Methodical approach to reducing the dimensionality of the task of requirements substantiation for protection of information systems against unauthorized access in organizational-technical systems

T V Meshcheryakova¹, O A Gulyaev², A A Abdullin³ and A V Batskikh¹

¹Voronezh Institute of the Ministry of Internal Affairs of the Russian Federation, 53, Patriots Avenue, Voronezh, 394065, Russia
²Voronezh State Technical University, 14, Moskovsky Avenue, Voronezh, 394026, Russia
³Center of information technologies, communications and information protection of the Ministry of Internal Affairs of the Republic of Bashkortostan. 7. Lenin street, Ufa. 450000, Russia

E-mail: mescher73@mail.ru, ptr@utw.su, azikk0089@yandex.ru, svatikova96@mail.ru

Abstract. The article proposes a methodological approach to reducing the dimensionality of the problem of forming the requirements for the security of information processed in organizational-technical systems with complex architecture. The methodological approach is based on the structural analysis of graphs that formalize the structural scheme of organizational-technical systems and on the construction of the adjacency matrix of the graph. Using the selected elements of strong connectiveness, which form the clusters of architecture, allows further to solve the problem of formation of requirements to the information protection system against unauthorized access and to go from the architecture of organizational-technical system as a whole to the consideration of individual clusters. In this case, the task of forming requirements is significantly simplified. With the use of the proposed method of clustering the architecture of organizational-technical systems, the problem of forming the sets of information protection of objects of biological activity during molecular-biological and genetic engineering studies is solved.

1. Introduction

The most important procedure implemented in the process of designing the organizational-technical system is the substantiation of the requirements for the information protection system (IPS) against unauthorized access (UAA). According to [1], its purpose is to ensure the security state of the subjects of automated systems (AS) (elements, subsystems) against various threats to the information spreading in them and the information processes.

Such legislative acts of the Russian Federation as the law "On state secrets" [2], the law "On information, information technologies and information protection" [3] are devoted to the issues of substantiation of requirements to IPS against UAA in solving organizational-technical tasks. In accordance with them, the formation of requirements to IPS against UAA is one of the important directions in the field of protection of state information resources from breach of confidentiality and

Content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence. Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.
Published under licence by IOP Publishing Ltd
integrity [4, 5].

In the Russian Federation, when developing organizational-technical systems, in the process of justifying the requirements for information security (IS), in accordance with the requirements of GOST [6-8], the guiding documents of the Federal Service for Technical and Export Control (FSTEC) of Russia are used [9-11].

Development of the international standard "General criteria..."(GC) [12] was the further creation of normative documentation of justification of requirements to IS. In GC, instead of the term "fixed security class", the term "security profile" is introduced, and the concept of class acquires a different meaning: classes are understood as sets of functional or warranty requirements that perform certain information protection (IP) tasks.

The set of possible requirements for the IS of organizational-technical systems should contain a number of positions. The most common requirements are stated for the following parameters of IPS against UAA [5, 13, 14]:

- Method of construction of IPS against UAA (separate components of IPS against UAA – software, software-hardware, hardware);
- Architecture (level of confidentiality of information and minimum configuration of software and hardware, orientation to certain software and hardware platforms, functional purpose, implementation of the interface);
- IP strategies;
- Total cost of resources for the provision of IS (including resources diverted to perform the functions of IP);
- Reliability of IPS against UAA (failure criteria, numerical values of the indicator of reliability of functioning taking into account the destructive actions related to UAA of the hacker and leading to violation of IS);
- Numerical value of the levels of confidentiality of information implemented in the IPS against UAA;
- Number of levels of authority implemented in the IPS against UAA;
- Ability to provide the required number of users;
- Duration of installation and configuration procedures;
- Length of procedures for loading IPS against UAA, starting from the moment of power supply to the AS components;
- Responses to emerging threats to IS;
- Availability and provision of service for IP (security administrator);
- Composition of the software (SW) used, the possibility of its modification, compatibility with other software platforms, etc.;
- External components of IPS against UAA (availability of license, certificate, etc.).

