Analysis and optimization of decision-making in integrated security systems

D G Zybin¹, S V Belokurov², O A Kondratov², A N Sidelnikov¹ and E D Ponomarev¹

¹Voronezh institute of the Russian Federal Penitentiary Service, Russia, Voronezh, Irkutskaya 1a
²Vo­ronezh State University of engineering technologies, Russia, Voronezh, Revolucii, 19

E-mail: zdg77@mail.ru

Abstract. The paper offers a comprehensive set of characteristics of integrated security systems for electronic document management, which allows conducting research on the degree of protection of such systems from external and internal threats from the point of view of system analysis and modeling their functioning in various conditions. Classification descriptions are given and data analysis is performed when modeling decision-making processes in integrated security systems on the example of responding to threats of information leakage through parametric channels. The optimal set of response measures is given for performing illegal actions by an attacker to intercept information via parametric channels when using the corresponding modes of operation of the TCP Protocol. The type of analytical models of performance characteristics of measures to respond to threats of information leakage through parametric channels is determined by the functional model of such measures. The resulting system-level characteristics of effective response to the threat of information leakage on parametric channels is based on the stochastic representation of the conditions for timely interventions.

1. Introduction
Electronic document management systems in modern realities, including in the context of a pandemic and remote access to information resources, are among the most popular and critical in terms of security integrated security systems (ISMS). This article offers a comprehensive set of characteristics of such ISB, which allows us to study the degree of protection of such systems from external and internal threats from the point of view of system analysis and to model their functioning in various conditions. We define a set of mathematical models for evaluating the characteristics of the effectiveness of measures to respond to threats of information leakage through parametric channels [1-7].

2. The theoretical part
In accordance with the compositional nature of the procedure for forming a system of characteristics of the effectiveness of measures to respond to threats of information leakage through parametric channels, the initial data for mathematical models of the characteristics of the second level of the hierarchy of such a system are
the values of the characteristics of the first (lower) level:

- set \( \{ \alpha(\rho_{\beta}) \} \) the temporal characteristics of the operations of illegal actions by eavesdropping on parametric channels;
- set \( \{ \tau(b_{\beta}) \} \) time characteristics of functions for detecting signs that an attacker is performing illegal actions to intercept information via parametric channels.

Characteristics \( \{ \alpha(\rho_{\beta}) \} \) and \( \{ \tau(b_{\beta}) \} \) are set empirically and represent random variables [8-10].

Characteristics of the second system-level characteristics of effective response to the threat of information leakage on parametric channels are graded on the following sets of models:

- set of models \( \{ M(\bar{o}(\rho_{\beta})) \} \) to estimate the average time of implementation of TSR operation modes in the process of illegal actions to intercept information via parametric channels;
- set of models \( \{ M(\bar{\tau}(b_{\beta})) \} \) to estimate the average time of establishing the facts of the implementation of certain modes of operation of the TSR in the process of illegal actions to intercept information via parametric channels.

Features of the third system level performance characteristics of responses to the threat of information leakage on parametric channels are graded on the following sets of models:

- set of models \( \{ M(\bar{o}(\epsilon_{1})) \} \) to estimate the average values of the time when an attacker implements certain stages of illegal actions to intercept information via parametric channels;
- set of models \( \{ M(\bar{\tau}(\epsilon_{1})) \} \) to estimate the average response time to the actions of an attacker during the implementation of certain stages of illegal actions to intercept information via parametric channels;
- set of models \( \{ M(P_{\gamma_{\beta}}) \} \) to assess the probability of timely response to the actions of an attacker when they implement certain stages of illegal actions to intercept information via parametric channels.

The assessment of the fourth level characteristic - the system indicator \( R \) of timely response to threats of information leakage through parametric channels is carried out on the assumption of independence of events related to timely response to the actions of an attacker during the implementation of certain stages of illegal actions to intercept information through parametric channels.

The time characteristics of the attacker’s ability to implement the TSR operation modes in the process of illegal actions to intercept information via parametric channels are formed at the second composite level of the system of characteristics of the effectiveness of response measures to such threats to information security [11, 12]. The formation procedure is based on establishing inter-level compositional relationships between these characteristics and the characteristics of the initial (first) level of this system. The content of these links, and, consequently, the type of mathematical models of characteristics of this level is determined by the corresponding functional models of illegal actions to intercept information via parametric channels. Typical formats of generated analytical dependencies are presented in [8-10].

The expressions (1) – (15) given below are mathematical models for estimating the average values of the implementation time of TSR operation modes in the process of illegal actions to intercept information via parametric channels. In accordance with the procedure given in [1, 2, 5] for performing operations by an attacker in the process of configuring AR equipment via channels of acoustoelectric transformations, RF irradiation, parasitic (auto) generation and RF imposition, the average value \( (P_{11}) \) of a random variable of the time spent by an attacker on implementing this mode of operation of the TSR is determined in accordance with the expression:

\[
\bar{\omega}(\rho_{11}) = \bar{\omega}(\alpha_{111}) + \bar{\omega}(\alpha_{112}) + \rho_{113}E(\omega(\alpha_{113})\omega(\alpha_{115})) + \rho_{114}\bar{\omega}(\alpha_{114}) + +\rho_{116}\bar{\omega}(\alpha_{116}) + \rho_{117}\bar{\omega}(\alpha_{117})
\]

(1)

where \( \rho_{113}, \rho_{114}, \rho_{116} \) and \( \rho_{117} \) – the probability of execution attacker in the process of illegal actions operations \( \alpha_{113}, \alpha_{114}, \alpha_{116} \) and \( \alpha_{117} \), respectively, \( \bar{\omega}(\alpha_{111}), \bar{\omega}(\alpha_{112}), \bar{\omega}(\alpha_{114}), \bar{\omega}(\alpha_{116}) \) and \( \bar{\omega}(\alpha_{117}) \) - average values of random variables of the time spent by an attacker to perform operations \( \alpha_{111}, \alpha_{112}, \alpha_{114}, \alpha_{116} \), and \( \alpha_{117} \), respectively, and \( E(\omega(\alpha_{113})\omega(\alpha_{115})) \) means the average value of the composition of random variables \( \omega(\alpha_{113}) \) and \( \omega(\alpha_{115}) \) run-time intruder operations \( \alpha_{113} \) and \( \alpha_{115} \), respectively.

The order of operations performed by the attacker in the process of determining the location of sources of informative acoustic signals of the intelligence object allows you to form an expression for determining
the average value (P12) of a random variable of the time spent by the attacker on the implementation of this mode of operation:

$$\tilde{\omega}(p_{12}) = \tilde{\omega}(o_{121}) + \tilde{\omega}(o_{122}) + \rho_{123}\tilde{\omega}(o_{123}) + \rho_{124}\tilde{\omega}(o_{124}) + \rho_{125}\tilde{\omega}(o_{125}) + \rho_{126}\tilde{\omega}(o_{126})$$

(2)

where $\rho_{123}$, $\rho_{124}$, $\rho_{125}$ and $\rho_{126}$ are the probabilities of the attacker performing operations $o_{123}$, $o_{124}$, $o_{125}$ and $o_{126}$ in the course of illegal actions, respectively. $\tilde{\omega}(o_{121})$, $\tilde{\omega}(o_{122})$, $\tilde{\omega}(o_{123})$, $\tilde{\omega}(o_{124})$, $\tilde{\omega}(o_{125})$ and $\tilde{\omega}(o_{126})$ are the average values of random variables of the time spent by the attacker on performing operations $o_{121}$, $o_{122}$, $o_{123}$, $o_{124}$, $o_{125}$ and $o_{126}$, respectively.

In accordance with the order of operations performed by the attacker in the process of calculating the availability zones of informative acoustic signals of the intelligence object, the average value $\tilde{\omega}(p_{13})$ of the random value of the time spent by the attacker on implementing this mode of operation of the transmission control Protocol (TCP) is determined in accordance with the expression:

$$\tilde{\omega}(p_{13}) = \rho_{131}\tilde{\omega}(o_{131}) + \rho_{132}\tilde{\omega}(o_{132}) + \rho_{133}\tilde{\omega}(o_{133}) + \rho_{134}\tilde{\omega}(o_{134}) + E(\omega(o_{135}) \omega(o_{136}) \omega(o_{137}))$$

(3)

where $\rho_{131}$, $\rho_{132}$, $\rho_{133}$ and $\rho_{134}$ are the probability of an attacker performing operations in the course of illegal actions $o_{131}$, $o_{132}$, $o_{133}$ and $o_{134}$, respectively. $\tilde{\omega}(o_{131})$, $\tilde{\omega}(o_{132})$, $\tilde{\omega}(o_{133})$ and $\tilde{\omega}(o_{134})$ are average values of random variables of the time spent by an attacker to perform operations $o_{131}$, $o_{132}$, $o_{133}$ and $o_{134}$, respectively, a $E(\omega(o_{135}) \omega(o_{136}) \omega(o_{137}))$ means the average value of the composition of random variables $\omega(o_{135})$, $\omega(o_{136})$ and $\omega(o_{137})$ when the attacker performs operations $o_{135}$, $o_{136}$ and $o_{137}$, respectively.

The given procedure for performing operations by an attacker in the process of determining the optimal availability of informative acoustic signals of the intelligence object allows you to form an expression for determining the average value $\tilde{\omega}(p_{14})$ random value of the time spent by the attacker to implement this mode of operation TSR, in:

$$\tilde{\omega}(p_{14}) = E(\rho(o_{141}) \omega(o_{142}))$$

(4)

where $E(\omega(o_{141}) \omega(o_{142}))$ means the average value of the composition of random variables $\omega(o_{141})$ and $\omega(o_{142})$ time when the attacker performs operations $o_{141}$ and $o_{142}$, respectively.

In accordance with the given procedure for performing operations by an attacker in the process of intercepting electrical signals modulated by informative acoustic signals using tracking equipment AR on the channel of acoustoelectric transformations, the average value $\tilde{\omega}(p_{21})$ random value of the time spent by the attacker to implement this mode of operation TSR, defined according to the expression:

$$\tilde{\omega}(p_{21}) = E(\omega(o_{211}) \omega(o_{212}))$$

(5)

where $E(\omega(o_{211}) \omega(o_{212}))$ means the average value of the composition of random variables $\omega(o_{211})$ and $\omega(o_{212})$ time when the attacker performs operations $o_{211}$ and $o_{212}$, respectively.

The given procedure for performing operations by an attacker in the process of increasing the intelligibility of intercepted informative acoustic signals using special software (hardware and software) methods allows you to form an expression for determining the average value $\tilde{\omega}(p_{22})$ a random value of the time spent by the attacker to implement this TSR mode, in the form of:

$$\tilde{\omega}(p_{22}) = E(\omega(o_{221}) \omega(o_{222}) \omega(o_{223}))$$

(6)

where $E(\omega(o_{221}) \omega(o_{222}) \omega(o_{223}))$ means the average value of the composition of random variables $\omega(o_{221})$, $\omega(o_{222})$ and $\omega(o_{223})$ time when the attacker performs operations $o_{221}$, $o_{222}$ and $o_{223}$, respectively.

In accordance with the order in which the attacker's operations in the process of intercepting the re-emitted high-frequency (HF) signals, modulated informative acoustic signals in the auxiliary technical tools and systems (VTSS) of the object exploration using equipment conduct acoustic intelligence (AR) channel RF-irradiation, mean value $\tilde{\omega}(p_{31})$ of a random variable the time spent by the attacker to implement this mode of operation of TSR is determined in accordance with the expression:

$$\tilde{\omega}(p_{31}) = E(\omega(o_{311}) \omega(o_{312}))$$

(7)
where \(E(\omega(o_{311}) \ast \omega(o_{312}))\) means the average value of the composition of random variables \(\omega(o_{311})\) and \(\omega(o_{312})\), time when the attacker performs operations \(o_{311}\) and \(o_{312}\), respectively.

The given procedure for performing operations by an attacker in the process of increasing the intelligibility of intercepted informative acoustic signals using special software (hardware and software) methods allows you to form an expression for determining the average value \(\hat{\omega}(p_{32})\) a random value of the time spent by the attacker to implement this mode of operation of the TSR, in the form of:

\[
\hat{\omega}(p_{32}) = E(\omega(o_{321}) \omega(o_{322}) \omega(o_{323}))
\]  

where \(E(\omega(o_{321}) \ast \omega(o_{322}) \ast \omega(o_{323}))\) means the average value of the composition of random variables \(\omega(o_{321}), \omega(o_{322})\) and \(\omega(o_{323})\) time when the attacker performs operations \(o_{321}, o_{322}\) and \(o_{323}\), respectively.

