И. С. Клименко [I. S. Klimenko] [1]
Н. А. Медетов [N. A. Medetov] [2]

УДК378.1+311.2

КОНЦЕПТУАЛЬНЫЕ И МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ КОМПЛЕКСНОЙ ЗАЩИТЫ СУБЪЕКТОВ И ОБЪЕКТОВ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ

CONCEPTUAL AND METHODOLOGICAL FRAMEWORK FOR THE COMPREHENSIVE PROTECTION OF SUBJECTS AND OBJECTS OF INFORMATION RELATIONS

[1] ФГАОУ ВО «Северо-Кавказский федеральный университет», Институт сервиса, туризма и дзайна (филиал) СКФУ в г. Пятигорск, Россия, E-mail: iskl@pfncfu.ru

[2] Костанайский государственный педагогический университет, г. Костанай, Казахстан

Аннотация. *Актуализация проблемы комплексной защиты объектов информатизации – это результат стремительного развития информационных технологий, которые привели не только к модернизации информационных отношений, но выявили необходимость создания комплексных систем обеспечения информационной безопасности объектов, как значимой компоненты концепции информационной безопасности региона и государства в целом. Информационная безопасность, по сути, это защищенность субъектов и объектов информационных отношений от угроз внутреннего и внешнего характера. Необходимость исследования проблем организации комплексной защиты субъектов/объектов информационных отношений обусловлена рядом причин, среди которых увеличение интенсивности информационных потоков, повышение требований к степени защищенности конфиденциальной информации, рост числа атак на системы хранения данных и каналы связи и др.*

Ключевые слова: методы описания сложных систем; математическое моделирование системы комплексной защиты; детерминированные модели; методы оптимизации комплексной защиты объекта.

Abstracts. *Actualisation of the problem of complex protection of information objects is the result of the rapid development of information technologies, which not only led to the modernization of information relations, but also revealed the necessity to create complex information security systems as a significant component of the information security concept of the particular region and the whole state. Information security, in fact, is the protection of subjects and objects of information relations from internal and external threats. The problems of organizing complex protection of subjects / objects of information relations should be studied because of an intensity of information flows, increasing requirements for the level of protection for confidential information, the growing number of attacks on data storage systems and communication links, etc.*

Key words: methods of description of complex systems; mathematical modeling of complex protection systems; deterministic models; methods for optimizing the complex protection of an object.

Introduction. The information security management system of an object is a complex dynamic system of collecting, processing, storing and transmitting of information. Fuzzy structure of its subsystems, the multiple nature of the system elements require developers to take into account all factors (including weak formalized), which affect the quality of information security.

Information security of subjects and objects of information relations means a flexible and rapid response to threats and attacks.

Traditional methods of information security management are mostly oriented towards the use of narrowly specialized methods of protection. To some extent, this approach can be described as “separatist”, as it allows to solve the problem of ensuring information security in certain areas:

– protection of computer networks;
– anti-virus protection;
– cryptographic methods of data protection;
– technical means of protection, etc.

The expediency of such an approach requires additional study, but to develop complex protection of informatization objects, it is necessary to implement the principles of a systems approach, adapt the mathematical apparatus of operations research and decision theory to solve information security system problems. That is why the creation of models, methods and algorithms for complex protection of information objects, which are to predict development and manage

risks, ensure information security of subjects and objects of information relations is, in the authors' opinion, of great theoretical and applied interest.

Materials and methods

System analysis of the problem of complex protection of subjects and objects of information relations. Complex protection of an object is a system of dynamically linked elements, the management of which should be based on a scientific basis. The total framework of the theory of systems and the logic of the systems approach, in relation to the problems of information security management, make it possible to classify and identify control objects by the levels of complexity of them:

Level 1 – the level of a static structure or the level of bases. At this level of complexity, the subjects of information exchange in the information protection system are considered in statics;

Level 2 – a simple dynamic system with predefined, mandatory actions, such as user identification, authorization in the system, etc .;

Level 3 – the cybernetic system, i.e. a "thermostat" system in which the transmission and analysis of information constitutes an essential part of the system, providing the ability to control the system;

Level 4 – open system, self-preserving structure. At this level of the object security system, the object of protection is divided into its constituent parts, and the individual protection mechanisms are formed for each component.

