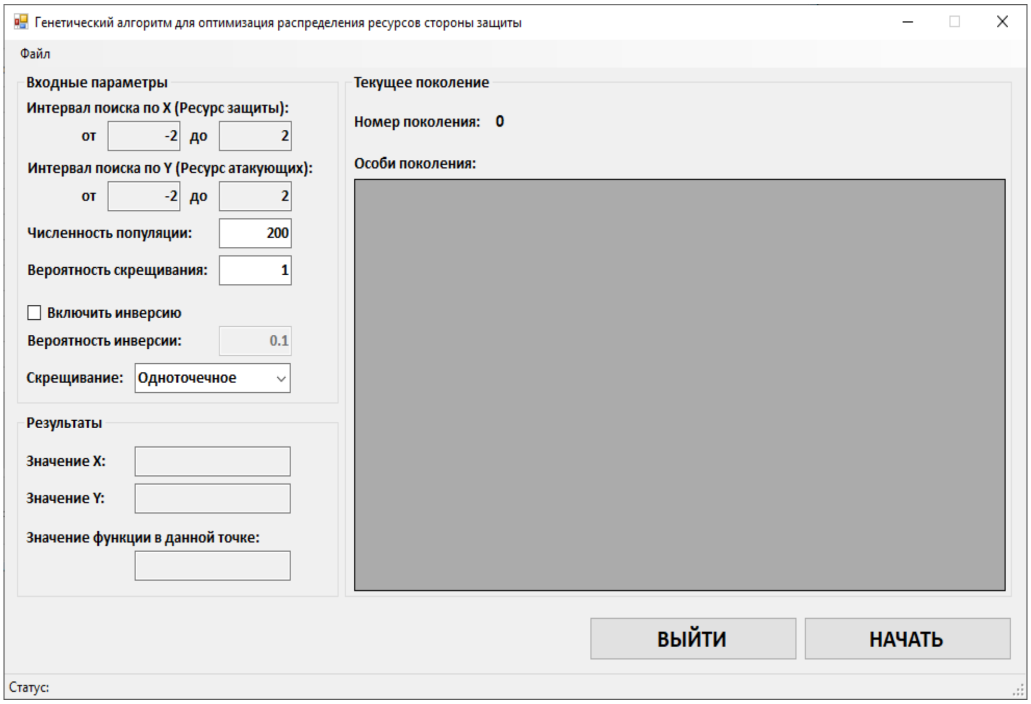
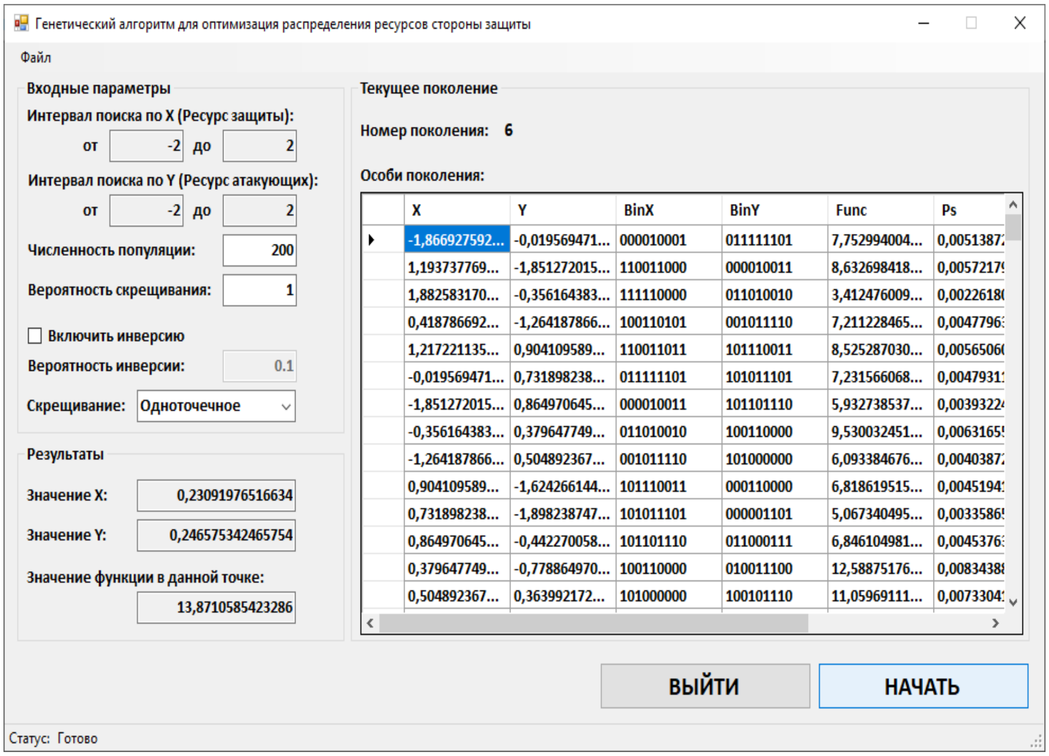