In accordance with the above procedure for performing operations by an attacker in the process of intercepting re-emitted RF signals modulated by informative acoustic signals in the VTSS of the reconnaissance object using the AR equipment for conducting RF radiation, the average value of \(\hat{\omega}(p_{44})\) the random value of the time spent by an attacker to implement this mode of operation of the TSR is determined in accordance with the expression:

\[
\hat{\omega}(p_{44}) = E(\omega(o_{441}) \omega(o_{442}) \omega(o_{443}))
\]  

where \(E(\omega(o_{441}) \ast \omega(o_{442}) \ast \omega(o_{443}))\) means the average value of the composition of random variables \(\omega(o_{441}), \omega(o_{442})\) and \(\omega(o_{443})\) time when the attacker performs operations \(o_{441}, o_{442}\) and \(o_{443}\), respectively.

The given procedure for performing operations by an attacker in the process of increasing the intelligibility of intercepted informative acoustic signals using special software (hardware and software) methods allows you to form an expression for determining the average value \(\hat{\omega}(p_{42})\) the random value of the time spent by an attacker to implement this mode of operation of the TSR is determined in accordance with the expression:

\[
\hat{\omega}(p_{42}) = E(\omega(o_{421}) \omega(o_{422}) \omega(o_{423}))
\]  

where \(E(\omega(o_{421}) \ast \omega(o_{422}) \ast \omega(o_{423}))\) means the average value of the composition of random variables \(\omega(o_{421}), \omega(o_{422})\) and \(\omega(o_{423})\) time when the attacker performs operations \(o_{421}, o_{422}\) and \(o_{423}\), respectively.

In accordance with the order in which the attacker’s operations during the interception of high-frequency electromagnetic signals generated during operation of the generators included in the technical means and (or) parasitic (auto) generation in the technical means of object exploration using the apparatus of reference AR channel spurious (auto) generation, the mean value \(\hat{\omega}(p_{51})\) the random value of the time spent by an attacker to implement this mode of operation of the TSR is determined in accordance with the expression:

\[
\hat{\omega}(p_{51}) = E(\omega(o_{511}) \omega(o_{512}))
\]  

where \(E(\omega(o_{511}) \ast \omega(o_{512}))\) means the average value of the composition of random variables \(\omega(o_{511})\) and \(\omega(o_{512})\) time when the attacker performs operations \(o_{511}\) and \(o_{512}\), respectively.

The given procedure for performing operations by an attacker in the process of increasing the intelligibility of intercepted informative acoustic signals using special software (hardware and software) methods allows you to form an expression for determining the average value \(\hat{\omega}(p_{52})\) a random value of the time spent by the attacker to implement this mode of operation of the TSR, in the form of:

\[
\hat{\omega}(p_{52}) = E(\omega(o_{521}) \omega(o_{522}) \omega(o_{523}))
\]  

where \(E(\omega(o_{521}) \ast \omega(o_{522}) \ast \omega(o_{523}))\) means the average value of the composition of random variables \(\omega(o_{521}), \omega(o_{522})\) and \(\omega(o_{523})\) time when the attacker performs operations \(o_{521}, o_{522}\) and \(o_{523}\), respectively.

In accordance with the above procedure for performing operations by an attacker during the conversion of data intercepted through channels of acoustoelectric transformations, RF irradiation, parasitic (auto) generation, and RF imposition, the average value of \(\hat{\omega}(p_{61})\) the random value of the time spent by an attacker to implement this mode of operation of the TSR is determined in accordance with the expression:

\[
\hat{\omega}(p_{61}) = E(\omega(o_{611}) \omega(o_{612}))
\]
where \( E(\omega(\alpha_{01}) \circ \omega(\alpha_{02})) \) means the average value of the composition of random variables \( \omega(\alpha_{01}) \) and \( \omega(\alpha_{02}) \) time when the attacker performs operations \( \alpha_{01} \) and \( \alpha_{02} \), respectively.

The given procedure for performing operations by an attacker in the process of searching for information of interest allows you to form an expression for determining the average value \( \bar{\omega}(p_{62}) \) a random value of the time spent by the attacker to implement this mode of operation of the TSR, in the form of:

\[
\bar{\omega}(p_{62}) = E(\omega(\alpha_{021})\omega(\alpha_{022})\omega(\alpha_{023}))
\]  

(14)

where \( E(\omega(\alpha_{021}) \circ \omega(\alpha_{022}) \circ \omega(\alpha_{023})) \) means the average value of the composition of random variables \( \omega(\alpha_{021}), \omega(\alpha_{022}) \) and \( \omega(\alpha_{023}) \) time when the attacker performs operations \( \alpha_{021}, \alpha_{022} \) and \( \alpha_{023}, \) respectively.

In accordance with the given procedure for performing operations by an attacker in the process of analyzing the sufficiency of information intercepted through the channels of acoustoelectric transformations, RF irradiation, parasitic (auto) generation and RF imposition to disclose the content of the information process, the average value of \( \bar{\omega}(p_{63}) \) the random value of the time spent by an attacker to implement this mode of operation of the TSR is determined in accordance with the expression:

\[
\bar{\omega}(p_{63}) = E(\omega(\alpha_{031})\omega(\alpha_{032}))
\]  

(15)

where \( E(\omega(\alpha_{031}) \circ \omega(\alpha_{032})) \) means the average value of the composition of random variables \( \omega(\alpha_{031}) \) and \( \omega(\alpha_{032}) \) time when the attacker performs operations \( \alpha_{031} \) and \( \alpha_{032} \), respectively.

The time characteristics of the attacker's ability to implement the stages of illegal actions to intercept information via parametric channels are formed at the third composite level of the system of characteristics of the effectiveness of response measures to such threats to information security. In this case, the formation procedure is based on establishing inter-level compositional relationships of these characteristics with the characteristics of the second level of this system.

The following expressions (16 – 21) are mathematical models for estimating the average time of implementation of stages of illegal actions to intercept information via parametric channels.

In accordance with the procedure given in [1, 2, 5] for an attacker to implement the TSR operation modes in the process of searching for places of intelligence availability of informative acoustic signals of the VP organs via channels of acoustoelectric transformations, RF irradiation, parasitic (auto) generation and RF imposition, the average value of \( \bar{\omega}(e_1) \) the random value of the time spent by the attacker on the implementation of this stage of illegal actions is determined according to the expression:

\[
\bar{\omega}(e_1) = E(\omega(p_{11})\omega(p_{12})\omega(p_{13})\omega(p_{14}))
\]  

(16)

where \( E(\omega(p_{11}) \circ \omega(p_{12}) \circ \omega(p_{13}) \circ \omega(p_{14})) \) means the average value of the composition of random variables \( \omega(p_{11}), \omega(p_{12}), \omega(p_{13}) \) and \( \omega(p_{14}) \) time when the attacker performs operations \( p_{11}, p_{12}, p_{13} \) and \( p_{14} \) TCP working, respectively.

The given order of implementation by an attacker of the TCP operation modes in the process of interception of electrical signals modulated by informative acoustic signals due to acoustoelectric transformations in the HTSS of the exploration object, the lines of which have an exit outside the controlled zone, allows us to form an expression for determining the average value \( \bar{\omega}(e_2) \) a random value of the time spent by the attacker on the implementation of this stage of illegal actions, in the form of:

\[
\bar{\omega}(e_2) = E(\omega(p_{21})\omega(p_{22}))
\]  

(17)

where \( E(\omega(p_{21}) \circ \omega(p_{22})) \) means the average value of the composition of random variables \( \omega(p_{21}) \) and \( \omega(p_{22}) \) time when the attacker performs operations \( p_{21} \) and \( p_{22} \) TCP working, respectively.

In accordance with the above procedure for implementing the attacker's TCP operation modes in the process of intercepting re-emitted RF signals modulated by informative acoustic signals in the VTSS of the intelligence object, the average value of \( \bar{\omega}(e_3) \) the random value of the time spent by the attacker on the implementation of this stage of illegal actions is determined according to the expression:

\[
\bar{\omega}(e_3) = E(\omega(p_{31})\omega(p_{32}))
\]  

(18)
where $E(\omega(p_{31}) \circ \omega(p_{32}))$ means the average value of the composition of random variables $\omega(p_{31})$ and $\omega(p_{32})$
time when the attacker performs operations $p_{31}$ and $p_{32}$ TCP working, respectively.