Thus, when solving the problem of formation of requirements for IPS against UAA of the organizational-technical system, the regulatory and legislative framework can be applied. At the same time, design of IPS against UAA of organizational-technical system is a creative process depending on a set of factors that defines limited standardization of set of methods and tasks of requirements justification [5, 15, 16].

Mathematically, the problem of formation of requirements for IPS against UAA of the organizational-technical system can be presented in the following form [17]:

$$W^* = \text{Arg} \min_{W \in W_d} C(W),$$

$$\{W_d\} = [W : P(W, U) \geq P_r, R(W, U) \subseteq R_d],$$

where: $C(W)$ – is the functional characterizing the real cost of development and practical use of IPS against UAA (its lowest value is equated to the rational variant $W^*$);

$W_d$ – multitude of permitted to operate variants of IPS against UAA;
\( P(W, U) \) – is the parameter characterizing the efficiency of operation – is quantitative indicator of the resistance of security features of variants of IPS against UAA in terms of the totality of threats to the IS \( U \):

- \( P_r \) – required value of the efficiency index;
- \( R(W, U) \subseteq R_d \) – specified resource constraints on IS provision.

The direct solution of the task (1) is not possible due to its structural complexity and high dimensionality. As the practice of solving problems of synthesis of organizational-technical systems in various applied areas shows, the main method of solution is the method of decomposition of the problem into a number of simpler ones. Thus, the hierarchical decomposition by a number of signs is carried out: levels of hierarchy, stages of the solution of a problem, elements making structure of organizational-technical system.

Justification of requirements to the IS of organizational-technical system is a multi-stage process, which can be based on the use of the hierarchy "system-element". In accordance with the hierarchy, a certain set of technical means, considered as a real element of a higher-level system, simultaneously contains elements in its composition, in respect of which it is a system [5, 17].

This functional hierarchy allows us to consider IPS against UAA as a IS system, which is part of the organizational-technical system, and at the same time containing in its composition the basic subsystems, such as: access control subsystem, identification and authentication subsystem, registration and accounting subsystem, cryptographic subsystem, subsystem of controls, etc. The basic subsystems are libraries and databases.

Thus, the problem of finding methods for solving problem (1) is currently relevant. A possible direction of its solution is the division into a number of individual simplified problems with less structural complexity. In this case, it is required to decompose the architecture of the organizational-technical system and for each \( j \)-th cluster to independently solve particular problems of the form:

\[
W_j^* = \underset{W_j \in W_jd}{\text{Arg min}} C(W_j) \\
\{W_{jd}\} = \{W_j: P_j(W_j, U_o) \geq P_r, R_j(W_j, U_j) \subseteq R_{jd}\}.
\]

2. Materials and methods

The method of constructing a model of organizational-technical system architecture in the form of a graph is a formalized procedure for constructing a vertex graph of the form [17].

The architecture of the organizational-technical system considers the purpose and relationship of its main functional parts (blocks). Each of the blocks is a functionally complete one-piece device.

In the process of solving the problem (1), depending on the desired granularity of the description of the architecture of organizational-technical system, as blocks, there can be considered both separate structural units included in the system, and special equipment or detailed software functional elements that do not require separate consideration.

Solving the problem of formalization, we select the blocks, using the principles that determine the possibility of functional description of the block and the unidirectionality of its action.

Methodically, verbal representation of AS based on the use of information and logical schemes, has the following form.

1. IPS against UAA is divided into separate subsystems (blocks), conventionally designated by symbols that define the role of the elements included in the subsystem.
2. The links that characterize the information aspect in the process of research of IPS against UAA are lines that connect related elements.
3. Directions of the implementation of the processes that characterize the connection (relationships) between certain blocks of the system are indicated by arrows on the communication lines.