*Figure 4 – Block Diagram Of The Expert Subsystem Functioning Algorithm For The Designed DSS*




a) general view of the DSS module interface




b) an example of a solution

*Figure 5 – General View of Module 2 - Genetic Algorithm for Optimizing the Cost of OBI ISS*

Figure 5 b) shows an example of solving the problem of finding rational parameters of the ratio of performance indicators of specific information security systems for OBI and cost indicators for their acquisition, maintenance, modernization) included in the target function, and depending on the list of works to ensure information protection on OBI (in particular, design, development, and deployment of an integrated information security system, improving the information security system, etc.

Unlike the existing classical VEGA algorithm, the modified algorithm additionally applies the Pareto principle, as well as a new selection mechanism. A code snippet that implements the Pareto principle is shown below.

```
// Check that the found solution is the best /
if (better [0]> = functional [0] [i] && better [1] <=
functional [1] [i])
{
// check the condition that the obtained parameter value is
better
// and other things are not worse than they were
if (better [0]! = functional [0] [i] || better [1]! = functional
[1] [i])
{
// Check that this entry has not been encountered before
better [0] = functional [0] [i];
better [1] = functional [1] [i];
for (int j = 0; j <numb_of_variables; j ++)
{better_pos [j] = point [j];
// Store the coordinates for the best point
}
find_itr = gener;
// Write down the generation number
for (int s = 0; s <len; s ++)
{
superM [s] = Popul [i] [s];
// Save the genotype for the best point
 }
doom = 0;
}
}
delete [] point;
// Remove the array containing the coordinate values in
decimal form
}
int ** inter_Populat = newint * [Populat_Size];
// Create an intermediate population for sampling
// for subsequent GA operations
for (inti = 0; i <Populat_Size; i ++)
{
inter_Populat [i] = new int [len];
}
```

The new selection mechanism involves the creation of an intermediate population - $PO_m$. This intermediate population is formed as follows:

Stage 1. The first half of the population $PO_m$ is formed based on the metric - the proportion of OBI vulnerabilities that were eliminated promptly.

Stage 2. The second half of the intermediate population $PO_m$ is formed based on the metric - the proportion of risks that are unacceptable to the levels for OBI information assets.

Stage 3. Parts of the intermediate population are mixed.

Step 4. After mixing, an array of numbers is formed and mixed.

