Assessment of efficiency of functioning the infocommunication systems a special purpose in the conditions of violation quality of relevance information

A V Parinov, L P Korotkikh, D B Desyatov, L V Stepanov
ET Department, Voronezh Institute Federal Penitentiary Service of Russia, 1a Irutskaya Street, Voronezh, RU

E-mail: a_dushkin@mail.ru

Abstract. The uniqueness of information processing mechanisms in special-purpose infocommunication systems and the increased interest of intruders lead to an increase in the relevance of the problems associated with their protection. The paper considers the issues of building risk-models for the violation of the relevance and value of information in infocommunication systems for special purposes. Also, special attention is paid to the connection between the qualities of relevance and the value of information obtained as a result of the operation of infocommunication systems for special purposes. Analytical expressions for the risk and damage function in the time range in special-purpose infocommunication systems are obtained, which can serve as a mathematical basis for risk assessment. Further, an analytical expression is obtained to assess the chance of obtaining up-to-date information in the operation of infocommunication systems up to the time the information quality is violated. An analytical expression for estimating the chance can be used to calculate the effectiveness of a special-purpose infocommunication system.

1. Introduction
At present, the functioning of the Special-Purpose Infocommunication System (SPIS) plays a key role in ensuring security and making effective strategic decisions. At the same time, the uniqueness of information processing mechanisms in SPIS and the increased interest of malefactors lead to an increase in the urgency of problems related to their protection [1-7].

Attacks on special-purpose infocommunication systems are used to achieve the following objectives: obtaining information of varying degrees of confidentiality, as well as for reducing the usefulness of information received from SPIS after the attack. Problems of protection of SPIS were considered [8, 9]. In these works, the directions of their solution, the risks of special-purpose infocommunication systems [10-15] and the survivability of SPIS were analyzed to some extent [16-24]. However, these studies did not consider violations of the quality of the relevance and value of information, which is especially relevant in that the specificity of SPIS is related to the relevance of the data it produces.

The aim of the work is to develop a method for constructing a risk-model of the violation of the relevance and value of information in special-purpose infocommunication systems, as well as their interrelationships [25-32]. This is necessary to assess the effectiveness of such systems in the context of a violation of the quality of the relevance of information.
2. Risk assessment
Information has aging properties, since it is subject to the influence of time, therefore, information resources have a certain "life" period.

And the effect of aging i.e. the decline in value over time and the artificial retention of information, depending on the importance of the decision taken, can lead to very harmful consequences. Risk analysis in this case is simply necessary.

A fundamental feature of the functioning of the SPIS is that its utility function has a non-linear nature of the buildup during the operation of the system. And, according to the law of marginal utility [4, 15], the first derivative in the dynamics of this function tends to the expression:

$$\frac{\partial \omega}{\partial x} = a \omega, \quad (1)$$

where $\omega$ – utility function, $x$ – quantity of consumed goods, $a$ – coefficient of value, depending on the specifics of the SPIS.

When operating an infocommunication system of a special purpose, its use is associated with the receipt of some information. Suppose that it comes with a relatively constant intensity $P\lambda$. From here it is possible to write down $x = \lambda t$. Carrying out the normalization for the average duration of the successful operation of SPIS $T_{sp}$, we rewrite the last expression in the following form, $x = \tilde{\lambda} \tilde{t}$ where $\tilde{t} = t/T_{sp}$ and $\tilde{\lambda} = \lambda T_{sp}$.

This approach allows us to further operate with $x$ as a dimensionless quantity.

Let us now return to expression (1) and carry out the corresponding substitution:

$$\frac{\partial \omega}{\partial \tilde{\lambda} \tilde{t}} = a \omega, \quad (2)$$

The solution of the last equation is obviously an exponential. Taking into account the start information $b$ and the current $\lambda_{sp}$ loss of information during the operation of the SPIS, we have:

$$\omega(t) = \exp\left(a\lambda_{sp}t + b - \lambda_{sp}t\right),$$

or

$$\omega(t) = \exp\left[a(\lambda_{sp} - \lambda_{sp})t + b\right],$$

or

$$\omega(t) = \exp[a \lambda t + b],$$

where $\lambda = \lambda_{sp} - \lambda_{sp}$, $a$ and $b$ – dimensionless (normalized) quantities.

