Mathematical modeling of mechanisms for detecting threats of information leakage through parametric channels

S V Belokurov, Y E Lvovich, S V Ivanov and A N Noev
ET Department, Voronezh Institute Federal Penitentiary Service of Russia,
1a Irkutskaya Street, Voronezh, RU

E-mail: noev87@mail.ru

Abstract. The article analyzes various conceptual aspects of the problem of protecting information from leakage through parametric channels. An indicator of the relevance of the threat of information leakage through parametric channels is considered in the form of a two-component vector, the first component of which is the probability of realizing the threat of leakage and the second is the coefficient of its danger. The characteristics of threats are given. The ways of information protection from leakage through parametric channels in the concept of information security management are explored. The principles of modeling mechanisms for detecting threats to information leakage through parametric channels are formalized in the interest of evaluating the effectiveness of its protection against leakage. A mathematical description of the effectiveness index of mechanisms for detecting threats of information leakage through parametric channels is proposed. The result of the conducted studies is a meaningful and formal statement of the problem of modeling mechanisms for detecting threats to information leakage through parametric channels in the interest of evaluating the effectiveness of information protection.

1. Introduction
Analyzing various conceptual aspects of the problem of protecting information from leakage through parametric channels, we have to state the fact that the methodology of information security has not been used consistently, which, in turn, is the reason for inadequate perception and assessment of the main factors that form the basis of this problem. In this paper, we will use terminology based on materials [1], which is coordinated with the main regulatory document of the Federal Service for Technical and Export Control (FSTEC) of Russia, which regulates the requirements for the protection of confidential information [2].

As a result of studies of such a specific phenomenon in the theory and practice of technical protection of information, as a parametric channel, a number of mathematical models describing its signal characteristics have been developed. At the same time, the main indicator of the potential for the formation of information leakage channels - an indicator of violation of its confidentiality - presupposes a more general, systemic characteristic, consistent with the functional features of the manifestation of such threats and ways to protect information from leakage. In accordance with the normatively defined requirements of FSTEC of Russia [3], such an indicator is the relevance of the leakage threat, which allows us to numerically assess the level of its danger from systemic positions.

The aim of this work is the development of mathematical models of threats to information leakage through parametric channels and mechanisms for identifying such threats, based on the correspondence of the functional description of information leakage threats and the mechanisms for...
their detection. To do this, it is necessary to formalize the substantive and formal statements of the task of modeling the mechanisms of detecting threats to information leakage through parametric channels, and also to present an illustrative example for explaining the advantages of the proposed approach in the form of a functional model of illegal actions to intercept information on parametric channels and demonstrate the practical implementation of the proposed method of structuring characteristics of mechanisms for identifying threats to information leakage on parametric their channels.

2. Characteristics of threats of information leakage through parametric channels

According to [4-5], the indicator of the urgency of the threat of information leakage through parametric channels is a two-component vector, the first component of which is the likelihood of realizing a leakage threat, and the second is the coefficient of its danger. To estimate the indicator of the urgency of information leakage threats on parametric channels, we use the provisions of the generalized methodology [6-7]. This indicator is calculated from the values of the hazard factor of the parametric leakage channels and the probabilities of their implementation. Using this technique to determine the list of current threats of information leakage through parametric channels, we introduce the following restrictions [8]:

- the list and characteristics of possible threats of leakage of speech information through parametric channels are specified before the calculations;
- the list of voice messages with protected information is determined before the calculations;
- the importance of the protected information is determined before the calculations;
- leak channels of this type can exist independently of each other;
- damage from information leakage through parametric channels is additive with respect to damage caused by the implementation of various channels of this type;
- the danger of a leakage channel is assessed with respect to each message with protected information, the confidentiality of which is violated in the implementation of this channel.

Threats of information leakage through parametric channels are realized for the considered period of time \( t \) with some probabilities represented in the form of a matrix:

\[
P(t) = \left[ p_{kl}(t) \right], \quad k = 1, 2, \ldots, K, l = 1, 2, \ldots, L,
\]

where \( p_{kl}(t) \) - probability of realizing the \( k \)-th threat of leakage in relation to the \( l \)-th message.

Damages from the implementation of parametric channels of information leakage are presented in the form of a matrix:

\[
D = \left[ d_{lm} \right], \quad l = 1, 2, \ldots, L, m = 1, 2, \ldots, M,
\]

where \( d_{lm} \) - damage from the implementation of the \( m \) leakage channel in relation to \( l \) messages.

If the damage from the implementation of the leakage channel exceeds the acceptable \( D_{np} \), then it is assumed equal to \( D_{np} \). The ratio \( d_{lm} / D_{np} \) is taken as a hazard factor for the threat of leakage, as a result of which the \( m \) channel is realized in relation to \( l \) messages. The relationship between the threats of leakage and the parametric channels that arise as a result of their implementation is represented by a matrix:

\[
T = \left[ \tau_{km} \right], \quad k = 1, 2, \ldots, K, m = 1, 2, \ldots, M,
\]

whose elements are defined as follows:

\[
\tau_{km} = \begin{cases} 1, & \text{if } k \text{ threat leads to the implementation of the } m \text{ channel leakage,} \\ 0 & \text{otherwise.} \end{cases}
\]

The threats of leakage can be realized by various sources of threats. The possibility of implementing a threat depends on the availability of favorable conditions for exploiting the
vulnerabilities associated with these threats. The procedure for determining the likelihood of favorable conditions for the use of certain vulnerabilities in the interests of realizing the threats of information leakage through parametric channels is represented by the matrix:

\[ P' = \begin{bmatrix} p'_{1n} & p'_{2n} & \cdots & p'_{Kn} \\ \end{bmatrix}, \]

where \( p'_{kn} \) – the likelihood that conditions may be favorable for the use of \( n \) vulnerabilities in order to realize the \( k \) threat of leakage. Moreover, the probability of favorable conditions for the realization of the \( k \) threat is determined from the relation:

\[ p_k^* = 1 - \prod_{n=1}^{N} (1 - p'_{kn}) \]

The likelihood of implementing \( n \) threat of leakage, with respect to at least one message is determined as follows:

\[ p_{n}(t) = 1 - \prod_{l=1}^{L} (1 - p_k^* \cdot p_{il}(t)). \]

The hazard factor \( k \) of the threat is determined by the formula:

\[ \overline{D}_k = \sum_{l=1}^{L} \sum_{m=1}^{M} (r_{km} \cdot \frac{d_{lm}}{D_{np}} \cdot P_{il}). \]

As applied to the types of information security threats under consideration, this technique will have a number of features.

When determining the indicator of the relevance of the threat of information leakage through parametric channels, the following list of possible classes of leakage channels was adopted [3]:

1) parametric acousto-vibro-optical (laser);
2) parametric acousto-vibro-electromagnetic;
3) parametric acousto-vibro-electric;
4) special acoustoradiotechnology;
5) special acoustoelectric;
6) special acousto-optical.

The importance of the protected information is determined by the source of the informative signal. In this case, the danger of a parametric channel of information leakage is estimated with respect to each protected message.

In this case, the dimension of the matrix (1) for this type of information security threat is \( 3 \times R \), and the matrices (2) and (3) are rows of length \( R \) and \( 3 \), respectively. The main vulnerable links with respect to threats of leakage of voice information over the parametric channel are [4]:

- presence in the allocated premises (AP) of the security-fire alarm system;
- availability of home appliances in the AP;
- possibility of placing radio locks and semi-active filling devices (SAFD) in furniture, AP walls;
- the presence in the AP of the network of electrical chasers;
- presence in the AP of the ventilation system;
- presence in the AP of the broadcast network and loudspeaker communication;
- presence of external telephone communication in the AP;
- The presence in the AP of operating technical means for processing and transmitting information;
- presence in the AP of working auxiliary technical means and systems;
- application in the AP for lighting fluorescent lamps.

In this case, the dimension of the matrix (5) for a given nomenclature of information security vulnerabilities is \( 7 \times 10 \).
Taking into account the considered features, it is possible to obtain numerical values of the system characteristic (5) of information leakage threats by parametric channels – the urgency of the threats of the type considered.

Thus, in the work it is necessary to formalize the statement of the task of modeling the mechanisms of detecting threats of information leakage through parametric channels in the interest of assessing the effectiveness of information protection.

3. Protection of information from leakage through parametric channels in the concept of information security management

The protection of information from leakage through parametric channels is part of the measures to ensure the information security of bodies [6, 7], conducted in accordance with its concept. The main guiding principles of such events are:

- legality of measures to identify information leakage through parametric channels;
- continuity of implementation and improvement of means and methods for monitoring the security of information activities;
- comparability of the control period and possible damage from violation of information security;
- the complexity of using existing means of protecting information from leakage through parametric channels [8] at all stages of information activities.

The latter gives the greatest effect when activities are implemented within the framework of a single managed process [9] ensuring information security using available technical protection of information.

This allows us to solve the following tasks:

- provide an integrated approach to the implementation of technical protection of information;
- objectively assess the current state of information security from leakage through parametric channels;
- prevent information leakage through channels of this type;
- to ensure centralized control over the security of information activities;
- organize a secure information interaction with territorially remote units;
- to ensure the confidentiality of information.

As an object of management measures to protect information from leakage through parametric channels are implemented in stages.

The first stage is the definition of the object of protection. Within the framework of this stage, the following is done:

- determination of the boundaries of the controlled zone;
- classification of information subject to threats of leakage through parametric channels, in terms of importance and confidentiality;
- evaluation of the aging time of confidential information;
- development of a scheme for informational interaction between the divisions of the body, taking into account the susceptibility to their threats of the type in question.

The second stage is the identification of threats. At this stage:

- detection of sources of threats - semi-active filling devices and radio electronic equipment used to illegally obtain information in the process of information exchange by its activation by an external physical field;
- definition of the objectives of threats - forms of familiarization with confidential information intercepted by parametric channels;
- detection of external electromagnetic radiation as a sign of possible realization of threats of information leakage through parametric channels;
- identification of necessary protection measures;
- evaluation of their effectiveness;
- implementation of measures taken to protect information, taking into account the priorities developed;
Bring decisions on protection measures to employees (in the part concerning);
- monitoring the security of information activities and eliminating (preventing) the consequences of threats to information leakage.

The third stage is the interaction of management processes. The process of managing the protection of information from leakage through parametric channels has links to other information security management processes, as in other processes actions are performed to ensure the security of information. In this case, the process of managing the protection of information from leakage through parametric channels provides other processes for managing information security with instructions on the structure of activities related to ensuring the security of information. The scope of such interaction is regulated by the head of the organization.

The fourth stage is the implementation of a set of measures to protect information from leakage through parametric channels. Within the framework of this stage, the following is done:
- management of incidents of occurrence of information leakage channels of the type in question;
- management of changes in operating conditions of basic and auxiliary technical facilities and systems;
- management of the level of capabilities of information security tools;
- management of information security continuity;
- management of adequacy of protection - compliance of technical protection of information to its types.

4. Principles of modeling mechanisms for detecting threats to information leakage through parametric channels in order to evaluate the effectiveness of its protection against leakage

The study of known methods for analyzing the influence of negative factors on the functioning of complex systems made it possible to establish that when solving such problems, the authors confine themselves mainly to heuristic rules for the formation of analytical, logical and semantic relationships between the analyzed parameters and intuitive (expert) estimates of the change in the efficiency of the processes under study [10-15]. This makes it necessary to formulate principles for solving the problem of modeling information leakage mechanisms using parametric channels in order to evaluate the effectiveness of its leakage protection [9]. To this end, we define the basic hypothesis and a number of principles for the solution of this problem from the point of view of the complex use of methods of the theory of modeling and the theory of recognition [7, 8, 16-23].

The fundamental hypothesis in solving the problem of modeling the mechanisms of information leakage through parametric channels in the interest of evaluating the effectiveness of its protection against leakage is the hypothesis of structural identity and functional opposition of the functional description of the processes of intercepting information through parametric channels and the processes of detecting its leakage through the channels of the type considered.

In accordance with this hypothesis, the methodology of structural analysis is used as a tool for the functional description of the processes of intercepting information over parametric channels, and the methodology of structural synthesis as a tool for the functional description of the processes of protecting information from leakage. In this case, there is a one-to-one correspondence between the levels of the structure of the functional description of the processes of interception of information and the processes of its protection from leakage.

From the above hypothesis, the basic principles for solving this problem follow [5].

The principle of analyzability of the description of the mechanisms of information leakage through parametric channels and the principle of synthesesizability of the description of the processes of its protection from leakage assume, as their basis for the formation of descriptions of such mechanisms and processes, their structural analysis and structural synthesis, respectively.

Logically stemming from these principles the principle of functional representation of the mechanisms of information leakage through parametric channels and the processes of its protection from leakage leads to the necessity of using functional modeling methods for the formation of descriptions of the investigated processes.
The principle of multilevel functional representation of descriptions of mechanisms of information leakage through parametric channels and processes of its protection from leakage presupposes the existence of several levels of functional representation of the processes being studied.

The realization of the principle of homogeneity of the description of the mechanisms of information leakage through parametric channels and the processes of its protection against leakage makes it possible to describe such processes by such characteristics through which all their other parameters can be expressed.

From these positions, it is most expedient to use the parameters of the volume of operations performed to use the means of interception and protection of information, as well as the characteristics of the means of interception of information and the characteristics of technical protection of information in the general case depend on the volume of operations performed. In addition, this parameter allows you to quantify the effectiveness of information protection from leakage through parametric channels.

5. Indicator of effectiveness of mechanisms for detecting threats to information leakage through parametric channels

To substantiate the format of the effectiveness index of the mechanisms for detecting threats of information leakage through parametric channels, let us consider a formalized representation of the functioning of these mechanisms.

To this end, we introduce the following notation:

- \( S^{(y)} \) – operating environment threats of information leakage through parametric channels;
- \( S^{(b)} \) – the operational environment of mechanisms for detecting such threats;
- \( k^{(y)} = \dim(S^{(y)}) \) – the size of the operating environment of threats of information leakage through parametric channels;
- \( k^{(b)} = \dim(S^{(b)}) \) – the size of the operating environment for mechanisms to detect such threats.

Let's consider in detail the mechanism for detecting parametric channels of information leakage. To uniquely identify the channels, the \( S^{(y)} \) and \( S^{(b)} \) media are divided into \( I \) disjoint fragments:

\[
S^{(y)} = \bigcup_{i=1}^{I} S_i^{(y)}, \quad S^{(b)} = \bigcup_{i=1}^{I} S_i^{(b)}, \quad i = 1, 2, \ldots, I.
\]

In this case, the operating environment \( S^{(y)} \) is divided to form one significant feature of the parametric channel in each fragment, and the operating environment \( S^{(b)} \) – for its detection and identification.

In the general case, a significant feature of the parametric channel characterizes the channel class [13].

Then the probability of identifying a parametric channel for an individual fragment \( s_i^{(y)} \) of the operating environment \( S^{(y)} \), can be determined as the probability of correspondence of the fragment \( s_i^{(b)} \) of the operating environment \( S^{(b)} \) to a given fragment of the operating environment \( S^{(y)} \) according to the formula:

\[
p_i = \frac{k_i^{(b)}}{k_i^{(y)} + k_i^{(b)}},
\]

where \( k_i^{(y)} \) - fragment size \( s_i^{(y)} \); \( k_i^{(b)} \) – fragment size \( s_i^{(b)} \).

To determine the characteristic of the dimension \( k \) of the operating environment, we use the Halstead metric [10].

In accordance with the provisions of this metric, the most significant characteristic of the
effectiveness of implementation as a function of illegal actions to intercept information on parametric channels, as well as mechanisms for detecting threats to intercept it, is their information volume, which consists of the algorithmic volume of functions being implemented and the volume of information used [8]:

\[ V = \alpha \log_2 A + \beta \log_2 B. \]  

(7)

where \( \alpha \) - number of unique (non-repetitive) actions to implement the threats of information leakage through parametric channels (procedures for detecting such threats); \( A \) – the total number of actions in the implementation of these threats (procedures for their detection); \( \beta \) – the number of unique operands used to implement the specified actions (procedures); \( B \) – the total number of operands used in the implementation of threats of information leakage through parametric channels (procedures for detecting such threats).

The first term (7) represents the algorithmic volume of procedures for identifying threats to information leakage through parametric channels, and the second – the amount of information used.

In this case, the information volume of the fragment \( s_{(y)} \) will be written as:

\[ v_{(y)} = \alpha_{(y)} \log_2 A_{(y)} + \beta_{(y)} \log_2 B_{(y)}, \]

and the information volume of the fragment \( s_{(b)} \) - as:

\[ v_{(b)} = \alpha_{(b)} \log_2 A_{(b)} + \beta_{(b)} \log_2 B_{(b)}. \]

Then expression (6) can be written in the form:

\[ p_i = \frac{v_{(b)}}{v_{(y)} + v_{(b)}} = \frac{\alpha_{(b)} \cdot \log_2 A_{(b)} + \beta_{(b)} \cdot \log_2 B_{(b)}}{\alpha_{(y)} \cdot \log_2 A_{(y)} + \beta_{(y)} \cdot \log_2 B_{(y)} + \alpha_{(b)} \cdot \log_2 A_{(b)} + \beta_{(b)} \cdot \log_2 B_{(b)}}. \]

Provided that the partitioning of the operating environment into fragments is based on the equiprobable presence of signs of the emergence of parametric channels of information leakage, and the entire operating environment is a potentially possible area for the formation of significant features of such channels, the probability \( P^{(b)} \) to identify the threats of information leakage through parametric channels for the entire the operating environment \( S^{(y)} \) and the entire operating environment \( P^{(b)} \) is determined according to the expression:

\[ P^{(b)} = 1 - \prod_{i=1}^{L} (1 - p_i) = 1 - \prod_{i=1}^{L} \left(1 - \frac{\alpha_{(y)} \cdot \log_2 A_{(y)} + \beta_{(y)} \cdot \log_2 B_{(y)} + \alpha_{(b)} \cdot \log_2 A_{(b)} + \beta_{(b)} \cdot \log_2 B_{(b)}}{\alpha_{(b)} \cdot \log_2 A_{(b)} + \beta_{(b)} \cdot \log_2 B_{(b)}} \right). \]

(8)

Given the uniform partitioning of the operating environment \( S^{(y)} \) and the operating environment \( S^{(b)} \) into fragments, the total volume of these media is determined according to the expressions:

\[ V^{(y)} = I_{S^{(y)}}, \]

where \( v_{(y)} = v_{1(y)} = v_{2(y)} = \ldots = v_{i(y)} \) – the volume of one piece of the operating environment \( S^{(y)} \); \( V^{(b)} = I_{S^{(b)}}, \) where \( v_{(b)} = v_{1(b)} = v_{2(b)} = \ldots = v_{i(b)} \) – the volume of one piece of the operating environment \( S^{(b)} \).

In this case, the expression for the probability \( P^{(b)} \) for identifying threats of information leakage through parametric channels can be represented in the form:
Expression (9) can be considered as an indicator of the effectiveness of mechanisms for identifying threats to information leakage through parametric channels:

$$E^{(b)} = P^{(b)}.$$  

6. **Illustrative example for explaining the advantages of the proposed approach**

Taking into account the existing practice of functional modeling of information processes [2, 3], we will form the decomposition structure of actions to intercept information via parametric channels (Figure 1).

In accordance with the decomposition structure of the functional description of the illegal actions to intercept information on parametric channels, shown in Fig. 1, the conceptual level of such description corresponds to the objective function of this kind of actions.

The decomposition of the objective function of unlawful actions to intercept secondary high-frequency (HF) radiation of elements of radio electronic equipment (REE) and SAFD as a result of its structural analysis and forms the functions of the first intermediate level of the functional description of unlawful actions.

![Diagram](image)

**Figure 1.** Decomposition structure of the functional description of illegal actions to intercept information via parametric channels

The format of the decomposition representation of the objective function has the form:
\[ \phi^{(\mu)} = \left\{ \phi^{(\mu)}, \mathcal{R}^{(\mu)}, \left\{ \phi^{(n1)}_m \right\} \right\} \] (11)

where \( \phi^{(\mu)} \) – the name of the objective function \( \phi^{(\mu)} \) of illegal actions to intercept information through parametric channels; \( \mathcal{R}^{(\mu)} \) – a sign of the structural correspondence of the objective function, the functions obtained as a result of its decomposition (functions of the first intermediate level); \( \phi^{(n1)}_m \) – is the representation of the function of the first intermediate level of the functional description obtained as a result of decomposition of the objective function, \( m = 1, 2, \ldots \); \( \Phi^{(n1)} = \{ \phi^{(n1)}_m \} \) – is the set of functions of the first intermediate level of the functional description.

The conceptual level of the functional description of the mechanisms of information leakage through parametric channels is presented in Figure 2.

Taking into account the contents of the decomposition process, the parameters (11) are represented as:

\( \phi^{(\mu)} \) – information leakage through parametric channels;

\( \mathcal{R}^{(\mu)} \) – a way of interception (removal) of the information of secondary HF radiation of elements of REE and SAFD;

\( |\Phi^{(n1)}| = 2 \).

Detailing the conceptual level of a functional description of threats to information leakage through parametric channels in accordance with the presented methodological approach leads to the following format of decomposition representation of the functions of the first intermediate level of the hierarchy of functional structuring of unlawful actions to intercept information via parametric channels:

\[ \Phi^{(n1)}_m = \left\{ \phi^{(n1)}_m, \mathcal{R}^{(n1)}_m, \left| \Phi^{(n2)}_m \right|, \left\{ \phi^{(n2)}_{ml} \right\} \right\}, \] (12)

where \( \phi^{(n1)}_m \) – the name of the function \( \phi_m \) (n1) of the first intermediate level of the functional representation of illegal actions to intercept information via parametric channels; \( \mathcal{R}^{(n1)}_m \) – a sign of the structural correspondence of the function \( \phi^{(n1)}_m \) of the first intermediate level to the functions obtained as a result of its decomposition (functions of the second intermediate level); \( \phi^{(n2)}_{ml} \) is the representation of the function of the second intermediate level of the functional description obtained as a result of the decomposition of the function of the first intermediate level, \( l = 1, 2, \ldots \); \( \Phi^{(n2)}_m = \{ \phi^{(n2)}_{ml} \} \) – is the set of functions of the second intermediate level of the functional description.
Figure 2. The conceptual level of the functional description of the mechanisms of information leakage through parametric channels

Thus, the functional model of illegal actions to intercept information through parametric channels is a multilevel hierarchical structure, the lower level of which is represented by the primary signs obtained as a result of the structuring of the objective function of unlawful actions.

7. Computational experiment to assess the effectiveness of mechanisms for identifying threats to information leakage through parametric channels

The effectiveness of mechanisms for identifying threats to information leakage through parametric channels, in accordance with the above methodology, will be considered in relation to the typical characteristics of illegal actions to intercept information through the channels of the type in question and the typical characteristics of mechanisms for identifying threats to information leakage.

For the purpose of implementing this methodology, a software package was developed to assess the effectiveness of mechanisms for identifying threats to information leakage through parametric channels. Figure 3 provides a dialog box for entering the initial data on the characteristics of threats in accordance with their representation in the form (7), obtained by analyzing the signs of illegal actions \( r_i, i = 1, 2, \ldots, 19 \) from their set.

In this case, the column "ID / IND" corresponds to the identifiers and names of the functions of the initial level of the description of the threats of information leakage through parametric channels, the columns "\( \alpha \)", "\( A_{\text{min}} \)", "\( A_{\text{max}} \)", "\( \beta \)", "\( B_{\text{min}} \)", "\( B_{\text{max}} \)" correspond to the parameters of the expression (7).

The values in the columns "\( V_{\text{min}} \)", "\( V_{\text{max}} \)", "\( V_{\text{sr}} \)", "\( V_{\text{sko}} \)" correspond to the minimum, maximum, average values of the information volume of functions and its root mean square deviation, respectively. These values are determined during the operation of the software package.

On the basis of these initial data, in accordance with the models given in the paper, we obtain the values of the information volume of the functions of the third intermediate level of the functional description of illegal actions to intercept information via parametric channels.

The values of the information volume characteristics of the target function of unlawful actions to intercept secondary HF radiation from the elements of the REE and the SAFD and the objective function for identifying information leakage threats through parametric channels obtained in the
experiment make it possible to determine, on the basis of (9) and (10), the efficiency index of the mechanisms for identifying information leakage threats by parametric channels, i.e. efficiency increased to 78%:

$$E^e = 1 - \left( \frac{V}{V(V)+V} \right)^i = 1 - \left( \frac{5152}{(1496+5152)} \right)^i \approx 0.78.$$ 

Figure 3. Dialog box for input of initial data on characteristics of information leakage threats by parametric channels

Thus, the way of structuring the characteristics of the mechanisms for detecting threats to information leakage through parametric channels in the article makes it possible to provide a significantly higher reliability of the estimate than the reliability of the evaluation for certain characteristics of threat detection mechanisms that are not connected to any system. The models considered in the work are the methodological basis for the synthesis of the procedure for evaluating the effectiveness of mechanisms for identifying threats to information leakage through parametric channels. The application of the effectiveness evaluation mechanisms developed in the article to detect threats to information leakage through parametric channels allows for a more reliable estimate than traditional valuation methods.

8. Substantial and formal formulation of the problem of modeling mechanisms for detecting threats to information leakage through parametric channels in the interest of evaluating the
effectiveness of information security
In order to formalize the task and the ways to solve it, in accordance with the formulated meaningful statement, let us denote by $R(N)$ the set of rules for evaluating the effectiveness of mechanisms for identifying threats to information leakage through parametric channels in terms of $E^{(b)}$ by a specified nomenclature of $N$ models. At the same time, it is possible to assess the threats $S(R)$.

Then the task of modeling mechanisms for detecting threats to information leakage through parametric channels can be considered as the task of developing a set of rules $R$ that maximizes the possibility $S$ to evaluate the effectiveness of mechanisms for identifying threats to information leakage through parametric channels in the nomenclature of $n$ models that does not exceed the specified $N$.

This allows us to formally formulate the problem in the form:

$$R = \arg \max S(R).$$

$$n \leq N$$

The formulated task of modeling the mechanisms of identifying threats of information leakage through parametric channels is expedient to be solved by presenting the following main successive tasks:
- structuring descriptions of the attacker's actions to intercept information through parametric channels and mechanisms for identifying such actions;
- finding the correspondence between the functional and mathematical description of the attacker's actions to intercept information on parametric channels and the mechanisms for identifying such actions in order to obtain a nomenclature of models that does not exceed the specified one;
- conducting experiments to assess the effectiveness of mechanisms for identifying threats to information leakage through parametric channels;
- determination of the value of the indicator of opportunities to assess the effectiveness of mechanisms for identifying threats to information leakage through parametric channels for different sets of evaluation rules.

9. Conclusion
Thus, the article presents mathematical models of information leakage threats on parametric channels and mechanisms for detecting such threats, based on the functional correspondence between the description of information leakage threats and the mechanisms for their detection, as well as the correspondence between the functional and mathematical representations of the processes being studied. A meaningful and formal statement of the task of modeling the mechanisms for identifying threats to information leakage through parametric channels will allow to determine the values of the indicator of the possibilities of evaluating the effectiveness of mechanisms for identifying threats to information leakage through parametric channels for different sets of evaluation rules.

References
[1] Zapevnikov S V, Miloslavskaya N G and Tolstoy A I 2006 Information security of open systems: a textbook for universities Threats, vulnerabilities, attacks and approaches to protection (Moscow: Hot line – Telecom) p 536
[2] Belokurov S V, Skryl S V and Jogan V K 2012 Models and algorithms for automated control of the effectiveness of information security systems in automated systems (Voronezh Institute of the Ministry of Internal Affairs of Russia) p 116
[3] Litvinov D V, Skryl S V and Tyamkin A V 2009 Research of mechanisms of counteraction to computer crimes: organizational-legal and criminalistic aspects (Voronezh Institute of the Ministry of Internal Affairs of Russia) p 218
[4] Minaev V A, Tyunyakin R N and Filippova N V 2006 Criminalistic identification of signs of unauthorized access to protected computer systems Information Technology Security 2(50) pp 67-70
[5] Lamonov A V 2007 Qualifying characteristics of illegal actions in the sphere of computer information Technology Security 1 pp 108-113

[6] Karpchev V Yu and Potanin V E 2006 Formal bases of functional modeling of harmful influences on protected information systems in the interests of revealing illegal actions in the sphere of computer information Science of production 3(89) pp 30-31

[7] Dushkin A V, Novoseltsev V I and Sumin V I 2016 Methodological foundations for the construction of secure automated system (The scientific book) p 76

[8] Belokurov S V, Krasnov P E and Boronenkov A I 2012 A way to identify negative impacts on information security systems Information and Security 3 pp 377-382

[9] Minaev V A, Skryl S V and Dvoryankin S V 2008 Informatics: a textbook for higher educational institutions of the Ministry of Internal Affairs of Russia (Maroseika) p 102

[10] Pisaruk N N 2013 Investigation of operations (BSU) p 464

[11] Dushkin A V, Kravchenko A S, Novoseltsev V I, Smolentseva T Ye and Sumin V I 2014 Matematicheskiye modeli i informatsionnyye protsessy upravleniya slozhnym ob"yektom (Nauchnaya kniga) p 125

[12] Dushkin A V, Barkalov S A, Kolodyazhnyy S A and Sumin V I 2017 Introduction to system analysis (Hot line – Telekom) p 234

[13] Dushkin A V, Barkalov S A, Kolodyazhnyy S A and Sumin V I 2017 Introduction to the system design of intellectual knowledge bases (Hot line – Telekom) p 108

[14] Novoseltsev V I, Kochedykov S S and Orlova D Ye 2017 Tensor analysis of Crohn and its applications: monografiya (Scientific book) p 220

[15] Sumin V I, Dushkin A V and Kravchenko A S 2014 Modeling systems (Scientific book) p 222

[16] Zarubin V S and Fomin A YA 2010 The problem of optimization of information protection processes in information and telecommunications systems in the sphere of critical applications Information and security 2 pp 239-242

[17] Skryl S V 2009 Evaluation of the security of information processes in territorial bodies of internal affairs: research models (Voronezh Institute of the Ministry of Internal Affairs of Russia) p 217

[18] Atlasov I V, Bagayev M A and Meshcheryakova T V 2012 Mathematical representation of the functional reserve for the implementation of technological control by software to protect information from unauthorized access in a computer system Information and security 2 pp 241-244

[19] Dushkin A V and Kiselev V V 2011 Substantiation of the method of supplementing the composition of the subsystem for detecting unauthorized impacts on information systems in conditions of limiting the time resource Information and security 2 pp 279-282

[20] Whitman M E and Herbert J 2009 Mattord Principles of Information Security (Cengage Learning EMEA) p 598

[21] Brett C 2004 Tjadjen Fundamentals of Secure Computer Systems (Beedle & Associates) p 498

[22] Balan V P, Dushkin A V, Novoseltsev V I and Sumin V I 2016 Risk and reflection (Hot line – Telecom) p 136

[23] Novoseltsev V I Balan V P and Dushkin A V 2015 Conflict Management (Hot line – Telecom) p 144