Stage 5. For crossing, specimens (individuals) by the number from this array will be taken. The numbers are chosen randomly.

```
int ** inter_Populat = newint * [Populat_Size];
// Create an intermediate population
// from which the instances for the GA are then taken
for (inti = 0; i <Populat_Size; i ++)
{
inter_Populat [i] = new int [len];
}
// Subpopulation for the share of OBI vulnerabilities,
// which were eliminated in a timely manner
fitness_filling (Populat_Size, functional [0], 0);
// Calculate the fitness function
 Propor_sel (fitness, Populat_Size);
// Apply proportional selection
intrazdel = Populat_Size / 2;
for (inti = 0; i <razdel; i ++)
{
for (int j = 0; j <len; j ++)
{
inter_Populat [i] [j] = Popul [lucky (possible, Populat_Size)]
[j];
}
}
// Subpopulation for the proportion of risks that
// not valid for OBI information assets
fitness_filling (Populat_Size, functional [1], 1);
// Calculate the fitness function
Propor_sel (fitness, Populat_Size);
// Apply proportional selection
for (inti = razdel; i <Populat_Size; i ++)
{
for (int j = 0; j <len; j ++)
{
inter_Populat [i] [j] = Popul [lucky (possible, Populat_Size)]
[j];
}
}
int * Posit = new int [Populat_Size];
for (inti = 0; i <Populat_Size; i ++)
{
Posit [i] = i;
}
// Shuffle the intermediate population
for (inti = 0; i <1000; i ++)
{
int buff = 0; int number1 = 0, number2 = 0;
number1 = rand ()% Populat_Size;
do
{
number2 = rand ()% Populat_Size;
}
while (number1 == number2);
buff = Posit [number1];
Posit [number1] = Posit [number2];
Posit [number2] = buff;
}
/ We carry out two-point crossing
for (inti = 0; i <Populat_Size - 1; i ++)
{
cross_2 (inter_Populat [Posit [rand ()% Populat_Size]],
inter_Populat [Posit [rand ()% Populat_Size]], Popul [i],
len);
```

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

To check the effectiveness of the proposed algorithm, computational experiments were carried out, in particular, to estimate the time spent by various algorithms to find a solution in the course of optimizing the costs of the OBI ISS. Based on a series of 500 computational experiments, it was found that for the final version of the algorithm and its software implementation in the DSS, it is enough to take 25 chromosomes in the population.

In the course of computational experiments, it was found that the GA is distinguished by a sufficiently high performance, see Figure 6.

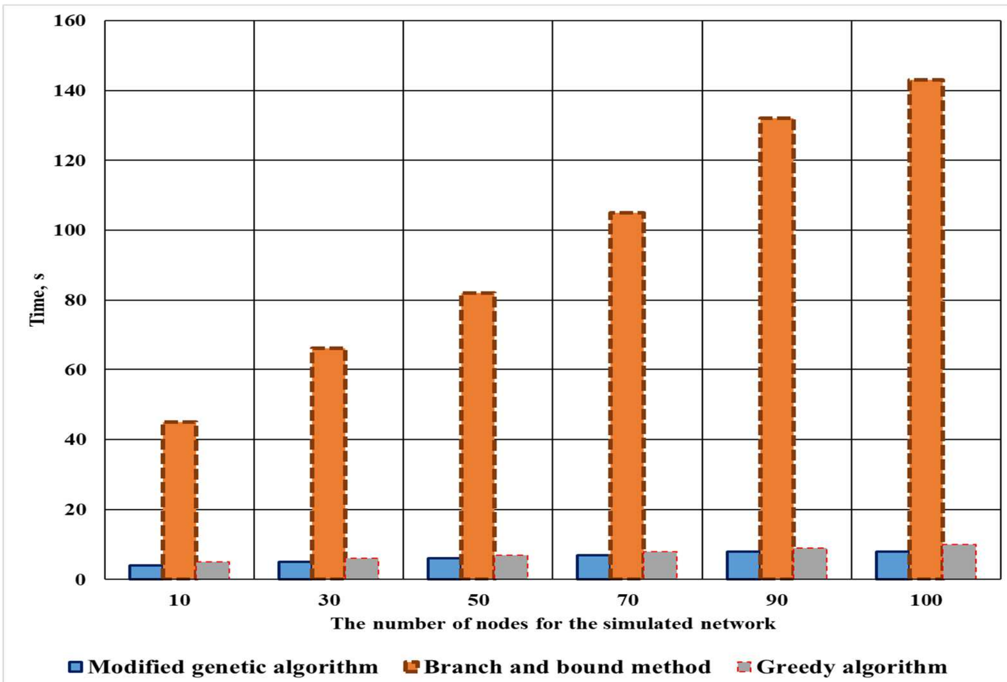



*Figure 6 – Results of Computational Experiments Comparing the Running Time of Algorithms*

## 6. DISCUSSION OF THE RESULTS OF THE COMPUTATIONAL EXPERIMENT

The time spent on solving the problem when using GA is about 16–25 times less in comparison with the indicators of the branch and bound method. The greedy algorithm is inferior to both the GA and the branch-and-bound method in terms of adaptability to solving a multicriteria optimization problem, taking into account the imposed restrictions and the number of variables.Certain disadvantages of the study, at the current stage of its implementation, include the fact that not all possible algorithms for solving the problem have been analyzed.

Currently, work is underway to add new algorithms to the list of those available in the DSS. A wider choice of DSS options will make it more functional for solving the problem under consideration.

And although, like all modifications of the GA, the solution we propose does not apply to exact methods, nevertheless, in our opinion, it is well suited for the selected subject area. Indeed, under conditions of dynamic confrontation with the attacking side, it is much more important to find a solution quickly and with acceptable accuracy than to scrupulously search for the exact solution. Our studies are in good agreement with the new results of other authors [22, 23], who are studying the possibility of a genetic algorithm and its modifications for solving optimization problems, in particular, related to the problem of plant equipment placement.

## 7. ACKNOWLEDGEMENTS

The research and article were carried out within the framework of the grant of the Republic of Kazakhstan registration number AP08855887-OT-20 "Development of an intelligent decision support system in the process of investing in cyber security systems."

## 8. CONCLUSIONS

The technique of multicriteria optimization of costs for the information protection system of the

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

object of informatization is stated. The technique is based on the use of a genetic algorithm.

A modified algorithm for solving the MCO problem of parameters of a multi-circuit information protection system of an informatization object is proposed, which allows one to substantiate the rational characteristics of the information security components, taking into account the priority metrics of the OBI cybersecurity selected by the expert.

Unlike the existing classical VEGA algorithm, the modified algorithm additionally applies the Pareto principle, as well as a new selection mechanism.

The Pareto principle applies to the best point. At this point, the solution, interpreted as the best, if there is an improvement in one of the cybersecurity metrics, and strictly no worse in the other metric (or metrics).

The new selection mechanism, in contrast to the traditional one, involves the creation of an intermediate population. This intermediate population is formed in several stages. At the first stage, the first half of the population is formed based on the metric - the proportion of OBI vulnerabilities that were eliminated on time. At the second stage, the second half of the intermediate population is formed based on the metric - the proportion of risks that are unacceptable for OBI information assets. Further, these parts of the intermediate population are mixed. After mixing, an array of numbers is formed and mixed. At the final stage of selection for crossing, specimens (individuals) will be taken by the number from this array. The numbers are chosen randomly.

**REFERENCES:**

[1] A. OKUTAN, S. J. YANG, K. MCCONKY and G. WERNER, "CAPTURE: Cyberattack Forecasting Using Non-Stationary Features with Time Lags," *2019 IEEE Conference on Communications and Network Security (CNS)*, 2019, pp. 205-213, doi: 10.1109/CNS.2019.8802639.

[2] BARRETO, Carlos & KOUTSOUKOS, Xenofon. (2019). Design of Load Forecast Systems Resilient Against Cyber-Attacks. Doi: 10.1007/978-3-030-32430-8_1.

[3] CHANDRA, Yogesh & MISHRA, Pallaw. (2019). Design of Cyber Warfare Testbed. Doi: 10.1007/978-981-10-8848-3_24.

[4] SÁNDOR, Hunor & BELA, Genge & SZÁNTÓ, Zoltán & MARTON, Lorinc & PIROSKA, Haller. (2019). Cyber Attack Detection and Mitigation: Software Defined Survivable Industrial Control Systems. International Journal of Critical Infrastructure Protection. 25. Doi: 10.1016/j.ijcip.2019.04.002.

[5] CHIBA, Zouhair & ABGHOUR, Noreddine & MOUSSAID, Khalid & EL, Amina & RIDA, Mohamed. (2019). New Anomaly Network Intrusion Detection System in Cloud Environment Based on Optimized Back Propagation Neural Network Using Improved Genetic Algorithm. International Journal of Communication Networks and Information Security. 11. 61-84.

[6] NOZAKI, Yusuke & YOSHIKAWA, Masaya. (2020). Security Evaluation of Ring Oscillator PUF Against Genetic Algorithm Based Modeling Attack. Innovative Mobile and Internet Services in Ubiquitous Computing. Doi: 10.1007/978-3-030-22263-5_33.

[7] DWIVEDI, Shubhra & VARDHAN, Manu & TRIPATHI, Sarsij. (2020). Incorporating evolutionary computation for securing wireless network against cyberthreats. The Journal of Supercomputing, 1–38.

[8] F. ZHANG, H. A. D. E. KODITUWAKKU, J. W. HINEs and J. COBLE, "Multilayer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System, and Process Data," in *IEEE Transactions on Industrial Informatics*, vol. 15, no. 7, pp. 4362-4369, July 2019, doi: 10.1109/TII.2019.2891261

[9] SURESHKUMAR, T. & ANAND, Bojan & PREMKUMAR, Thathan. (2019). Efficient Non-Dominated Multi-Objective Genetic Algorithm (NDMGA) and network security policy enforcement for Policy Space Analysis (PSA). Computer Communications. 138. Doi: 10.1016/j.comcom.2019.03.008.

[10] SHANG, Q., CHEN, L., WANG, D., TONG, R., & PENG, P. (2019). Evolvable Hardware Design of Digital Circuits Based on Adaptive Genetic Algorithm. In International Conference on Applications and Techniques in Cyber Security and Intelligence (pp. 791–800). Springer, Cham. Doi: 10.1007/978-3-030-25128-4_97.

[11] YANG, Y. (2019). Research on Hybrid Quantum Genetic Algorithm Based on Cross-Docking Delivery Vehicle Scheduling. In The International Conference on Cyber Security Intelligence and Analytics (pp. 893–900). Springer, Cham. Doi: 10.1007/978-3-030-15235-2_119.

[12] SAENKO, I., & KOTENKO, I. (2019). A role-base approach and a genetic algorithm for VLAN design in large critical infrastructures. In Proceedings of the Genetic and Evolutionary Computation Conference Companion (pp. 1643–1650). Doi: 1643-1650. 10.1145/3319619.3326853.

[13] Y. ALEKSIEVA, H. VALCHANOV and V. ALEKSIEVA, "An approach for host based botnet detection system," *2019 16th Conference on Electrical Machines, Drives and Power Systems*

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

*(ELMA)*, 2019, pp. 1-4, doi: 10.1109/ELMA.2019.8771644

[14] R. VINAYAKUMAR, M. ALAZAB, K. P. SOMAN, P. POORNACHANDRAN, A. AL-NEMRAT and S. VENKATRAMAN, "Deep Learning Approach for Intelligent Intrusion Detection System," in *IEEE Access*, vol. 7, pp. 41525-41550, 2019, doi: 10.1109/ACCESS.2019.2895334

[15] MALARVIZHI, N., SELVARANI, P., & RAJ, P. (2019). Adaptive fuzzy genetic algorithm for multi biometric authentication. Multimedia Tools and Applications, 1–14. Doi: 10.1007/s11042-019-7436-4.

[16] ALHIJAWI, B., KILANI, Y., & ALSARHAN, A. (2020). Improving recommendation quality and performance of genetic-based recommender system. International Journal of Advanced Intelligence Paradigms, 15(1), 77–88. Doi: 10.1504/IJAIP.2018.10010165.

[17] BAROUDI, U., BIN-YAHYA, M., ALSHAMMARI, M., & YAQOUB, U. (2019). Ticket-based QoS routing optimization using genetic algorithm for WSN applications in smart grid. Journal of Ambient Intelligence and Humanized Computing, 10(4), 1325–1338. Doi: 10.1007/s12652-018-0906-0.

[18] LLANSÓ, T., MCNEIL, M., & NOTEBOOM, C. (2019). Multi-Criteria Selection of Capability-Based Cybersecurity Solutions. In Proceedings of the 52nd Hawaii International Conference on System Sciences, pp. 7322–7330. Doi: 10.24251/HICSS.2019.879.

[19] T. KONG, L. WANG, D. MA, Z. XU, Q. YANG and K. CHEN, "A Secure Container Deployment Strategy by Genetic Algorithm to Defend against Co-Resident Attacks in Cloud Computing," *2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, 2019, pp. 1825-1832, doi: 10.1109/HPCC/SmartCity/DSS.2019.00251.

[20] LAKSHMANAPRABU, S. K., MOHANTY, S. N., KRISHNAMOORTHY, S., UTHAYAKUMAR, J., & SHANKAR, K. (2019). Online clinical decision support system using optimal deep neural networks. Applied Soft Computing, 81, 105487. Doi: 10.1016/j.asoc.2019.105487.

[21] V. LAKHNO, B. AKHMETOV, S. ADILZHANOVA, A. BLOZVA, R. SVITLANA and R. DMYTRO, "The Use of a Genetic Algorithm in the Problem of Distribution of Information Security Organizational and Financial Resources," *2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT)*, 2020, pp. 251-254, doi: 10.1109/ATIT50783.2020.9349310..

[22] 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. Doi: 10.1007/978-3-030-77448-6_5

[23] C. DOU, P. GU, M. ZHAO and S. WANG, "Research on Mobile Path Planning Model of Equipment Maintenance Support Unit Based on Improved Genetic Algorithm," *2021 IEEE International Conference on Power Electronics, Computer Applications (ICPECA)*, 2021, pp. 157-160.

[24] BEBESHKO, B., KHOROLSKA, K., KOTENKO, N., KHARCHENKO, O., & ZHYROVA, T. (2021). Use of neural networks for predicting cyberattacks. Paper presented at the CEUR Workshop Proceedings, 2923 13-223. http://ceur-ws.org/Vol-2923/paper23.pdf

[25] KHOROLSKA K., LAZORENKO V., BEBESHKO B., DESIATKO A., KHARCHENKO O., YAREMYCH V. (2022) Usage of Clustering in Decision Support System. In: Raj J.S., Palanisamy R., Perikos I., Shi Y. (eds) Intelligent Sustainable Systems. Lecture Notes in Networks and Systems, vol 213. Springer, Singapore. doi: 10.1007/978-981-16-2422-3_49

[26] LAKHNO V., AKHMETOV B., YDYRYSHBAYEVA M., BEBESHKO B., DESIATKO A., KHOROLSKA K. (2021) Models for Forming Knowledge Databases for Decision Support Systems for Recognizing Cyberattacks. In: Vasant P., Zelinka I., Weber GW. (eds) Intelligent Computing and Optimization. ICO 2020. Advances in Intelligent Systems and Computing, vol 1324. Springer, Cham. https://doi.org/10.1007/978-3-030-68154-8_42.

[27] KRYVORUCHKO, O., BEBESHKO, B., KHOROLSKA, K., DESIATKO, A., & KOTENKO, N. (2020). Artificial intelligence face recognition for authentication. *Technical Sciences and Technology*, (2(20), 139–148. Retrieved from http://tst.stu.cn.ua/article/view/215780