The given order of implementation by an attacker of the TCP operation modes in the process of interception of "imposed" high-frequency electrical signals modulated by informative acoustic signals in the VTSS lines of the intelligence object that go beyond the controlled zone allows us to form an expression for determining the average value $\bar{\omega}(e_4)$ a random value of the time spent by the attacker on the implementation of this stage of illegal actions, in the form of:

$$\bar{\omega}(e_4) = E(\omega(p_{41})\omega(p_{42}))$$

(19)

where $E(\omega(p_{41}) \circ \omega(p_{42}))$ means the average value of the composition of random variables $\omega(p_{41})$ and $\omega(p_{42})$
time when the attacker performs operations $p_{41}$ and $p_{42}$ TCP working, respectively.

In accordance with the given procedure for the implementation by an attacker of the TSR operating modes in the process of intercepting high-frequency electromagnetic signals that occur during the operation of generators that are part of technical means and (or) parasitic (auto) generation in the technical means of the intelligence object, the average value of $\bar{\omega}(e_5)$ the random value of the time spent by the attacker on the implementation of this stage of illegal actions is determined according to the expression:

$$\bar{\omega}(e_5) = E(\omega(p_{51})\omega(p_{52}))$$

(20)

where $E(\omega(p_{51}) \circ \omega(p_{52}))$ means the average value of the composition of random variables $\omega(p_{51})$ and $\omega(p_{52})$
time when the attacker performs operations $p_{51}$ and $p_{52}$ TCP working, respectively.

The given procedure for implementing the TCP operation modes by an attacker in the process of analyzing the amount of intercepted information by the criterion of sufficiency for its disclosure allows us to form an expression for determining the average value $\bar{\omega}(e_6)$ a random value of the time spent by the attacker on the implementation of this stage of illegal actions, in the form of:

$$\bar{\omega}(e_6) = E(\omega(p_{61})\omega(p_{62})\omega(p_{63}))$$

(21)

where $E(\omega(p_{61}) \circ \omega(p_{62}) \circ \omega(p_{63}))$ means the average value of the composition of random variables $\omega(p_{61})$, $\omega(p_{62})$ and $\omega(p_{63})$
time when the attacker performs operations $p_{61}$, $p_{62}$ and $p_{63}$ TCP working, respectively.

3. Practical research

These studies are a continuation of the complex experiment described in [1-5]. Assessment of the
effectiveness of mechanisms for identifying threats information leakage on parametric channels, in accordance with the above method, consider the model in relation to the characteristics of illegal acts of interception of information by channels of this type and typical characteristics of mechanisms for identifying threats information leakage.

In order to implement this method, a set of programs has been developed to evaluate the effectiveness of mechanisms for detecting threats of information leakage through parametric channels. Figure 1 shows a dialog box for entering initial data on threat characteristics in accordance with their representation in the form (22), obtained by analyzing the signs of illegal actions $i$, $i = 1, 2, ..., 19$ from their set [5].

$$V = a \log_2 A + b \log_2 B$$

(22)

where: $a$ – the number of unique (non-repeating) actions performed to implement threats of information leakage through parametric channels (procedures for detecting such threats); $A$ – the total number of actions when implementing these threats (procedures for detecting them); $b$ – the number of unique operands used when implementing these actions (procedures); $B$ – the total number of operands used when implementing threats of information leakage through parametric channels (procedures for detecting such threats).
In this case, the column "ID/IND" corresponds to the identifiers and names of functions of the initial level of describing threats of information leakage through parametric channels, the columns "α", "Amin", "Amax", "β", "Bmin", "Bmax" correspond to the parameters of the expression (22).

The values in the "Vmin", "Vmax", "Vsr", and "Vsko" columns correspond to the minimum, maximum, and average values of the information volume of functions and its standard deviation, respectively. These values are determined during the operation of the software package.

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

4. Conclusions
The values obtained in the experiment of the information volume characteristics of the target function of illegal actions to intercept secondary RF radiation of radio-electronic equipment elements (REO) and semi-active tab devices (PAZU) and the target function for detecting threats of information leakage through parametric channels allow us to determine the effectiveness of mechanisms for detecting threats of information leakage through parametric channels, i.e. the efficiency has increased to 78%:

$$E(\theta) = 1 - \left(\frac{V}{V_{\theta} + V}\right)^{7} = 1 - \left(\frac{5152}{(1496+5152)}\right)^{6} \approx 0.78$$  \hspace{1cm} (23)

Thus, the method given in the article for structuring the characteristics of mechanisms for detecting threats of information leakage through parametric channels allows for significantly higher reliability of the assessment than the reliability of the assessment for individual characteristics of threat detection mechanisms that are not connected to any system. The models considered in this paper are a
methodological basis for synthesizing the procedure for evaluating the effectiveness of mechanisms for
detecting threats of information leakage through parametric channels. The use of the efficiency
assessment of mechanisms for detecting threats of information leakage through parametric channels
developed in the article makes it possible to provide a more reliable assessment than traditional methods
of assessment [6-10].

In order to formalize the problem and ways to solve it, in accordance with the formulated content
statement, we denote by \( R(N) \) a set of rules for evaluating the effectiveness of mechanisms for detecting
threats of information leakage through parametric channels by the indicator \( E(b) \) of the specified
nomenclature of \( N \) models. At the same time, \( s(R) \) threat assessment capabilities are provided. Then the
task of modeling mechanisms for identifying threats information leakage on parametric channels can be
viewed as the task of developing a rule set \( R \) that maximizes the possibility's assessment of the
effectiveness of mechanisms for identifying threats information leakage on parametric channel in the
range \( n \) models not exceeding a given \( N \).

This allows you to formally present the problem statement as:
\[
R = \text{argmax} S(R) \\
\text{s.t. } n \leq N 
\]  

The formulated problem of modeling mechanisms for detecting threats of information leakage through
parametric channels should be solved by presenting the following main sequentially solved problems:
- structuring descriptions of the attacker's actions to intercept information via parametric channels and
mechanisms for detecting such actions;
- finding correspondences between the functional and mathematical description of the attacker's actions to
intercept information via parametric channels and mechanisms for detecting such actions in order to obtain a
nomenclature of models that does not exceed the specified one;
- conducting experiments to evaluate the effectiveness of mechanisms for detecting threats of information
leakage through parametric channels;
- determining the value of the indicator of the ability to evaluate the effectiveness of mechanisms for
detecting threats of information leakage through parametric channels for various sets of evaluation rules.

References
[1] Belokurov S V, Lvovich Ya E and Noev A 2019 Applied mathematics, computational Science
and mechanics: current state of the problem 1202. P. 012012
[2] Belokurov S V, Minin Yu V and Morozova O N 2019 Science and mechanics: current state of the
problem 1203. P. 012081
[3] Belokurov S V, Boronenkov A I and Krasnov P E 2012 J Information and security (Voronezh: VSTU)
pp 377-82
[4] Belokurov S V, Skryl S V, Dzhogan V K and Linacre J M 2012 J Voronezh: VI MVD of Russia p116
[5] Belokurov S V, Kuzmenko R V and Shatovkin R R 2017 J Bulletin of the Voronezh Institute of the
Federal penitentiary service of Russia pp 85-97
[6] Zapechnikov S V, Miloslavskaya N G and Tolstoy A I 2006 J Moscow: Hotline-Telecom p 536
[7] Minaev V A, Tyunyakin R N and Filippova N V 2006 J Security of information technologies (M.: MEPhI)
pp 67-70
[8] Lamonov A V 2007 J Security of information technologies (M.: MEPhI) pp 108-13
[9] Minaev V A, Skryl S V and Dvoryankin S V 2008 J Informatics: Conceptual foundations (Moscow:
Maroseyka) p 464
[10] Skryl S V 2009 J Voronezh: VI Ministry of internal Affairs of Russia p 217
[11] Michael E W and Herbert J J 2009 Mattord principles of information security Cengage Learning EMEA
p 598
[12] Brett S J 2004 Tjaden fundamentals of secure computer systems Beedle & Associates ISBN: 1-887902-
66-X.498