Level 5 – in a complex system, functions are differentiated: it is the division of objects of protection, respectively, the definition of the subjects implementing this protection;

Level 6 – mobility, awareness and teleological behavior. At this level the receivers of information and a highly developed system of response to external influences appear. For information security systems, a profile of a potential attacker is determined at this level of complexity, a system for identifying and diagnosing attacks is built, statistics on reflected and realized threats are collected, and so on;

Level 7 – At this level the ability of the system to analyze the situation, the ability to adapt, and self-study are added to all previous conditions. In the information security management system of a facility, this level of complexity presupposes the existence of a complex information protection plan, which allows for managing either by rejection or perturbation;

Level 8 – management of the complex protection system of an object at this level of complexity requires taking into account the influence of behavioral factors that have a significant impact on the effectiveness of protection. Such factors should include professional incompetence of information exchange participants in terms of information security, lack of responsibility when working with confidential information, etc.

Level 9 – unknowable systems. The probabilistic nature of the interaction in the "object of protection - means and methods of protection - the attacker" make a part of the protection system "closed" for study.

The solution of problems of complex systems managing is based on the integration of formal and informal modeling methods, the nature of which requires the decomposition of the control object, which, as a rule, practically does not take into account interconnections with other subsystems. As a consequence, the solution of individual local problems does not provide a complete picture of the system as a whole. When forming a complex plan, we need a fundamentally different approach, based on a study of the decision-making process that unites the system of relations, the organizational structure, and the development of the system and the effect of uncertainties. This approach allows you to create and explore more complex models of behavior in the process of administrative management, that is, it will allow you to use the results of research in the field of special management issues.

Hierarchical security management system of an info-communication facility has a hierarchical structure:

– at the first level, there is a system of material processes and distribution;

– at the second level – the processes of making programmed decisions;

– at the third level, non-programmable decision making processes, which are necessary for managing the processes of the lower levels, their re-planning and reassessment of the system parameters.

The main attention in the hierarchical structure should be given to the analysis of information flows and the synthesis of the information model of the control object.

All existing methods for describing complex systems can be divided into two classes: quantitative (analytical) and qualitative, which, as a rule, are subjective.

Quantitative methods for describing systems

The main task of modeling, as a tool for describing a complex system, is to correctly interpret the goals of the system, its properties, parameters, characteristics, behavior in certain conditions. Understanding of the structure of a complex system allows the researcher to independently determine the level of elementaryness of the system, to identify the main structural elements (subsystems and relations between them), to determine the level of description of the system.

Such research is possible only if there is a mathematical description of the process of functioning of the system, i.e. its mathematical model.

The complexity of real systems does not allow building "absolutely" adequate models for them. The mathematical model (MM) describes some simplified process, which presents the main phenomena involved in the real process and the main factors acting on the real system.

What phenomena are the main ones, what factors are the main factors – essentially depends on the purpose of the model, what research it is for. Therefore, the process of functioning of the same real object can receive different mathematical descriptions depending on the task.

As there are a lot of mathematical models of a complex system and all of them are determined by the adopted level of abstraction, consideration of tasks at any one level of abstraction allows you to give answers to a certain group of questions, and to get answers to other questions, you must conduct research at another level of abstraction. Each of the possible levels of abstraction has limited capabilities that are unique to this level. To get the maximum completeness of information, it is necessary to study the same system using different types of models.

By convention, the first four levels relate to the highest levels of system description, and the last four – to the lowest [1].