In the normalized form, the last expression takes the following form:

$$\omega(\tilde{t}) = \exp\left[\tilde{a} \tilde{\lambda} \tilde{t} + \tilde{b}\right]. \quad (2)$$
We now determine the chances and risks \([3,11]\) of the violation of the quality of the information's relevance at a time \(t_0\). In this case, the probability density and the accumulated probability of violation of the quality of the information's topicality will be denoted by \(f(t)\) and \(F(t)\), respectively.

Usually, the risk is defined as the product of the amount of damage to the likelihood of its occurrence \([4]\).

\[
Risk(t) = f(t) \cdot u(t) \Delta t,
\]

where \(u(t)\) – amount of damage, \(f(t)\) – the probability of occurrence of an event of a violation of the quality of the information's relevance, \(\Delta t\) – sampling step.

The damage function can be obtained with the utility function, the graph of this function is shown in figure 1.

The area of the shaded figure in the gap is the damage \([0; t_0]\) due to the current loss of information, and the area of the shaded figure on the gap \([t_0; T_{av}]\) represents a lost profit that a special-purpose information-communication system could have brought had it not lost its operability at time \(t_0\).

![Figure 1. The graph of the utility function.](image_url)

Hence the damage is:

\[
u(t_0) = \int_0^{t_0} \exp[a\lambda_p t + b] dt - \int_0^{t_0} \exp[a(\lambda_p - \lambda_y) t + b] dt + \int_{t_0}^T \exp[a(\lambda_p - \lambda_y) t + b] dt.
\]

Performing simple mathematical operations, we obtain the formula (4):

\[
u(t_0) = \int_0^{t_0} \exp[a\lambda_y t + b] dt + \int_{t_0}^T \exp[a(\lambda_p - \lambda_y) t + b] dt = \frac{\exp[b] \left( \exp[a\lambda_p T_{av} - a\lambda_y T_{av}] - \exp[a\lambda_p t_0 - a\lambda_y t_0] \right)}{a(\lambda_p - \lambda_y)} + \frac{\exp[b] \left( \exp[a\lambda_y t_0] - 1 \right)}{a\lambda_y}.
\]

The graph of the damage function is shown in the figure 2.

This chart is schematically similar to the utility function graph, which corresponds to its physical meaning, the ISSN brings little damage at the implementation stage, and since the loss of its efficiency, the value of the damage has increased dramatically.
Thus, the value of damage was found throughout the lifetime of the SPIS.

![Figure 2](image)

**Figure 2.** The schedule of the damage function.

According to [6, 12-14], cases of violation of the quality of the information’s relevance correspond to the log-logistic distribution law [28-32]. The probability density function for the log-logistic distribution law is [7, 16-18]:

\[
f(t) = \frac{(\beta / \alpha)^{t / \alpha}}{[1 + (t / \alpha)^{\beta}]}.
\]

(5)

where \( t > 0, \alpha > 0, \beta > 1 \),

\( \alpha \) – scale parameter,

\( \beta \) – form parameter.

The probability density function – mode [7] assumes the maximum value at the point:

\[
t_{\text{max}} = \alpha \beta \sqrt{\beta - 1} \sqrt{\beta + 1}.
\]

(6)

Substituting \( t_{\text{max}} \) in (5) we obtain:

\[
f_{\text{max}} = \frac{\beta^{-1}}{(\beta - 1)^{\beta} (\beta + 1)^{\beta}} \frac{(\beta + 1)^{\beta+1}}{4\alpha\beta}.
\]

(7)

Thus, the step of sampling is:

\[
\Delta t = \frac{4\alpha\beta}{(\beta - 1)^{\beta-1} (\beta + 1)^{\beta+1}}.
\]

(8)

Taking into account formulas (4), (5) and (8), the analytic expression for the risk function is represented as follows:
\[ \text{Risk}(t_0) = \left[ \frac{b}{a} \left( \frac{a \lambda_y t - a \lambda_y t_0}{a \lambda_y - \lambda_y} \right) - \exp \left[ a \lambda_y t - a \lambda_y t_0 \right] \right] \times \frac{4 \alpha \beta}{\left[1 + (t_0 / \alpha)\right]^{\beta-1}} \times \frac{4 \alpha \beta}{(\beta - 1) (\beta + 1)^{\beta-1}}. \]  

(9)

In the subsequent calculations, to simplify the calculations, one should take for a constant value $\Delta t = \text{const}$, and the $a(\lambda_y - \lambda_y) = z$, $a \lambda_y = c$ value then:

\[ \text{Risk}(t_0) = \left[ \frac{e^b \left( e^{cT} - e^{c_0} \right) + e^b \left( e^{c_0} - 1 \right)}{c} \right] \times \frac{(\beta / \alpha)(t_0 / \alpha)^{\beta-1}}{\left[1 + (t_0 / \alpha)\right]^{\beta-1}} \times \Delta t. \]  

(10)

To solve the problems of preserving the quality of the actuality of information in general, it is necessary to determine the risk parameters. We calculate the risk parameters for the resulting damage expression and the log-logistic distribution law.

