ABSTRACT

The dissertation work of Adilzhanova Saltanat on the topic «Methods, models and information technologies for the dynamic management of cybersecurity resources» submitted for the degree of Doctor of Philosophy (Ph.D.) on the specialty «8D06301- Information security systems»

Relevance of the work. In the conditions of permanent confrontation between the parties of defense and attack, the purpose of the information security service of any object of informatization is to minimize the possibilities of its theft, distortion, loss of confidentiality as a consequence of the actions of the attacking party. At the same time, the attackers have diametrically opposite tasks – the distribution of their resources in such a way as to minimize the costs of gaining access to information resources of the object of informatization.

The distribution of the limited resources of the protection side properly constitutes the essence of many areas of research in the field of cybernetic or information security. This approach in relation to the information security and design bureau leads to the formulation of the problem of optimizing the allocation of resources between the objects of protection.

In conditions of uncertainty, when the actions of the opponent can be assumed only with a certain probability, the search for the optimal distribution of limited resources between the objects of information protection through the use of game-theoretic methods and taking into account the dynamics of changes in the conditions of confrontation will reduce the amount of damage caused by the implementation of threats to information to a minimum. At the same time, it seems advisable to focus on the development of evolutionary methods and genetic algorithms for generating a variety of solutions in the search for optimal configurations of multi-circuit systems of information protection and cyber security for the object of informatization, as well as the use of genetic algorithm to solve the problem of dynamic redistribution of resources of the defense side, based on the relevance of existing threats.

The increase in the cost of information security tools actualizes the problem of optimal use of protected resources. In the process of finding solutions, it is necessary to consider the change in the conditions of confrontation with the attacking side over time. This is due to the "aging" of information resources, their updating, the emergence of new means of attack, the modernization of information security tools, and the like. As a result, we come to the need to solve the problem of dynamic resource management in complex security structures.

Thus, to build an effective information security tools, it is necessary to consider a sufficiently large number of indicators, which together determine its effectiveness. At the same time, achieving optimal values of various indicators is difficult and often impossible due to the inconsistency of their requirements is difficult. As a result, we come to a multi-criteria problem. Solving such a problem is always a compromise in meeting the requirements for individual indicators. When solving such multi-criteria problems, choosing solution algorithms is always difficult. This is especially true for tasks related to information protection since the protection side's actions mostly occur in uncertain conditions.

The purpose of the dissertation work is to increase the level of security of the object of informatization due to the optimal allocation of information protection resources between the objects of protection, taking into account the actions of the attacker.

Research objectives:

1. Analyze the security management models of internet control server object of informatization, in particular, models for finding the optimal distribution of funds between information security objects;

2. To develop an to solve the multi-criteria task of optimizing the allocation of resources of the defense side in the process of implementing projects to ensure the cyber security object of informatization;

3. To supplement the genetic algorithm to solve the problem related to the selection and optimization of options for the configuration of information security tools for the safety circuits of the internet control server;

4. Programmatically implement a multimodule to analyze and select a rational option for allocating resources by the information security side.

The research subject is methods and models of resource management of the protection side in the construction of information security systems.

Research methods. The Belman-Zade dynamic programming method to find optimal resources of the defense side; evolutionary algorithms – to solve the multi-criteria optimization problem of allocating resources of the defense side in the process of implementing projects to ensure cyber security object of informatization;

The scientific novelty of the research conducted and the results obtained:

– The methodology for selecting the objective function of the model describing the damage caused by the implementation of threats and the vulnerability of information resources of the the object of informatization.

– For the first time, the modified genetic algorithm was developed, which, unlike the existing ones, makes it possible to simplify the solution of the multi-criteria optimization task of allocating resources of the protection side in the process of implementing projects to ensure the cyber security of the object of informatization.

– The genetic algorithm was further developed to solve the problem related to the selection and optimization of options for the configuration of the information security tools for the security circuits of the internet control server for optimizing the composition of the information security tools.

The theoretical significance of the study: the methodology for selecting the objective function of the model describing the damage caused by the implementation of threats and the vulnerability of information resources of informatization objects has been supplemented. The modified genetic algorithm has also been developed, which makes it possible to simplify the solution of the multi-criteria optimization task of allocating the resources of the defense side in the process of implementing projects to ensure the cyber security of the object of informatization. The genetic algorithm has also been further developed to solve the problem related to the selection and optimization of options for the configuration of information security tools for the security circuits of the which, unlike existing solutions, uses the total amount of risks from information loss, integral indicators of information security tools, as well as cost indicators for each class of internet control server as a criterion for optimizing the composition of information security tools.

Practical value.

The practical value of the “DSS Dynamic allocation of cybersecurity resources” is confirmed by the acts of implementation, in particular, the effectiveness of the open multimodule architecture of the with the ability to add dynamically attached libraries for the computing core for the its architecture as the functionality of the expands.

The following provisions are submitted for protection:

- The method of selecting the target function of the model describing the damage caused by the implementation of threats and the vulnerability of information resources of the object of informatization;
- Modified genetic algorithm, which makes it possible to simplify the solution of the multi-criteria optimization task of allocating resources of the protection side in the process of implementing projects to ensure the cybersecurity of informatization objects, which makes it possible to optimize the allocation of resources for work related to measures aimed at reducing the vulnerabilities of components in the informatization objects and simulate different variants of the volumes of resources that ensure the achievement of the specified values of the security of informatization objects in in the absence of data on the resources of the attacking party;
- A genetic algorithm for solving a problem related to the selection and optimization of information security configuration options for information and communication systems security circuits in which.

Personal contribution of the researcher. All the results of the dissertation work that were submitted for defense were received by the doctoral student personally. Among the main results: modified genetic algorithm to solve the multi-criteria task of optimizing the allocation of resources of the protection side in the process of implementing projects to ensure the cyber security, genetic algorithm to solve the problem associated with the selection and optimization of options for the configuration of information security tools for the security circuits of the internet control server. Software implementation of the module in the form of a dynamically attached library for the decision support system computing core based on the proposed modification of the genetic algorithm, taking into account the total amount of risks from information loss, integral indicators of the information security tools, as well as cost indicators for each class of the information security tools.

Approbation of the results of the dissertation. The main results of the dissertation work were reported and discussed at seminars of the Department of “Information Systems” of Al-Farabi Kazakh National University and the Department of Computer Systems, Networks and Cybersecurity of the National University of Bioresources and Environmental Management of Ukraine; «Institute of information and computational technologies», International Scientific Conference of Students and Young Scientists “Farabi alemi,” Al-Farabi Kazakh National University, (Almaty, 2020, 2021);

Publications. The results presented in the dissertation work have been published in printed works, including 5 articles in journals recommended by Committee for Control in the Field of education and Science of the Ministry of Education and Science of the Republic of Kazakhstan; 4 publications in the materials of international conferences, 3 articles in journals included in the Scopus database, and 1 author's certificate was obtained.

The results of the dissertation were presented in 11 scientific papers, of which 5 articles were reviewed in the Scopus database, 4 articles in journals recommended by the Committee for Quality Assurance in the Field of Education and Science of the Ministry of Education and Science of the Republic of Kazakhstan, and 2 articles in the proceedings of international conferences:

Journal article in the Scopus database:

1. Akhmetov, B., Lakhno V., Adilzhanova S. Automation of Information Security Risk Assessment. International Journal of Electronics and Telecommunications 2022, 68(3), pp. 549–555.
2. B. Akhmetov, V. Lakhno, S.Adilzhanova, B. Yagaliyeva Conseptual Diagram of intelligent Decision Support System in the Prosses of Investing in Cybercecurity Systems. Journal of Theoretical and Applied Information Technology, 2021, 99(18), стр. 4297–4310.
3. V. Lakhno, S.Adilzhanova, O. Kryvoruchko Genetic algorithm for solving the problem of scaling a cloud-oriented object of information. Journal of Theoretical and Applied Information Technology, 2022, 100(7), стр. 1693–1705.
4. V. Lakhno, S.Adilzhanova, O. Kryvoruchko, A. Desiatko Allocation of Organizational and Financial Resources of the Information Protection Side Using a Genetic Algorithm. Informatics and Cybernetics in Intelligent Systems. CSOC 2021. Lecture Notes in Networks and Systems, vol 228. Springer, Cham.
5. B. Akhmetov, V. Lakhno, S.Adilzhanova 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, стр. 251–254, 9349310

In journals recommended by the Education and Science Control Committee of the Ministry of Education and Science:

1. V. A. Lahno, S. A. Adilzhanova K. T. Sauanova . Application of the genetic algorithm in dynamic monitoring problems of cyber security resources. Bulletin of kaznrtu named after Satpayev No. 6 (142). Article 2020. pp. 565-568
2. S. A. Adilzhanova, G. A. Tyulepberdinova M. Zh. Sakypbekova . Analysis of mathematical methods for multidimensional optimization and dynamic management of cybersecurity resources of informatization objects. Bulletin of Abai Kaznpu, Series "physical and Mathematical Sciences", No. 4(72), 2020 pp. 145-148.
3.Adilzhanova S. A., B. C. Akhmetov, Abuova A. K., Sagyndykova Sh. A modular system for supporting decision-making when optimizing the distribution of resources between defense objects. Bulletin of Abai Kaznpu, Series "physical and Mathematical Sciences" No. 4 (76), 2021 G. I. P. 128 - 135.
4.Adilzhanova S. A., B. C. Akhmetov, V. A. Lahno . Development of a genetic algorithm to solve the problem of selection, optimization and redistribution of resources of the Information Protection party. Bulletin of Almaty University of energy and communications No. 1 (56) 2022., p. 116 - 123

In international conferences:

1. S.A. Adilzhanova . Cyberkauipsizdik resursstaryn dynamikalyk baskarudyn mathematikalyk adisterin taldau.International Scientific Conference of students and Young scientists "FARABI ALEMI", Al-Farabi Kazakh National University, 2020. P.41
2. S.A. Adilzhanova The use of a genetic algorithm in the problem of dynamic management of cybersecurity resources. International Scientific Conference of students and Young scientists “FARABI ALEMI”, Al-Farabi Kazakh National University, 2021. P.73

The structure and scope of the dissertation. The dissertation consists of an introduction, four sections, a conclusion set out on 128 pages and contains 23 figures, 9 tables, 93 sources used and 2 appendices.

The introduction substantiates the relevance of the dissertation. The purpose of the work, the object and the subject of the study are formulated. The scientific novelty and practical significance are revealed. The results of the study are described. Information is provided on the approbation of the results of the study and publication.

The first section presents an analysis of mathematical methods of multi-criteria optimization and dynamic management of cybersecurity resources of informatization objects.

The second section describes a genetic algorithm for solving the problem of optimizing the allocation of resources of the defense side in the process of implementing cyber security projects.

The third section describes the work of decision support for optimizing the placement of information security tools based on the use of a modified genetic algorithm.

The fourth section presents the results and software implementation of the DSS modules during the search for rational strategies for the dynamic allocation of resources of the protection side.

In conclusion the main results obtained in the dissertation are formulated.