The highest levels of systems description

The linguistic level of description is the highest level of abstraction, which operates with terms and functors. Terms are identifiers of system components, their names. Functors - statements that define the relationship between terms. So, the system of complex protection of information objects at the linguistic level of description can be represented as a set of identifiers, classifiers and unified forms of presentation of documents to be protected. This part of the system, defined as terms, must be supplemented with a description of the links; in this case, the role of the functor is played by the information model of the protected object.

Lower levels of system description

The logical-mathematical level of the description of systems is widely used to describe complex systems associated with information processing, formalizing the activities of devices in which information acts as a property of objects and phenomena (processes) to generate a variety of states. For the system of complex protection of information objects, the logical-mathematical description level should contain algorithms for collecting, processing, storing and transmitting data and specific modules providing the necessary level of security.

At the dynamic level of the abstract description of systems, the key terms are the concepts of "input" and "output" of the system and the system itself is considered as an object ("black box") inside which the processes of discrete or continuous nature can take place. The main purpose of such a description is to establish the relationship between the input and output of the system, to determine its state. The system of complex protection of information objects represented as a "black box" is a combination of a set of problems at the input of the system and, accordingly, a set of goals at the output.

For example, the problem to be solved: provide a high level of document security. As a solution to the problem - the development of cryptographic protection algorithms; use of secure data transmission channels; increasing the personal responsibility of participants in the data transfer process.

For example, problems that need to be addressed: the high level of confidentiality of the documents to be protected; as a solution to the problem: the development of cryptographic protection algorithms; use of secure data transmission channels; increasing the personal responsibility of participants in the data transfer process.

The heuristic level of the abstract description of systems provides for the search for a satisfactory solution of control problems due to the presence in a complex system of a person who is able to generalize the experience of solving similar problems, to build an algorithm that cuts out "unsuitable" solutions using game methods, simulation modeling, brainstorming and other methods which are based on human intellectual activity.

Qualitative methods for describing systems

If it is not possible to identify patterns of development of a complex system using analytical methods, qualitative description methods are applied.

Brainstorming is a group method for solving creative problems, based on a special technology of searching for alternative solutions. The method involves the free expression of ideas in the process of discussing the problem; any ideas are welcomed, even if they, at first glance, look absurd. The number of ideas should be as large as possible, that is, the mechanism for generating alternatives allows for their combination, addition, development, use of part of the alternative, etc. The effectiveness of the procedure largely depends on the quantitative and qualitative composition of the participants, their professional competence, occupation, sphere of professional interests, work experience. Interesting results are given by groups of participants, which include experts from various fields.

Brain relay is a special method of solving creative problems, which is based on the method of active sociological testing, analysis and control [2].

Scenario method. A scenario as a description of the development of a situation, taking into account the initial state of the system and plausible proposals for its development, can be: pessimistic, optimistic, most likely taking into account the coefficient of optimism / pessimism. The main idea of the method is to analyze the capabilities of a complex system and identify ways of development with minimizing loss / damage. The multivariance of the method allows us to group alternatives into classes and determine the optimal strategy based on the principle of mixed strategies. In design of a scenario, quantitative methods of operations research, system analysis methods (decomposition and aggregation), and structural correlation analysis methods can be used.

The method of scenario, as a practical implementation of the sequential resolution of uncertainty method, aimed at determining the most likely paths for the development of a system / complex situation / problem, is carried out in several stages:

– problematization: setting a task / issue;
– identification of factors, external influences, etc .;
– determining the expected parameters of the system;
– formation of development proposals and their selection;
– comparative analysis of system parameters taking into account the influence of external influences;
– generation of a probabilistic order of events;
– impact analysis;
– adjusting behavior strategies.

Methods of expert assessments. Examination is a procedure that allows you to get a competent conclusion on the studied problem. To quantify the degree of consistency of expert opinions, the coefficient of concordance is used.

$$W = \frac{12d}{m^2(n^3 - n)},$$

Where

$$d = \sum_{i=1}^{n} d_i^2 = \sum_{i=1}^{n} [\sum_{i=2}^{m} r_{ij} - 0.5m(n+1)]^2$$

m – the number of experts,

j= $\overline{1,m,n}$ — the number of considered properties,

$i = \overline{1,n;r_{ij}}$ – the place that was taken by the property i of the j-th expert;

d_i – is the deviation of the sum of ranks in the *i*-th property from the arithmetic mean of sums of ranks in n properties.

The coefficient of concordance W makes it possible to assess how consistent the series of preferences, constructed by each expert, are.

Its value is within 0≤W≤1; W=0 means the exact opposite, and W = 1 means complete coincidence of the value of the criterion by evaluation of all experts.

The opinion is considered consistent when W = 0.7 ... 0.8. If the value of the coefficient of concordance, indicates a weak consistency of expert opinions, it is necessary to analyze whether there is indeed no unity of opinion within the group of the totality of experts. Additional information on the coincidence of expert opinions can be obtained by determining the degree of agreement in a pair of experts A and B by calculating the coefficient of pair rank correlation:

$$\rho_{AB} = 1 - \frac{\sum_{i=1}^{n} \psi_1^2}{\frac{1}{6}(n^3 - n) - \frac{1}{n}(T_A + T_B)},$$

where ψ_i is the difference (in absolute value) of the values of the ranks of the assessments of the i -th property, appointed by experts A and B: $\psi_i = \left| R_{A_i} - R_{B_i} \right|$; T_A и T_B –indicators of related ranks of assessments of experts A and B.

The coefficient of pair rank correlation takes values $-1 < \rho < +1$.

The value $\rho = +1$ corresponds to the complete coincidence of assessments in the ranks of the two experts (complete consistency of the opinions of the two experts), and $\rho = -1$ – two mutually opposite opinions of the experts.

The Delphi method is a well-known method of individual peer review, which does not involve a collective discussion procedure.

This format of the peer review procedure is intended to reduce the desire of the participants in the examination to join the opinion of the most authoritative expert, suppress the expert's desire to refuse to publicly express their own opinions and follow the majority opinion.The idea of the method is to organize a multi-step (iterative) expert survey, while at the first iteration the experts may not argue the answers; after processing the results of the first iteration, questions can be refined, modified, and the answers of the experts should be reasoned; the third, fourth iterations, in essence, the repetition of the previous steps. Stable, unchanging expert answers are a sign of the completion of the examination process.

Disadvantages of the method: the complexity; Experts are not always ready to work in a multi-step format.

Advantages of the method: an individual mode of operation reduces the psychological pressure on the expert, which increases the objectivity of the expert assessment. The procedure can be used as an introductory, "immersive" in conducting the method of scenarios.

Method "objective tree" The idea of the "objective tree" method involves building a hierarchical structure, at the top level of which is a global object, then the global object is decomposed into sub-objects, down to the elementary level, which is determined by the researcher. So, with regard to the information security management system, the objective tree can have the following form: the global object is to minimize the damage from threats.

Objectives of the first level:

1 – self-determination in position;

2 – self-determination in a situation.

Second level objects:

1.1 analysis of opportunities; 1.2 preference analysis; 1.3 - forecast of results.

2.1 – analysis of the sources of threats; 2.2 – forecast of possible damage.

Advantages of the method in its invariance with respect to the subject area; Tree-like hierarchical structures can be used not only within the framework of the object-setting of the subject of management of a complex system; A possible area of application of this method is the construction of a hierarchy of directions for the development of a complex system and the prediction of results. When using the concept of "predication graph", it is possible to more accurately define the concept of a tree as a connected digraph, each pair of nodes of which is connected by a single chain.

Morphological methods. The main idea of morphological methods is to systematically find all "conceivable" solutions to a problem or system implementation by combining selected elements or their signs. Currently, there are three known methods of morphological research: the method of systematic field coverage, the method of denial and design, the morphological box method.

The most common is the morphological box method. Its idea is to build a matrix containing possible solutions to the problem and their parameters; analysis of possible combinations of options, their evaluation allows you to make a choice in favor of the best option. The matrix can be two-dimensional and three-dimensional.

Methods of system analysis: decomposition and aggregation

Techniques that implement system analysis procedures under specific conditions are intended to formalize the system research process, in cases where the researcher does not have sufficient information about the system, which allows to choose an adequate method of a formalized system representation.

Principles of complex protection system modeling

The concept of information security of an object, implemented in a complex information protection plan, ensures effective protection, subject to certain fundamental principles:

– systematic and integrated approach;
– compliance with current legislation;
– unambiguous understanding by developers and users;
– continuity, timeliness and sufficiency;
– economic feasibility;
– separation of functions and delegation of authority;
– accordance of user rights to official authority and personal responsibility;
– protection system flexibility;
– mandatory control.

Analysis of the problem of managing information security of objects highlights the development of models and algorithms for information security [3, 5].

Defining the process of forming a complex plan of information protection of an object as a complex dynamic system, we will assume that effective management should be based on the principles of classical management of complex systems, methods of system analysis using mathematical modeling of information objects, information exchange processes.

Information security management systems have certain specific features:

– to assess the quality of information security is difficult to apply direct measurement methods;

– the task of assessing the quality of information protection is complex, its solution requires various methods, which should be based on a systematic approach;

– models and algorithms for managing information security of an object should have a scientific basis and use modern technologies. The analysis of management methods for complex protection of information objects that are used in real practice, served as the basis for the choice of modeling as a tool for synthesizing an information security management system for an object.

The conceptual model of the information security system is based on the life cycle of the system:

1. Determining the need for the final product.
2. Planning the trajectory of the control object. .
3. Control of the actual state of the control object, analysis of the need / feasibility of forming control actions.
4. Regulation.

Table 1 presents a conceptual model of managing information security of an object in the form of life cycle stages.

Table 1

Stages of the process of the information security management of an object

Stage name	**Stage content**
Risk analysis	1. Determine the object of protection. 2. Determine the profile of the attacker. 3. Analysis of problems and their source (threat; vulnerability; violators). 4. Creating a quality management system for training specialists.
Policy Formation	1. The system of views on the problem of information security: – goals and objectives of protection. – analysis of the current state and security threats; – legal basis of the object information security management system; – organizational, technological procedures, methods and means of ensuring the information security of an object.
Planning	1. Determination of the required level of security of the object. 2. Accounting of resources that require protection: information, tasks, documents, communication systems, servers, etc. 3. Training of staff responsible for ensuring the security of information and its processing in each unit. 4. Drawing up a comprehensive plan of information protection using physical and technical (software and hardware) tools to protect system resources and continuous administrative support for their use.

Implementation of a comprehensive plan	1. Practical actions to ensure the security of information; coordination of actions of persons responsible for ensuring information security in the units. 2. Identification, reflection and liquidation of the consequences of the implementation of various types of information security threats. 3. Making management decisions aimed at improving the legal, regulatory, technical and organizational support for the information security of an object.
Intrusion Detection	1. Development of a mechanism for rapid response to security threats. 2. Accounting for potential and realized threats. 3. Identification of sources of threats. 4. Identification of the causes and conditions conducive to the realization of the threat.
Analysis and control	1. Development of a system for assessing the quality of protection of information objects. 2. Development of technology for assessing the quality of protection of information objects. 3. Creation of a quality control system for the protection of information objects. 4. Monitoring the compliance by all parties of information relations with the requirements for maintaining information security at workplaces / in departments / at the facility as a whole. 5. The accumulation of statistics, analysis of the situation and making changes to improve the quality of training.

To create a model suitable for solving specific problems, we need to determine the level of the hierarchy on which the control object is located, goals and objectives. The qualitative description of the object is transformed into a system of formalized indicators that are to be measured using the method of expert assessments, the method of analyzing hierarchies, and the methods of game social simulation.

Information security system management, as a rule, takes place under conditions of uncertainty under the influence of objective factors: an increase in the number of informatization objects; great people attraction to the information processing; avalanche-like growth in the number of information services; low awareness of the subjects of information relations about the appropriateness and the need to protect data / information / objects of informatization, etc.

Many factors affecting the quality of protection of objects and subjects of information relations requires the development of methodological bases for the formation of a complex protection of an informatization object, especially since even the term "quality of protection" is subjective. The term "quality of information protection" is proposed to mean a quantitative indicator reflecting the amount of damage caused by attackers to the object of protection. General view of the mathematical model:

$$W = \min F \{Ai, xj\}$$

where W is an indicator of the quality of information security;

A_i – active and passive factors that ensure the implementation of a complex protection plan (resources, methods, tools, technologies);

x_j – controlled variables, with which you can get the extremum of the utility function;

F – functional, which determines the type of relationship between the criterion of efficiency and the other factors of the model.

Results. The system analysis of the problem of assessing the quality of protection and managing the security of an object allows to divide the existing approaches into classes: class A are methods for assessing the degree of compliance of the result with the user's system of preferences. Of course, this is a subjective approach, which, in fact, is nothing more than a statement of fact that does not provide the ability to conduct operational management of the information security system. Class B includes methods for assessing the quality of information protection, which are based on mathematical models and algorithms that provide the ability to compare quantitative indicators of a comprehensive plan of information protection, both in terms of the costs of implementing the plan and in terms of the results obtained.

Despite the obvious differences in methods for assessing the quality of information protection which belong to different classes, their basis is the general principles of systems theory, control theories and methods for researching operations [4].

It is the general systemological basis that allows to build a sequence of actions necessary to evaluate the quality of information protection at an object:

– definition of the standard;

– calculation of the trajectory of the control object;

– formation of a set of methods / means of assessing the state of the system (observation, measurement, etc.)

– creation of a mechanism for implementing control actions;

– comparison of the actual state (behavior) of the system with the standard;

– analysis of existing deviations;

– development of control actions;

– return the system to the previously calculated trajectory of movement / correction of the trajectory.

Model of complex protection system for an info-communication facility

Problem statement. It is possible to include events from m groups into the complex protection system; each of the measures provides at least two protection functions (a and b), and creates certain inconveniences (d) for users. The main objective of this task is to draw up such a work plan, which would ensure all consumer requirements for the quality of a comprehensive action plan with a minimum of expenses for its implementation.

Conventions used in this model:

i – the number of the production site (i = 1, 2, ..., m)

a_i – the effectiveness of the first protection function in the i-th group of measures;

b_i – effectiveness of the second protection function in the i-th group of events;

d_i – "inconvenience" for the user in the i-th group of events;

K_i^{max} and K_i^{min}, respectively, the maximum possible and minimum necessary amount of implemented protection functions on the i-th segment;

c_i – the cost of implementing a plan of protection measures at the i-th site;

$к_{pl}$ – the planned volume of implemented information security functions at the facility;

a_{pl} – the planned number of events;

$в_{min}$ and $в_{max}$ respectively the minimum and maximum allowable values of measures implementing the second protection function

d_{max} – the maximum allowable number of "inconveniences" for the user associated with the implementation of measures to protect information

As managed variables, it is proposed to accept the number of activities from the i-group, which will be included in the integrated information protection plan of the area – x_i. We will solve the problem, minimizing the cost of implementing the plan, subject to the restrictions on the number of activities of each group, on the total volume of functions, on the quality of protection. This mathematical model is not unique for this type of problem. Changing the optimality criterion, we can formulate other variants of the model.

First version of the problem statement. Efficiency criteria – the cost of implementing a complex protection plan

Mathematical model of the problem

a) objective function: minimum cost of implementing an integrated information protection plan

$$\sum_{i=1}^{m} c_i x_i \to \min$$

b) limiting the number of events in each group

$$K^{\min} \le x_i \le K^{\max} \qquad (i = 1, 2, \ldots, m)$$

c) restriction on the total amount of work

$$\sum_{i=1}^{m} x_i \ge к_{пл}$$

d) restriction on the quality of protection

$$\frac{\sum_{i=1}^{m} x_i a_i}{\sum_{i=1}^{m} x_i} = a_{пл}$$

$$b_{\max} \geq \frac{\sum_{i=1}^{m} x_i b_i}{\sum_{i=1}^{m} x_i} \geq b_{\min}$$

$$\frac{\sum_{i=1}^{m} x_i d_i}{\sum_{i=1}^{m} x_i} \leq d_{\max}$$

e) boundary conditions ensuring the positivity of the solution:

$$x_i \geq 0$$

Second version of the problem statement. The criterion of efficiency is the total volume of the implemented protection functions or the deviation of the quality indicator of the protection from the planned quality level.

Mathematical model of the problem

$$\sum_{i=1}^{m} x_i \rightarrow \max$$

or minimum of quality deviation from the planned target:

$$\left| a - a_{пл} \right| \rightarrow mir$$

Where $a = \frac{\sum_{i=1}^{m} x_i a_i}{\sum_{i-1}^{m} x_i}$.

Solving the same problem according to various optimality criteria allows us to make a comparative analysis of the solutions obtained and to increase the validity of the solution.

As an illustrative material, the task of forming a complex protection plan for an object is given.

It is proposed to include three types of measures in the protection plan: legislative measures (No. 1), organizational and technical measures (No. 2), and technological measures (No. 3). Each of the groups of measures allows you to implement two types of functions: protection against unauthorized access, protection against infections. The numerical values of the parameters for each group of protections are given in Table 3. The minimum and maximum values of the implemented functions are presented in terms of value.

Table 3

The numerical values of the parameters for each group of protective equipment

№ Group number	Minimum number of implemented functions m	Protection against unauthorized access %	Malware protecti on %	Total number of implemented functions %	Maximum number of implemented functions	Costs of implementation of the plan (m.u.)
1	2	3	4	5	6	7
1	22	14	2	75	24	14
2	25	20	0,8	60	28	10
3	15	16	1,2	75	17	12
Plan		≤ 17	≤1,4	≥ 35		

Mathematical model of the problem

Performance criterion

$$W=14x_1 + 10x_2 + 12x_3 \rightarrow \min$$

System of restrictions

a) the total number of implemented functions

$$0,75\ x_1 + 0,6\ x_2 + 0,75\ x_3 \geq 35$$

b) by the number of implemented functions for each group

$$22 \le x_1 \le 24$$

$$25 \le x_2 \le 28$$

$$12 \le x_3 \le 17$$

c) restrictions on the implementation of the protection function from unauthorized access

$$0{,}14x_1 + 0{,}2x_2 + 0{,}16x_3 \le 0{,}17(x_1 + x_2 + x_3)$$

d) restrictions on the implementation of the protection function against malicious software

$$0{,}02x_1 + 0{,}008x_2 + 0{,}12x_3 \le 0{,}014(x_1 + x_2 + x_3)$$

Boundary conditions: $x_{1\div 9} \ge 0$

After reducing the system of restrictions to the canonical form

$$0{,}75\,x_1 + 0{,}6\,x_2 + 0{,}75\,x_3 - x_4 = 35$$

$$x_1 + x_5 = 24$$

$$x_1 - x_6 = 22$$

$$x_2 + x_7 = 28$$

$$x_2 - x_8 = 25$$

$$x_3 + x_9 = 17$$

$$x_3 - x_{10} = 12$$

$$-0{,}03\,x_1 + 0{,}03\,x_2 - 0{,}01\,x_3 + x_{11} = 0$$

$$0{,}008\,x_1 - 0{,}006\,x_2 - 0{,}002\,x_3 + x_{12} = 0$$

The problem is solved using standard software.

Conclusion. Thus, it can be argued that the mathematical model of the information security system allows you to find a set of components, their quantitative ratio that meets the specified technological requirements for the quality of object protection, as well as the requirements of the adopted criterion (minimum cost price or maximum profit)).

Modeling, as an indispensable condition for the scientific substantiation of the effectiveness of protection, determining the price of an issue and the degree of risk, allows the decision maker to form the concept of complex protection of information objects, to determine strategic and tactical solutions to problems associated with maintaining the level of security of an object.

ЛИТЕРАТУРА

1. Романов В. Н. Системный анализ для инженеров. СПб.: СЗГЗТУ, 2006. 186 с.

2. Клименко И. С. От технологии 2С к технологии 2Д / Saarbrücken: PalmariumAcademicPublishing, 2014. 284 с.

3. Запечников С. В. Информационная безопасность открытых систем. В 2-х т. Т.1 - Угрозы, уязвимости, атаки и подходы к защите / С. В. Запечников, Н. Г. Милославская. М.: ГЛТ, 2006. 536 с.

4. Клименко И. С. Модели и методы управления: учебное пособие. Алматы: Отан, 2015. 187 с.

5. Клименко И. С. Направления повышения эффективности сотрудничества образования и бизнеса // Актуальные проблемы развития вертикальной интеграции системы образования, науки и бизнеса: экономические, правовые и социальные аспекты Материалы II Международной научно-практической конференции. 2014. С. 30-35.

6. Клименко И. С. Алгоритм сетевого планирования и управления на базе инновационных технологий // Математические методы и модели в исследовании актуальных проблем экономики России Сборник материалов Международной научно-практической конференции / отв. ред. Р. Р. Ахунов. 2016. С. 289-294.

REFERENCES

1. Romanov V. N. Sistemnyi analiz dlya inzhenerov. SPb.: SZGZTU, 2006. 186 s.

2. Klimenko I. S. Ot tekhnologii 2S k tekhnologii 2D/ Saarbrücken: PalmariumAcademicPublishing, 2014. 284 s.

3. Zapechnikov S. V. Informatsionnaya bezopasnost' otkrytykh sistem. V 2-kh t. T.1 Ugrozy, uyazvimosti, ataki i podkhody k zashchite / S. V. Zapechnikov, N. G. Miloslavskaya. M.: GLT, 2006. 536 c.

4.Klimenko I. S. Modeli i metody upravleniya. Uchebnoe posobie. Almaty: Otan, 2015. 87 s.

5. Klimenko I. S. Napravleniya povysheniya effektivnosti sotrudnichestva obrazovaniya i biznesa // Aktual'nye problemy razvitiya vertikal'noi integratsii sistemy obrazovaniya, nauki i biznesa: ekonomicheskie, pravovye i sotsial'nye aspekty Materialy II Mezhdunarodnoi nauchno-prakticheskoi konferentsii. 2014. S. 30-35.

6. Klimenko I. S. Algoritm setevogo planirovaniya i upravleniya na baze innovatsionnykh tekhnologii // Matematicheskie metody i modeli v issledovanii aktual'nykh problem ekonomiki Rossii Sbornik materialov Mezhdunarodnoi nauchno-prakticheskoi konferentsii. Otvetstvennyi redaktor R. R. Akhunov. 2016. S. 289-294.

ОБ АВТОРАХ

Клименко Ирина Сергеевна, начальник отдела организации проектно-грантовой деятельности, Института сервиса, туризма и дизайна (филиала) автономного образовательного учреждения «Северо-Кавказский федеральный университет»
Klimenko Irina Sergeevna, Head of the Organization of Project and Grant Activities of the Institute of Service, Tourism and Design (branch) of North Caucasus Federal University in Pyatigorsk

Медетов Нурлан Амирович, проректор по научной работе и стратегическому развитию, Костанайский государственный педагогический университет
Medetov Nurlan Amirovich, Vice Rector for Research and Strategic Development, Kostanay State Pedagogical University

Дата поступления в редакцию 12.07.2018