Optimization mathematical model of protected infocommunication system structure

To cite this article: O S Avsentiev et al 2019 J. Phys.: Conf. Ser. 1202 012033

View the article online for updates and enhancements.
Optimization mathematical model of protected infocommunication system structure

O S Avsentiev¹, V V Menshikh², A O Avsentev³
¹Department of information security, Voronezh Institute of the Ministry of internal Affairs of the Russian Federation, 53, prosp. Patriotov, Voronezh, 394065, Russia
²Department of mathematics and systems modeling, Voronezh Institute of the Ministry of internal Affairs of the Russian Federation, 53, prosp. Patriotov, Voronezh, 394065, Russia
³Department of physics, Voronezh Institute of the Ministry of internal Affairs of the Russian Federation, 53, prosp. Patriotov, Voronezh, 394065, Russia
E-mail: aoaao8787@mail.ru

Abstract. There is an optimization mathematical model of protected infocommunication system structure. The model takes into account as both features of the system and its elements like factors, characterizing the vulnerabilities and determining a violators possibilities to implement information leakage technical channels, as functions of the information security system to localize these vulnerabilities.

1. Introduction

Modern infocommunication systems are the backbone of efficient functioning of various structures and systems. Information circulating in these systems is used as a providing resource for their activities [1–3]. The properties of such systems, as well as the features of information processes implemented in them, determine objectively the existence of plenty of factors characterizing the vulnerability of these systems that can be used by enemy for implementation of information security violation threats [4].

Currently used methods for the assessment of the characteristics of these threats are empirical in nature, are mainly implemented with the help of experts and do not take into account the dynamics of impact of threats to information processes of information and telecommunication systems. Identification of weak links in these systems for implementation of the security threats of information is carried out using instrumental and computational methods. For the determination of the probability of threats as the characteristics of the dynamics of its emergence and manifestation, it is required have its own calculation model for each threat. These models do not currently exist, and their development is an actual problem. In its turn, the lack of threat models of this type determines the problem of selecting mechanisms of information protection in information and telecommunication systems.

This paper considers the mathematical model of optimization of mechanisms of information protection in information and telecommunication systems, taking into account the heterogeneity of the elements of the structure of information — telecommunication systems and the possibility of the offender applying different technical means to implementation the threats of information security and also the opposition of purposes of the offender on the one hand and legitimate users of this information in organizing its protection on the other hand.
An information threat is understood as a threat to an object by influencing its information sphere [4]. Many ways of implementing these threats are associated with the concept of information leakage technical channel, which implies the totality of information source, technical means of its security violation and physical environment of information signal spread [5]. The possibility of emergence of these channels is objectively linked to the presence of spurious radiations from various kinds of physical fields which are used as carriers of information during its transmission from source to destination [6, 7].

Similar to [8] elements of infocommunication system itself can be considered as sources of information in the leakage channels. A large number of these elements and their distribution in space condition the heterogeneity and multiplicity of information leakage technical channels. Determining the exact number of these channels and their characteristics is not possible both for a violator and for legitimate users of information. On the one hand it is determined by the uncertainty regarding the characteristics of the elements of infocommunication system as sources of information and characteristics of spurious emissions of heterogeneous informative physical fields as its carriers, on the other hand — by uncertainty regarding technical means and strategies of implementation of information leakage channels used by a violator.

It should be noted that these strategies are of an active character. The activity is in the constant and purposeful search for vulnerabilities in the infocommunication system and its information security system in order to overcome the mechanisms of protection and to ensure the implementation of information security threats.

These circumstances determine the necessity to use protected infocommunication systems, including both elements of the information structure in the form of information arrays and elements of information protection system. In these conditions the problem of optimization of this system structure arises. This article is dedicated to the development of the appropriate mathematical model.

2. Subject — functional structure of protected infocommunication system

We will refer to the same type the information arrays of the equal presentation form (speech, documentary, telecommunication, etc.), for transmission, reception, processing and storage of which the same type elements of infocommunication system are used. In this case, for arrays of the same type the danger will be the information security threats caused by the same vulnerabilities of the infocommunication system and its elements.

To locate vulnerabilities in order to prevent threats to information security, information protection system is built. This system includes the elements, which affect the vulnerability of infocommunications systems to varying degrees.

We denote:
- \( \mu_1, \mu_2, \ldots, \mu_n \) — types of array of information to be transferred, received, processed and stored in the infocommunication system;
- \( \theta_1, \theta_2, \ldots, \theta_J \) — infocommunication system vulnerabilities;
- \( \phi_1, \phi_2, \ldots, \phi_l \) — elements of information protection system, the use of which is potentially possible;
- \( \pi_1, \pi_2, \ldots, \pi_s \) — possible strategies of using technical means by a violator employing certain vulnerabilities of infocommunication system.
- \( p_{ij} \) — probability of implementation of information security vulnerabilities to \( i \) — information array, \( i = 1, 2, \ldots, I \), determined by \( j \) — set of vulnerabilities, \( j = 1, 2, \ldots, J \);
- \( r_{jm} \) — probability of using \( j \) — set of infocommunication system vulnerabilities using \( m \) — option of information leakage technical channel, \( m = 1, 2, \ldots, M \);
- \( q_{ik} \) — probability of decrease of security level threat of \( i \) — array of information in case of application of \( k \) — option of information protection system design, \( k = 1, 2, \ldots, K \).
The generalized subject — functional structure of the protected infocommunication system, taking into account the entered symbols is shown in the Figure 1. Information array types $\mu_n$ are defined by infocommunication system purpose, and potential vulnerabilities $\theta_j$ — by its structure, composition, interrelations and elements features. In its turn, on the basis of analysis of vulnerabilities as factors determining possible threats to information security, legitimate users of the information define composition of elements $\phi_l$ and functions of the system of its protection, and a violator has opportunity to form a strategy $\pi_s$ to use technical means to achieve his goals. Estimation of the mentioned above probabilistic parameters of the task $p_{ij}$ and $q_{jk}$ can be obtained using the mathematical models developed in [9]. In addition it was assumed that in the information leakage channel a successive transformation of its form in transforming, transmitting and receiving devices is carried out. Every subsequent transformation is interrelated with the previous one and converts the previous state of information into the subsequent one with some distortions.

As one of the main conditions of minimizing these distortions, the condition of matching the input characteristics of the subsequent transforming device and the output characteristics of the previous device is accepted. As estimation of a leakage probability it is offered to consider the probability to adjust this matching.

There are a number of difficulties in assessing the parameter $r_{jm}$ as the probability of using the vulnerabilities of the information and telecommunication system when using various variants of strategy of applying technical means to implement information leakage technical channels by the offender.

In this case, since the characteristics of the electronic devices of the information transmission path in infocommunication system and the characteristics of the technical means used by a violator, are identified in the process of their development and manufacture, then in the leakage channel the matching conditions are determined by the output characteristics of radio electronic devices of infocommunication system elements and the input characteristics of technical means used by a violator.

**Figure 1.** The generalized subject — functional structure of the protected infocommunication system
Using these models allows to consider both the heterogeneity of radio — electronic devices of infocommunication system elements and capabilities of a violator applying various technical means for implementation of information security threats, as well as opposition of the goals of a violator on the one hand, and legitimate users of this information for organization of its protection on the other hand.

In addition quality of information leakage technical channels, occurring while implementing security threats by a violator, depends as on correctness of choosing technical means for the purpose, as on the characteristics of the electronic devices elements of infocommunication system for which the technical means are used, that is, on a violators choice of application strategy option.

This dependence is shown in the Figure. The type of information array and the structure of the infocommunication system determine its vulnerabilities as factors defining a violators possibilities for the use of technical means in implementation of information security threats. On the other hand existence of these vulnerabilities in the infocommunications system requires their localization by using information system protection.

There are a number of difficulties in assessing the parameter \( r_{jm} \) as the probability of using the vulnerabilities of the information and telecommunication system when using various variants of strategy of applying technical means to implement information leakage technical channels by the offender.

Taking into account the known physical principles of functioning of both technical means applied by a violator, and electronic devices elements of infocommunication system, we can assume the possibility of determining this parameter of the considered task on the basis of the method of expert estimations.

3. Assessment of information protection performance indices

We denote:

- \( c_i, v_i \) — value and volume of \( i \) — information array, \( i = 1, 2, \ldots, I \);
- \( s_j \) — cost of infocommunication system, in which there is \( j \) — option of vulnerabilities;
- \( s_{PoI}^k \) — cost of \( k \) — option of infocommunication system implementation;

Then

- \( c_i \cdot v_i \) — possible damage to \( i \) — information array;
- \( p_{ij} \cdot c_i \cdot v_i \) — risk of threat to information security of \( i \) — information array in case of implementation of \( j \) — option of vulnerabilities;
- \( q_{ik} \cdot p_{ij} \cdot c_i \cdot v_i \) — risk of threat to information security of \( i \) — information array in cases of implementation of \( j \) — option of vulnerabilities and application of \( k \) — option of information system protection;
- \( \sum_{i=1}^{I} p_{ij} \cdot c_i \cdot v_i \) — risk of threat to information security of infocommunication system in case of implementation \( j \) — option of vulnerabilities;
- \( \sum_{i=1}^{I} q_{ik} \cdot p_{ij} \cdot c_i \cdot v_i \) — risk of threat to information security of infocommunication system in case of implementation of \( j \) — option of vulnerabilities under conditions of applying \( k \) — option of information protection system. In order to solve the optimization problem it is necessary to estimate the parameters of the information value.

In order to define \( c_i, v_i \) of value and volume respectively of information array it is possible to use the approach of determining a generalized index of information value proposed in [3]. This index characterizes analytical relationship of different information properties in relation to \( i \) — its array:

\[
C_0 = \sum_{i=1}^{I} w_i c_i
\]
where \( c_i \) — a set of measurable indices of properties of \( i \) — information array, \( (i = 1, 2, \ldots, I) \);
\( w_i \) — weight coefficients characterizing the importance of corresponding properties of information for the activity under consideration, identified by expert way;
\( I \) — number of information properties that determine the massage value, depending on the type of the activity provided.

For the numerical estimation of properties \( c_i \) of information and their relevance for formation of a generalized index of its value the logical — linguistic approach is used, and for determining of the importance coefficients of these properties, we propose a method of analyzing hierarchies. With this approach, index (1) characterizes numerical evaluation of both properties of information and its volume (properties of completeness and relevance of the array information studied [3]).

4. Optimization model of protected infocommunication system structure

We will consider possibilities of solving the task of optimizing the choice of options for building a protected infocommunication system that minimizes the risks of information security violations.

The formal model for solving the problem of optimizing the choice of mechanisms of infocommunication systems information protection.

We introduce the variables:

\[
x_j = \begin{cases} 
1, & \text{if there is an option of building infocommunication system in which there is a } j \text{ — option of vulnerabilities;} \\
0, & \text{unless otherwise;} 
\end{cases}
\]

\[
y_k = \begin{cases} 
1, & \text{if there is a } k \text{ — option of building of information protection system;} \\
0, & \text{unless otherwise;} 
\end{cases}
\]

\[
z_m = \begin{cases} 
1, & \text{if there is an } m \text{ — option of strategy for applying technical means by a violator to implement violation threats to information security;} \\
0, & \text{unless otherwise.} 
\end{cases}
\]

In this case, the task of choosing the structure of infocommunication system and information protection system under the conditions of a violator using infocommunication system vulnerabilities and information security weaknesses and implementing strategies for employing appropriate technical means to achieve his goals is as follows:

To find

\[
(X, Y, Z) = \text{Arg min} \sum_{m=1}^{M} \sum_{k=1}^{K} \sum_{j=1}^{J} \sum_{i=1}^{I} z_m \cdot r_{jm} \cdot y_k \cdot q_{ik} \cdot x_j \cdot p_{ij} \cdot c_i \cdot v_i
\]  

(2)

under restrictions:

\[
\sum_{j=1}^{J} x_j s_j + \sum_{k=1}^{K} y_k s_k^{pol} \leq \hat{S},
\]  

(3)

\[
\sum_{j=1}^{J} x_j = 1,
\]  

(4)

\[
\sum_{k=1}^{K} y_k = 1,
\]  

(5)
\[ \sum_{m=1}^{M} z_m = 1. \]  

(6)

where \( \hat{S} \) cost restrictions of the protected infocommunication system.

The models of definition of the values entering the problem formulation are given in [2, 3, 6–8].

The difference of forms of information presentation in various structural components of information and telecommunication systems, diversity of physical principles of equipment construction, as well as the diversity of informative physical fields and their propagation environments determine the complexity of the problem under consideration.

5. Conclusions

Task (2)–(6) belongs to the class of tasks of nonlinear binary programming [9]. Its solution will allow to optimize the procedures for selecting information protection mechanisms in information and telecommunications systems, taking into account the interrelationships of various radioelectronic elements composing these systems, capabilities of the infringer, using various technical means to implement threats to information security, as well as the opposition of purposes of the offender and legitimate users of this information in organizing its protection from threats.

References