The elements of the organizational-technical system correspond to the vertices of the graph \( X = \{x_1, x_2, \ldots, x_n\} \), and elementary connections – to the arcs of the graph \( U = \{u_1, u_2, \ldots, u_m\} \). As a
result, we have a vertex graph $A$ described by the adjacency matrix, which reflects the structure of the system.

The process of clustering makes it possible to distinguish in the structure of the organizational-technical system all its constituent information elements (subsystems), which are mutually achievable due to feedback. The allocation of strongly and weakly related information elements in the system structure makes it possible to carry out clustering of information objects in order to reduce the structural complexity of the problem (1). The formalization of the decomposition process can be accomplished by reducing the oriented graph.

In the process of solving the problem of separation (decomposition), the following algorithm is used, developed in [18]:

1. Using the adjacency matrix $A G_u(X, U)$.
2. Finding the matrix $R_1 = A + E$ (logical addition), where: $R_1$ is the first reachability matrix, $E$ is the unit matrix.

The matrix $R_2 = R_1^2$ is calculated ($*$ – the sign of logical multiplication and summation of matrix elements in the calculation of $R_1 \times R_1$). Similarly, all matrices can be defined, ending with $R = R_n = R_1^n$, where $R$ is the reachability matrix of the graph $G(X, U)$.

3. Determining the condition $R = Q$ under which the graph will be bi-connected, where $Q = \{q_{ij}\}$ – the universal matrix, where $q_{ij} = 1$ for all available values $i$ and $j$. In this case, the separation of a system containing one strongly coupled subsystem is not possible. It can be realized when $R \neq Q$. It is necessary to calculate the matrix of the spanning (undirected) graph $G^0(X, U)$ corresponding to the oriented graph $G(X, U)$, $R_0 = (A + A^T + D)^m$, where $A^T$ is the transposed matrix.

Next, we define the connected subgraphs of the directed graph $G(X, U)$. The vertices of a connected subgraph containing vertex $i$ in accordance with [18] in the $i$-th row of the matrix $R^0$ are defined by units. Since the graph $G(X, U)$ contains one connected subgraph at $R^0 = Q$, the decomposition of the system cannot be realized. Under the condition $R^0 \neq Q$, the vertices of the graph $G(X, U)$ (matrix $A$) are ordered by the connected subgraphs. Then, to develop the connectivity matrix $C = R + R^T$ (arithmetic addition), from the matrix $C$, it is necessary to allocate bi-connected subgraphs. A bi-connected subgraph containing vertex $i$, according to [18], in the $i$-th row of a matrix $C$ is determined by deuces. The matrix $A$ is ordered so that the bi-connected subgraphs form square submatrices $E_\varphi \subseteq A$, $\varphi = 1, 2, \ldots, p$.

The adjacency matrix $R_0^0 = (A_0^0 + A_0^T + E_+)^0\delta$ is calculated, where $A_0^0$ – adjacency matrix of a subgraph with the multitude of vertices $V = W \cup \bigcup_{\varphi=1}^{p} B_\varphi$, $B_\varphi$ – a subset of the constituent parts of $\varphi$-th strongly connected subsystem.

The connections between subsystems that must be broken as a result of separation are determined by the edges of the ordered matrix $A'$.

3. Results and their discussion

The present time is characterized by increased rates of development of such sciences as biotechnology, genetic engineering, biochemistry, pharmacology, etc. To save and support genetic resources outside the natural environment (ex-situ), special repositories, collections, gene banks are created. The specified scientific organizations which are objects of biological activity (OBA), form the national genetic resources providing genetic material for scientific, research and other purposes to other domestic and foreign scientific and commercial organizations [19]. On the basis of the transferred material, intellectual property objects are further created, the subsequent use of which can be profitable. Therefore, genetic resources have become the object of scientific and commercial interests and, accordingly, the IP.

The method of reducing the structural complexity of the problem (1) is applicable when justifying the requirements for IS of OBA in the process of molecular-biological and genetic-engineering studies.

Traditionally, OBA is understood as enterprises, R&D and testing institutions, health care
institutions, individual laboratories, biological stations and other facilities, in the production cycles or processes of which pathogenic, industrial or technophilic microorganisms and dangerous biological substances are used, which requires molecular-biological and genetic-engineering studies. It should be noted that, in contrast to virological studies (and other activities related to microorganisms of I-IV groups of pathogenicity), molecular-biological and genetic-engineering studies do not fall under the action of instructions for handling and accounting of infectious material, and work with them is organized in accordance with the ideas of performers about the need for restrictions. The peculiarity of the work on cloning, study of genetic homogeneity of strains and the development of genetic-engineering methods for obtaining medical and special drugs is a wide range of methods and techniques used. In this case, banks of individual components can be formed: proteins (antigens and plasmids – producers of recombinant antigens), genetic material (genome fragments, plasmids with attachments, synthetic primers), as well as specific sera, antibodies and hybrids-producers of monoclonal antibodies. Another important feature from the point of view of IP of OBA is the fact of resistance to environmental factors of plasmids, as well as amplicons – DNA fragments obtained by performing genetic-engineering works on the development of recombinant structures. This leads to the accumulation of genetic material in the objects of the external environment outside the working area of the OBA.

By themselves, these data are not intellectual property, and therefore objects for IP or objects of IS provision (they do not belong to the creations of the human mind). Nor can they be directly protected by intellectual property rights. However, the results of the activities and the entire technological cycle of OBA in the conduct of molecular-biological and genetic-engineering research, based on genetic research, can be protected by patent law or the rights of breeders. In this case, some of the data obtained may relate to state secrets, trade secrets or personal data. In all these cases, the requirements for ensuring IS of OBA during molecular-biological and genetic-engineering studies have a legislative basis.

Due to the fact that the IP of molecular-biological and genetic-engineering activities is not provided by standard methods of biological protection used in research related to infectious material, it is necessary to implement special measures aimed at preventing UAA to information about the species of the original and newly obtained strains of microorganisms and their biological properties. In this case, the information can be contained both in the form of individual components of microorganisms and on carriers of different species.

Based on the analysis of the main types of work carried out in the course of research in this subject area, the architecture of the OBA can be presented in the form of a graph $G_u(X, U)$ shown in figure 1.

---

**Figure 1.** The architecture of the OBA when carrying out molecular-biological and genetic-engineering research.
The graph reveals the following basic elements of the structure of molecular-biological and genetic-engineering studies of OBA [20]:
- Fractionation of viral material, proteins and nucleic acids;
- Preparation of recombinant proteins;
- Preparation of monoclonal antibodies;
- Synthesis of nucleotide structures;
- Genetic-engineering works;
- Works with virus collections and their components in working units;
- Works with plasmid collections and recombinant antibodies;
- Works with collections of hybrids and monoclonal antibodies;
- Works with collections of oligonucleotide primers;
- Works with collections of genetically engineered structures;
- Laboratory for the study of protein structure and function;
- Laboratory for the study of the structure and function of nucleic acids;
- Laboratory of development of diagnostic products;
- Laboratory of development of preventive and medical preparations;
- Laboratory of development of vaccine preparations;
- Laboratory of development of preparations with the set properties;
- Diagnostic works;
- Work in the central collection of microorganisms;
- Virological biotechnological works.

According to the clustering technique, the adjacency matrix of graph $A$, shown in figure 1, has the form shown in figure 2.

\[
\begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}
\]

**Figure 2.** Clustering of the adjacency matrix of graph $A$.  

The reachability matrix of the graph $G_u(X,U)$ formalizing the OBA architecture has degree 19.
The matrix view $R_{19}$ is shown in figure 3.

Since the matrix $R_{19}$ is not a universal matrix $Q = |q_{ij}|$ in which $q_{ij} = 1$ for all values $i$ and $j$, clustering is possible. Connectivity matrix of graph of structure OBA of molecular-biological and genetic-engineering research $C = R + R^T$ has the form shown in figure 4.

$$
\begin{align*}
1000010000110111011 & \\
010000100001000100 & \\
0010000100001000100 & \\
0001000010001000100 & \\
10001100011111111111 & \\
1000010000110111011 & \\
000000100001000100 & \\
0000000100001000100 & \\
0000000010001000100 & \\
1000010000111111111 & \\
0000000000010000000 & \\
0000000000010000000 & \\
0000000000010000000 & \\
000000000001000100 & \\
100010000110111011 & \\
100010000110111011 & \\
100010000110111011 & \\
000000000000000100 & \\
100010000110111011 & \\
\end{align*}
$$

Figure 3. Reachability matrix of graph $G_u(X,U)$.

$$
\begin{align*}
2000120001110222022 & \\
020000100001000100 & \\
0020000100001000100 & \\
0020000100001000100 & \\
10002100011111111111 & \\
2000120001110222022 & \\
010000200001000100 & \\
0010000200001000100 & \\
0010000200001000100 & \\
1000110002111111111 & \\
10001100021200111011 & \\
10001100010200111011 & \\
011110111102000100 & \\
2000120001110222022 & \\
2000120001110222022 & \\
2000120001110222022 & \\
0111101111010000200 & \\
2000120001110222022 & \\
2000120001110222022 & \\
\end{align*}
$$

Figure 4. Connectivity matrix of graph of structure OBA.

The analysis of the connectivity matrix allows to draw a conclusion that, in the structure of molecular-biological and genetic-engineering studies of OBA, there are the following clusters of
objects characterized by strong connectivity: $R_1 = \{18, 19\}; R_2 = \{14, 15, 16\}; R_3 = \{1, 6\}$.

The analysis of the elements that are part of the clusters of molecular-biological and genetic-engineering studies, characterized by strong connectivity, shows that the elements in which works with strains of microorganisms is carried out are mainly subject to IP against UAA. In particular, the cluster $R_1$ is subject to protection with the use of a set of IPS against UAA-1.

The main content of the works in the $R_1$ cluster are virological biotechnological works, as well as intensive exchange of biological materials with the Central collection of microorganisms. In accordance with this, when protecting information at OBA in the course of carrying out molecular - biological and genetically engineering researches, set of IPS against UAA-1 should provide protection of data on a patrimonial accessory of strains of microorganisms and to be formed in the context of IPS against UAA of virological biotechnological works.

The set of IPS against UAA-2 is intended for IP in the $R_2$ cluster. It includes components on which works related to the development of drugs (therapeutic and special vaccines) are performed. Cluster $R_2$ is characterized by intensive exchange of biological materials and technical information and, accordingly, the set of IPS against UAA-2 should include means of protection against UAA to information about the biological properties of these materials. In addition, the set of IPS against UAA-2 should include traditional means of IP from leakage through technical channels.

The $R_3$ cluster mainly exchanges biological materials. In this regard, the set of IPS against UAA-3 in composition should be similar to the set of IPS against UAA-1. Given that the $R_3$ cluster contains the “Collection of viruses and their components” element, the IPS against UAA-3 set should be justified taking into account the IPS against UAA sets, intended for IP at OBA when carrying out virological and biotechnological works.

4. Conclusion
The article proposes a methodological approach to reducing the task dimensionality of the requirements justification for IPS against UAA as applied to the information processed in organizational-technical systems with complex architecture. The methodological approach is based on the structural analysis of the oriented graph formalizing the block architecture of the organizational-technical system. Allocation of strongly and weakly connected information elements in structure of complex system allows to carry out clustering of information objects and to pass from consideration of architecture of organizational-technical system as a whole to consideration of separate clusters for the purpose of decrease in structural complexity of a task of justification of requirements to IPS against UAA. Formalization of the decomposition process is carried out by reduction of the directed graph and construction of its adjacency matrix.

As an example of application of the stated methodical approach, the clustering is presented of architecture of organizational-technical system of type OBA at carrying out molecular-biological and genetic engineering researches in the interests of justification of requirements to IS.

The use of the proposed methodological approach in solving the problem of justification of requirements for IPS against UAA will increase the real security of existing and prospective organizational-technical systems with complex architecture in the process of their design and operation.
[4] Melnikov V V 1997 Protection of information in computer systems (Moscow: Finance and statistics) p 368 (in Russian)

[5] Drovnikova I G, Meshcheryakova T V, Rogozin E A and Popov A D 2019 Formation of requirements for information protection systems against unauthorized access to automated systems of Internal Affairs bodies on the basis of genetic algorithm (Voronezh: Voronezh Institute of the Ministry of Internal Affairs of Russia) p 128 (in Russian)

[6] GOST R 51624-2000 2001 Information Protection Automated systems in secure execution General requirements (Moscow: State standards of Russia) p 34 (in Russian)

[7] GOST R ISO/IEC 15408-2013 2014 Methods and means of security assessment Criteria of information technology security (Moscow: Standartinform) p 161 (in Russian)

[8] GOST 34.601-90 2014 Information technology. Set of standards for automated systems Creation stages (Moscow: Standartinform) p 6 (in Russian)

[9] FSTEC of the Russian Federation Guidance document Concept of protection of computer equipment and automated systems from unauthorized access to information (app on 30 March 1992) p 7 (in Russian)

[10] FSTEC of the Russian Federation Guidance document Computer equipment Protection against unauthorized access to information Indicators of security against unauthorized access to information (app on 30 March 1992) p 21 (in Russian)

[11] FSTEC of the Russian Federation Guidance document Automated systems Protection against unauthorized access to information Classification of automated systems and information security requirements (app on 30 March 1992) p 29 (in Russian)

[12] Common Criteria for Information Technology Security Evaluation 1999 National Institute of Standards and Technology & National Security Agency (USA) Communication Security Establishment (Canada) Communications-Electronics Security Group (United Kingdom) Bundesamt fur Sichereit in der Informationstechnik (Germany) Service Central de la Securite des Systemes d’Information (France) National Communications Security Agency (Netherlands) Version 2.1

[13] Oz E 2009 Management Information Systems 6th Edition (USA: Thomson Course Technology) p 592

[14] Rebovich G and White B 2011 Enterprise Systems Engineering: Advances in the Theory and Practice (Boca Raton: CRC Press) p 459

[15] Silva L C and Costa A P C S 2013 Decision model for allocating human resources in information system projects (Int. Journal of Project Management) 31 pp 100-8

[16] Dordevic N 2017 Software quality standards (Vojnotehnicki Glasnik. Militaiy Technical Courier) 65 1 pp 102-4

[17] Khvostov V A 2013 Methods and means of increasing the security of automated systems (Voronezh: Voronezh Institute of the Ministry of Internal Affairs of Russia) p 108 (in Russian)

[18] Zmeev A A, Machtakov C G, Meshcheryakova T V, Nikulina E Yu, Rogozin E A, Stukalov V V and Khvostov V A 2015 Methods and means of evolutionary and structural modeling in substantiating the requirement for software systems of information security (Voronezh: Voronezh Institute of the Ministry of Internal Affairs of Russia) p 94 (in Russian)

[19] Huckins L M, Dobbyn A and Douglas M 2019 Gene expression imputation across multiple brain regions provides insights into schizophrenia risk (Nature Genetics) 51 pp 659-74

[20] Proceedings of the Institute of Microbiology named after S N Vinogradsky 2004 12 ed V F Galchenko (Moscow: Science) p 423 (in Russian)