We now turn to the calculation of the mode and the peak of risk. The mode is found by solving the task of investigating the risk function for extremes [19, 20].

Equate the resulting expression to zero:

\[ \Delta t \frac{e^b \left( \beta / \alpha \right)(t_0 / \alpha)^{\beta-1}}{c \left[1 + (t_0 / \alpha)\right]^{\beta-1}} \times \left((t_0 / \alpha)^\beta + 1\right) \times \left(c ze^{c_0} - cze^{c_0} + z \beta (e^{c_0} - 1) - \right. \]

\[ \left. - z(e^{c_0} - 1) - c \beta \left(e^{cT} - e^{c_0} \right) - c\left(e^{cT} - e^{c_0} \right) \right) = 0. \]

Critical points, functions $\text{Risk}(t_0)$ on the investigated interval $[0; T_0]$:

\[ \frac{e^b \left( \beta / \alpha \right)(t_0 / \alpha)^{\beta-1}}{c \left[1 + (t_0 / \alpha)\right]^{\beta-1}} = 0; \]

or

\[ (t_0 / \alpha)^\beta + 1 = 0; \]

or

\[ (c ze^{c_0} - cze^{c_0} + z \beta (e^{c_0} - 1) - z(e^{c_0} - 1) - c \beta (e^{cT} - e^{c_0}) - c\left(e^{cT} - e^{c_0} \right) = 0. \]

The first equation has a solution $t_0 = 0$, that does not satisfy the condition $t_0 > 0$. The second equation has no positive solution.

We now turn to the solution of the last equation:

\[ cze^{c_0} - cze^{c_0} + z \beta e^{c_0} - z \beta - ze^{c_0} + z - c \beta e^{cT} + c \beta e^{c_0} - ce^{cT} + e^{c_0} = 0 \]

\[ e^{c_0} (c z + \beta z - z) - e^{c_0} (c z - c \beta - z) - c \beta e^{cT} - ce^{cT} - z \beta + z = 0. \]

To simplify the notation, we introduce the notation

\[ cz + \beta z - z = N; \]
The equation takes the form:

\[ e^{c_0} \cdot N - e^{c_0} \cdot P - Q = 0. \]

We use the expansion of the exponential in a Taylor series, restricting ourselves to the first three terms. We have:

\[
\begin{align*}
&
\left(1 + t_0 c + \frac{t_0^2 c^2}{2}\right)N + \left(1 + t_0 z + \frac{t_0^2 z^2}{2}\right)P - Q = 0; \\
&
N + t_0 c N + \frac{c^2 N}{2} t_0^2 + P + t_0 z P + \frac{z^2 P}{2} t_0^2 - Q = 0; \\
&
\left(\frac{c^2 N}{2} + \frac{z^2 P}{2}\right) t_0^2 + (cN + zP) t_0 + N + P - Q = 0.
\end{align*}
\]

We have a quadratic equation:

\[
D = (cN + zP)^2 - 4(N + P - Q)\left(\frac{c^2 N}{2} + \frac{z^2 P}{2}\right);
\]

\[
t_{1,2} = \frac{-(cN + zP) \pm \sqrt{D}}{c^2 N + z^2 P}.
\]

Presumably, the value of the second root is equal to the negative value, which contradicts the assertion that then the value \( t > 0 \), of the mode is equal to:

\[
t_1 = \frac{- (cN + zP) + \sqrt{(cN + zP)^2 - 4(N + P - Q)\left(\frac{c^2 N}{2} + \frac{z^2 P}{2}\right)}}{c^2 N + z^2 P}.
\]

Let the value of the mode \( t_1 = t_n \), then the maximum damage will be equal to:

\[
u(t_n) = \frac{e^b (e^{c_0} - e^{c_1})}{z} + \frac{e^b (e^{c_1} - 1)}{c}.
\]

Consequently, the calculation formula for the risk peak has the following form:

\[
\text{Risk}(t)_{\text{max}} = \text{Risk}(t) \approx \left[ \frac{e^b (e^{c_0} - e^{c_1})}{z} + \frac{e^b (e^{c_1} - 1)}{c} \right] \times \frac{(\beta / \alpha) (t_n / \alpha)^{\beta-1}}{\left[1 + (t_n / \alpha)^{\beta}\right]} \times \Delta t.
\]

The obtained analytical expressions for risk can serve as a mathematical basis for assessing the risk of SPIS. In turn, the risk function will be used by us in the future when assessing the viability of these systems.
3. Evaluation of the chance of obtaining up-to-date information

If the risk function has the meaning of a probabilistic evaluation of the occurrence of damage at some point in time, then the chance function is something else like a probabilistic estimate of the receipt by some system of use at an arbitrary moment in time.

In general, the function of chance is as follows [3, 21-24]:

\[ \text{Chance}(t_0) = v(t_0)\left[1 - F(t_0)\right], \]  \hspace{1cm} (13)

where \( v(t_0) \) – the benefits of using a special-purpose infocommunication system, 

\( (1 - F(t_0)) \) – probability of failure-free operation of system components up to the moment \( t_0 \).

Thus, we have:

\[ F(t_0) = \int_0^{t_0} f(t) dt = \frac{(t_0 / \alpha)^\beta}{1 + (t_0 / \alpha)^\beta}. \]  \hspace{1cm} (14)

Then the probability of failure-free operation:

\[ 1 - F(t_0) = \frac{1}{1 + (t_0 / \alpha)^\beta}. \]  \hspace{1cm} (15)

We will count the favor as a benefit obtained from the use of SPIS in a period of time \([0; t_0]\). To find it, we use the utility function, developed by us earlier.

The benefit received by the system at the supposed moment of violation of the quality of the information's relevance is determined from the utility function by integrating the latter by the parameter \( dt \) in the interval \([0; t_0]\), where \( t_0 \) is the alleged moment of violation of the quality of the information's relevance.

\[ v(t_0) = \int_0^{t_0} \exp\left[a(\lambda_\nu - \lambda_\gamma)t + b\right] dt = \frac{e^\beta(e^{\lambda_\nu \alpha / \beta} - 1)}{a(\lambda_\nu - \lambda_\gamma)}. \]  \hspace{1cm} (16)

Thus, we have an expression for assessing the chance of obtaining up-to-date information from the infocommunication system up to the time of the violation of the quality of the information's relevance \( t_0 \):

\[ \text{Chance}(t_0) = \frac{e^\beta(e^{\lambda_\nu \alpha / \beta} - 1)}{a(\lambda_\nu - \lambda_\gamma)} \cdot \frac{1}{1 + (t_0 / \alpha)^\beta} = \frac{e^\beta(e^{\lambda_\nu \alpha / \beta} - 1)}{a(\lambda_\nu - \lambda_\gamma)[1 + (t_0 / \alpha)^\beta]}. \]  \hspace{1cm} (17)

We use the substitution as in solving the risk, let \( a(\lambda_\nu - \lambda_\gamma) = z \), then:

\[ \text{Chance}(t_0) = \frac{e^\beta(e^\gamma - 1)}{z[1 + (t_0 / \alpha)^\beta]}. \]  \hspace{1cm} (18)

This formula shows the dependence of the chance on time \( t_0 \), as well as \( a, b, \lambda_\nu, \lambda_\gamma, \alpha, \beta \).

Thus, an analytical expression was obtained to assess the chance of obtaining up-to-date information in the operation of SPIS until the quality of the information is violated \( t_0 \). The analytical expression for the assessment of the chance will be used by us in the future to calculate the performance of the infocommunication system for special purposes.
4. Evaluation of the effectiveness of the infocommunication system

In the context of the risk analysis of the violation of the quality of the information’s relevance, it is appropriate to solve the task of determining the effectiveness of the work of the SPIS [5, 9].

Traditionally, the efficiency of a system is understood to mean the ratio of the cost to total costs. We estimate the efficiency of the system using the expression [4, 11]:

\[
E = \frac{\text{Chance}(t_0) - \text{Risk}(t_0)}{Z(t_0)} - 1, \tag{19}
\]

where \( \text{Chance}(t_0) \) and \( \text{Risk}(t_0) \) – risk assessment and the chance of SPIS at the moment \( (t_0) \);

\( Z(t_0) \) – total costs of maintaining the life of the SPIS at the time \( (t_0) \).

Costs in this case are understood, in particular, the cost of deployment and commissioning of SPIS, as well as the costs of maintaining the system of protection of SPIS and the elimination of destructive influences.

Thus, we will define an expression for the evaluation of the effectiveness of SPIS.

\[
E = \frac{\text{Chance}(t_0) - \text{Risk}(t_0)}{Z(t_0)} - 1 = \left[ \frac{e^\beta (e^{\alpha} - 1)}{z} \right] - \left[ \frac{e^\beta (e^{\alpha} - e^{\alpha_n}) + e^\beta (e^{\alpha} - 1)}{z} \right] \times \frac{(\beta / \alpha)(t_0 / \alpha)^{\beta-1}}{1 + (t_0 / \alpha)^{\beta}} - 1 = \tag{20}
\]

\[
Z(t_0) \times e^{\beta} - \left[ ce^\beta (e^{\alpha} - e^{\alpha_n}) + ze^\beta (e^{\alpha} - 1) \right] (\beta / \alpha)(t_0 / \alpha)^{\beta-1} - 1.
\]

The expression of efficiency over the whole period of the functioning of the SPIS, taking into account the discretization of time, can be written in the form:

\[
E = \sum_{k=1}^{n} \left[ 1 + (k / n\alpha)^{\beta} \right] \left( e^{\beta} (e^{\alpha} - 1) - \sum_{k=1}^{n} \left( e^\beta (e^{\alpha} - e^{\alpha_k}) + ze^\beta (e^{\alpha} - 1) \right) (\beta / \alpha)(k / n\alpha)^{\beta-1} \right] \times \frac{Z(k / n) \times e^{\beta} (1 + (k / n\alpha)^{\beta})^2}{1}\times \Delta t \tag{21}
\]

5. Calculation of risk sensitivity coefficients

The dynamics of the risk movement will be estimated using the sensitivity coefficients. Consider the risk function obtained earlier:

\[
\text{Risk}(t_0) = \left[ \frac{e^\beta (e^{\alpha} - e^{\alpha_n}) + e^\beta (e^{\alpha} - 1)}{z} \right] \times \frac{(\beta / \alpha)(t_0 / \alpha)^{\beta-1}}{1 + (t_0 / \alpha)^{\beta}} \times \Delta t, \tag{22}
\]

where: \( t_0 \) – the moment of violation of the quality of the relevance of the information, \( T_{\alpha} \) – the average duration of use of SPIS, \( \alpha, \beta \) – the parameters of the probability distribution of the occurrence of a violation of the quality of the information's relevance.

To find the coefficient of differential sensitivity with respect to the parameter \( \beta \), we find the partial derivative of the risk function with respect to the shape parameter:
Let us analyze the behavior of the sensitivity function for various values of $\alpha$ for a given value vector of the shape parameter (fig. 3-4).

![Graph](image1)

**Figure 3.** Graph of the differential sensitivity function depending on the form parameter when $t_0=0.8$, $\alpha=2$.

![Graph](image2)

**Figure 4.** Graph of the differential sensitivity function depending on the form parameter when $t_0=0.8$, $\alpha=4$.

Let us find the partial derivative with respect to the scale parameter:

$$
\frac{d\text{Risk}(t_0)}{\alpha} = \Delta t \left[ \frac{e^{\beta (e^{\alpha t_0} - 1)} - e^{\beta t_0 (e^{\alpha t_0} - e^{\alpha t_0})}}{t_0} \right] \frac{(\beta / \alpha) (t_0 / \alpha)^{\beta-1}}{[1 + (t_0 / \alpha)^{\beta}]^{2}}.
$$

(24)

Let us analyze the behavior of the sensitivity function for various values of $\beta$ for a given vector of parameter values (fig. 5-6).

Analysis of the graphs in figures 3-6 allows us to conclude that the risk function is sensitive to changing the shape and scale parameter over the entire time range, and it is advisable to take measures...
to regulate the risk of violating the quality of the information's topicality in the SPIS at any stage of its life cycle.

Figure 5. Graph of the differential sensitivity function depending on the scale factor when $t_0=0.8$, $\beta=2$.

Figure 6. