ТЕХНИЧЕСКИЕ НАУКИ | TECHNICAL SCIENCE

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ INFORMATICS, COMPUTER ENGINEERING AND MANAGEMENT

Клименко Ирина Сергеевна
[Klimenko Irina Sergeevna]

УДК: 621.391

DOI:10.37493/2307-910X.2023.1.1

МОДЕЛИРОВАНИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ АЛГОРИТМОВ МНОГОКРИТЕРИАЛЬНОЙ ОПТИМИЗАЦИИ

MODELING OF INFORMATION SECURITY SYSTEMS BASED ON MULTI-CRITERIA OPTIMIZATION ALGORITHMS

Пятигорский институт (филиал) Северо-Кавказский Федеральный Университет, Пятигорск, РФ E-mail: iskl@bk.ru / Pyatigorsk Institute (branch) of North-Caucasus Federal University, Stavropol, Russian Federation E-mail: iskl@bk.ru

Аннотация

Система обеспечения информационной безопасности объекта рассматривается как многокритериальная задача выбора. Анализируется возможность применения методов многокритериальной оптимизации к проектированию системы защиты инфокоммуникационного объекта. Представлены формализованные процедуры решения многокритериальной задачи выбора; показаны алгоритмы расчета и обоснования выбора.

Ключевые слова: исследование операций, принятие решений, многоэтапная задача, качество решения.

Abstract

The system of ensuring the information security of an object is considered as a multi-criteria task of choice. The possibility of applying multicriteria optimization methods to the design of an infocommunication facility protection system is analyzed. Formalized procedures for solving a multi-criteria selection problem are presented; algorithms for calculating and justifying the choice are shown.

Key words: operations research, decision-making, multi-stage task, solution quality.

Introduction. The relevance and need to improve the design tools for information security systems (ISS) are due to such factors as the involvement in info communication processes of people who often have little understanding of the methods and principles of information security and confidentiality; increasing the complexity of technological processes associated with data processing; growth of volumes of the information which circulates at the enterprises/organizations. The high level of digitalization of the processes of collecting, processing, transmitting and storing information, the transition to electronic document management systems, the introduction of automated systems for various purposes and degrees of complexity makes the problem of information security relevant not only for specialists, but for all participants in info communication processes.

The development and implementation of modern systems for the integrated protection of info communication objects should, a priori, be based on an analysis of objective data on the degree of actual security of an object, determining the protection class, statistical data on threats and attacks on the system, and assessing the possible consequences of unauthorized access (UA) to information. The modern approach to the design of the information security system is based on the use of typical and standard methods [1] that ensure security at the hardware, software, physical and technical levels, which in itself increases the vulnerability of the information security system.

An analysis of modern research into the problem of developing effective information security systems suggests that most of the work is devoted to applied aspects of design: the choice of protection tools, the assessment of the economic efficiency of the protection system, etc.

Most research is focused on a specific subject area. So, the studies of Korobkin D.I., Popov A.D., Rogozin E.A., Khisamov F.G., Sherstobitov R.S. devoted to the design of means of protection of automated systems [2-4].

The author seemed interested in the approach to modeling design processes, presented by the team of authors Prokushev Ya.E.

In the work presented by a team of authors [5], the design of a protection system is positioned as a complex task, the solution of which requires a systematic integrated approach and the use of mathematical modeling methods.

Research on the possibilities of mathematical modeling in the development of ISS today are, as a rule, of a highly specialized nature, focused on the economic and organizational aspects of designing ISS or, as mentioned above, on the subject area to which the object of protection belongs [6-8].

The idea of an integrated approach to the creation of ISS was reflected in the works of Glebova S.A., Konichenko A.V. Larionova I.P., Putilkina K.I., Khoreva P.B. Models based on expert assessments and intelligent decision support systems are considered in the works of Baranova E.M., Baranov A.N., Borzenkova S.Yu., Vitenburg E.A., Glushchenko I.S., Nikishova A.V.

It was practically not possible to find the results of studies published in the open press on the application of criterion optimization to the problems of choosing the optimal structures of the information security system. The concept of multi-criteria in adapting to the process of designing the information security system in combination with other methods of operations research will make it possible to make a quantitative justification of the decisions made and determine the optimal alternative in the decision space.

The purpose of the article is to expand the understanding of the possibilities of operations research as a science of quantitative justification of decisions made, to substantiate the expediency of adapting multi-criteria choice algorithms to solving the problem of designing information security systems.

Materials and Methods. Modeling of complex systems, as a process of building a certain image of the object under study, can be performed using different methods. The choice of method is determined by the purpose of modeling (cognitive or practice-oriented), modeling tools (material, abstract), resources and research capabilities. The methods of mathematical modeling that underlie operations research make it possible to build models of various types, take into account uncertainty factors, the probabilistic nature of the behavior of the object under study, etc. All of the above has become a decisive argument when choosing methods for studying such a subject area as information security systems, the order of their development.

The methodological basis for the study of the problem of choice in the development of information security systems used the methods of control theory, decision theory, the theory of multi-criteria optimization, the main provisions and principles of system analysis, for collecting and processing data, methods of expert assessments, probability theory and methods of mathematical statistics were used.

Results and discussion. The choice and decision-making in solving complex problems, which in essence is the modeling of a complex protection system for an info communication object, is based on methods of multicriteria optimization. To form selection algorithms under conditions of uncertainty, it is advisable, in the author's opinion, to classify multicriteria tasks on three grounds: the number of objects, the degree of complexity, and the result obtained.

According to the number of objects, multicriteria tasks (MCT) are proposed to be divided into two classes: tasks with a finite number of objects (discrete) and with an infinite number of objects (continuous); the degree of complexity of the task is determined by its dimension (the number of criteria) and the presence of a relationship between the criteria; the result can be obtained in the form of an ordered set, the most preferred alternative, an alternative with a given degree of utility, and in the form of an alternative that is Pareto optimal [9].

Assuming that the task of designing the information, security system is discrete, we identify it as some object, a complex system that has a goal; tasks that need to be solved to achieve the goal; system input, in this case these are potential threats and attacks; the output of the system, that is, the measures that are taken to transform the input into an output in order to achieve the goal; a system of restrictions and a complex of processes occurring in the system. This is the set of parameters $x_{1,}\ x_{2,}\ ...,\ x_n$ whose optimal values are to be found.

To solve a discrete multi-criteria problem of designing the information security system in such an interpretation, it is required to determine a set of criteria $K_{1,}\ K_{2,}\ \dots K_m$ (i =1…, m), which are interconnected and which form *a space* of criteria; the domain of definition of the parameters is given in the form of a system of constraints and an objective function $f_1(x_1,.,x_m);.;\ k_n=f_m(x_1,.,x_m)$.

In the case when the criteria have a formal representation, their number and numerical values are correctly defined, then it is legitimate to represent the discrete problem in matrix form (Table 1), where the rows of the matrix are the number of analyzed objects, in this case, information security systems, the columns are the criteria, according to which each object is evaluated; at the intersection of rows and columns, the numerical values (characteristics) of each object according to one or another criterion.

Table 1. Matrix representation of a discrete multicriteria problem

Criteria Options	**K1** _	**K2** _	**….**	**Km** _
x_1	x_{11}	x_{12}	…	x_{1m}
x2 _	x21 _	x22 _	…	x_{2m}
….			…	
x_n	x_{n1}	x_{n2}	…	x_{nm}

The practice of real design allows us to state that in most cases, customers of the design system and the decision maker (DM) operate with poorly formalized criteria, which poses a choice problem for the developers of the information security system: to use heuristic methods that have a number of limitations and features to solve the ISS, or to apply classical decision theory methods (convolution, binary relations, search for a guaranteed result, etc.).

Without dwelling in detail on the heuristic methods for solving the MCT design of the information security system, we note two positions that are most important from the point of view of the author: heuristics has serious limitations on the dimension of the space of criteria and the space of alternatives. The assertion that a person is able to operate with a limited number of categories in the decision-making process does not require special evidence. The use of human-machine selection procedures is beyond the scope of this study and is not subject to discussion. The second, no less important factor that refutes the expediency of using heuristic methods to solve the ISS of MCT design is the problem of adequate evaluation of experts participating in the selection procedure, and the methodology for coordinating their estimates.

Considering all of the above, we return to the classical methods of solving the ISS. The system for ensuring the information security of an object is a complex set of tools and methods of an organizational and technical nature, which implies the presence in the system of means of anti-virus, network, cryptographic, software and hardware, and physical protection of the object. The whole set of means of protection is formed into a certain system, which must comply with the terms of reference.

In accordance with this approach, the solution space is formed:

A { A 1, A 2, A 3, A 4},

where A1 - IPS with full protection; A2- ISS with controlled (programmable) protection; A3 - ISS with encryption; A4 - complex ISS.

The selection procedure consists in finding an alternative that meets the requirements of the decision maker, while it is proposed to accept the following statements as restrictions:

- for each alternative there is a utility function;
- the choice on the decision space is deterministic, that is, the alternative is evaluated in its current state, without any attempts to predict and analyze history;
- the choice is made in terms of the integrity and completeness of information about the proposed alternative.

The space of criteria is formed:

K {K1, K2, K3, K4, K5},

where K1 is the functionality of the ISS; K2 - reliability; K3-provided security level; K4 - control flexibility; K5-cost.

A matrix model of the ISS is being built (Table 2), which contains the quantitative characteristics of the possible options for the ISS and will become the basis for finding the optimal alternative.

The estimates given in the table were made on a ten-point scale by a group of experts using the method of active sociological testing of analysis and control [10].

Table 2. Quantitative characteristics of the solution space

	Functionality _	Reliability _	security level	bending - bone	stop bridge
ISS with full protection	6	7	4	2	5
ISS with controlled protection	5	7	8	3	6
ISS with classification	4	6	8	5	7
Integrated ISS	8	3	6	4	9

Table 3 shows the rank matrix for the criteria space.

Table 3. Matrix of ranks for the space of criteria

Alternatives	Criteria					Total rank R $_i$
	K1	K2	K3	K4	K5	
A1	2	1	3	4	4	14
A2	3	1	1	3	3	eleven
A3	4	2	1	1	2	10
A4	1	3	2	2	1	9

After constructing the matrix of ranks and determining the space of ranks R {R 1, R 2, R 3, R 4}, it is possible to transform the MCT to a single-criteria problem; alternatives are ordered in ascending order of rank; the alternative with the minimum rank value is considered to be consistent. For the data used in tables 2 and 3, the rank space has the form R {9,10,11,14}, it is advisable to give preference to alternative A4.

The transformation of the MCT to a single-objective problem can serve as an additional tool for substantiating the choice on the solution space. As the main method, the method of weight coefficients is proposed, the idea of which is that the criteria are given a numerical value, reflecting its significance, weight in a given system for evaluating alternative solutions. In the evaluation table of alternatives (table 4), the criteria are entered in descending order of weight, for each alternative, the significance coefficient is calculated; for each column is the sum; the alternative with the highest score is considered agreed.

Table 4. - Evaluation of alternatives by the method of weight coefficients

Criteria	Weight	Alternatives			
		A1	A2	A3	A4
K2	1.0	7	7	6	3
K3	0.8	3,2 _	6.4	6.4	4.8
K1	0.7	4.2	3, 5	2.8	5.6
K4	0.6	1.2	1.8	3	2, 4
K5	0.5	2.5 _	3	3.5	4.5
Sum		18.1	21.7	21.7	20.3

Alternatives A2 and A3 are more preferred in a given space of alternatives.

The use of two selection algorithms in solving a multi-criteria problem gave ambiguous results: when reducing the problem to a single-criteria one, preference was given to the alternative A4 - “Complex ISS”; the method of weight coefficients determines A2 - "ISS with controlled protection" and A3 - "ISS with encryption" as optimal alternatives. Obviously, such a discrepancy in choosing the optimal strategy is not fatal; the fact of “disagreements” requires additional research of the solution space from the decision maker. Research can be carried out in at least two directions: this ISS can be solved by other methods: formal (pairwise comparison, ordering, Pareto optimization) and / or heuristic (commission method, expert assessment method, morphological box method, etc.) The second direction of research should be aimed at proving the reliability of input data for calculations and eliminating both direct errors and incorrect processing of data received from experts.

The choice of the optimal solution is an iterative process, at each iteration it is necessary to establish a correspondence between the system of preferences declared at the beginning of the procedure with those claims that exist at a particular stage of the choice. Formal methods based on the criteria-based approach to substantiate the decisions made make it possible to keep the system of preferences unchanged at all stages of the justification of the choice.

Conclusions. ISS design is a complex, semi-structured process in which there are connections and relationships between objects and subjects of design. The presence in the system of links that are not determined by quantitative characteristics poses a difficult task for the decision maker to choose. You can optimize the selection process by introducing restrictions on the number of alternatives offered for comparison; on the number of criteria for evaluating alternatives. The formalized methods of choice justification discussed above operate with specific categories, require correct quantitative determination of input data, which is some limitation on their use for the study of complex systems. Positioning the problem of modeling the information security system as a multicriteria problem, for which the initial data were obtained by heuristic methods, expands the possibilities of operations research and provides the decision maker with an effective tool for justifying the choice.

ЛИТЕРАТУРА

1. Гарькушев А.Ю., Супрун А.Ф., Сысуев С.Ю. Методика интеграции модулей защиты информации в отечественные системы автоматизированного проектирования в кораблестроении // Проблемы информационной безопасности. Компьютерные системы. 2022. № 1. С. 121-131.
2. Коробкин Д.И., Рогозин Е. А. Модель оценки эффективности программной системы защиты информации автоматизированной системы на начальном этапе проектирования // Наукоемкие технологии в космических исследованиях Земли. 2014. Т. 6. № 5. С. 72-74.
3. Попов А.Д. Алгоритм проектирования систем защиты информации в автоматизированных системах // Охрана, безопасность, связь. 2016. № 1-2. С. 243-245.
4. Хисамов Ф.Г., Шерстобитов Р.С. Принципы формирования комплекса средств защиты информации при проектировании автоматизированных систем в защищенном исполнении // Технологии разработки информационных систем. Материалы VIII Международной научно-технической конференции (Геленджик, 03–09 сентября 2017 г.). Ростов н/Д, ЮФУ, 2017. С. 71-76.
5. Прокушев Я.Е., Пономаренко С. В., Пономаренко С. А. Моделирование процессов проектирования систем защиты информации в государственных информационных системах // Computational nanotechnology. 2021. Т. 8. № 1. С. 26–37. DOI: 10.33693/2313-223X-2021-8-1-26–37.
6. Борисов Р. С. Обзор математических моделей для модели оптимизации комплексной системы защиты информации в современных автоматизированных системах обработки данных // Международный журнал прикладных наук и технологий Integral. 2019. № 2-1. С. 7.
7. Кляус Т.К., Гатчин Ю.А. Математическая модель оценки эффективности системы защиты информации от атак типа advanced persistent threat // Волновая электроника и инфокоммуникационные системы. Сборник статей XXIII международной научной конференции (Санкт-Петербург, 01–05 июня 2020 г.). СПб., СПбГУАП, 2020. С. 250-260.
8. Скрыль С.В. Математическая модель для оценки эффективности механизмов защиты информации от вирусных атак // Промышленные АСУ и контроллеры. 2018. № 4. С. 54-61.
9. Клименко И. С. Комплексная защита объектов информатизации: системный анализ и модели управления. М.: КДУ, Добросвет, 2019. 147 с. DOI:10.31453/kdu.ru.91304.0085.
10. Клименко И. С. Морфологический подход Фрица Цвикки к проектированию систем комплексной защиты инфокоммуникационных объектов // Современная наука и инновации. 2021. №3. С. 52-60.
11. Klimenko I.S. Mathematical model of complex protection of an infocommunication object based on "playing with nature" // Modern Science and Innovations. 2022. No. 1. (37). С. 34-43.

REFERENCES

1. Gar'kushev A.Yu., Suprun A.F., Sysuev S.Yu. Metodika integracii modulej zashchity informacii v otechestvennye sistemy avtomatizirovannogo proektirovaniya v korablestroenii. // Problemy informacionnoj bezopasnosti. Komp'yuternye sistemy. 2022. No. 1. P. 121-131.
2. Korobkin D.I., Rogozin E. A. Model' ocenki effektivnosti programmnoj sistemy zashchity informacii avtomatizirovannoj sistemy na nachal'nom etape proektirovaniya // Naukoemkie tekhnologii v kosmicheskih issledovaniyah Zemli. 2014. Vol. 6. No. 5. P. 72-74.

3. Popov A.D. Algoritm proektirovaniya sistem zashchity informacii v avtomatizirovannyh sistemah // Ohrana, bezopasnost', svyaz'. 2016. No. 1–2. P. 243-245.

4. Hisamov F.G., Sherstobitov R.S. Principy formirovaniya kompleksa sredstv zashchity informacii pri proektirovanii avtomatizirovannyh sistem v zashchishchennom ispolnenii // Tekhnologii razrabotki informacionnyh sistem. Materialy VIII Mezhdunarodnoj nauchno-tekhnicheskoj konferencii (Gelendzhik, 03–09 sentyabrya 2017 g.). Rostov n/D, YUFU, 2017. P. 71-76.

5. Prokushev YA.E., Ponomarenko S.V., Ponomarenko S.A. Modelirovanie processov proektirovaniya sistem zashchity informacii v gosudarstvennyh informacionnyh sistemah // Computational nanotechnology. 2021. T. 8. No. S. 26-37. DOI: 10.33693/2313-223X-2021-8-1-26–37

6. Borisov R.S. Obzor matematicheskih modelej dlya modeli optimizacii kompleksnoj sistemy zashchity informacii v sovremennyh avtomatizirovannyh sistemah obrabotki dannyh // Mezhdunarodnyj zhurnal prikladnyh nauk i tekhnologij Integral. 2019. No. 2-1. P. 7.

7. Klyaus T.K., Gatchin YU.A. Matematicheskaya model' ocenki effektivnosti sistemy zashchity informacii ot atak tipa advanced persistent threat / Volnovaya elektronika i infokommunikacionnye sistemy. Sbornik statej XXIII mezhdunarodnoj nauchnoj konferencii. (Sankt-Peterburg, 01–05 iyunya 2020 g.). SPb, SPbGUAP, 2020. P. 250-260.

8. Skryl' S.V. Matematicheskaya model' dlya ocenki effektivnosti mekhanizmov zashchity informacii ot virusnyh atak // Promyshlennye ASU i kontrollery. 2018. No. 4. P. 54-61.

9. Klimenko I. S. Kompleksnaya zashchita ob"ektov informatizacii: sistemnyj analiz i modeli upravleniya. Moskva: KDU, Dobrosvet, 2019. 147 p. DOI:10.31453/kdu.ru.91304.0085.

10. Klimenko I. S. Morfologicheskij podhod Frica Cvikki k proektirovaniyu sistem kompleksnoj zashchity infokommunikacionnyh ob"ektov // Sovremennaya nauka i innovacii. 2021. No. 3. S. 52-60.

11. Klimenko I.S. Mathematical model of complex protection of an infocommunication object based on "playing with nature" // Modern Science and Innovations. 2022. No. 1. (37). P. 34-43.

ОБ АВТОРЕ / ABOUT THE AUTHOR

Клименко Ирина Сергеевна, доктор технических наук, доцент, ведущий научный сотрудник отдела организации проектно-грантовой деятельности СКФУ (Пятигорский институт), E-mail: iskl@bk.ru

Irina S. Klimenko, Dr. Sci. (Tech.), Associate Professor, Leading Researcher of the Department of Organization of Project and Grant Activities of NCFU (Pyatigorsk Institute), E-mail: iskl@bk.ru

Дата поступления в редакцию: 12.12.2022
После рецензирования: 13.01.2023
Дата принятия к публикации: 07.02.2023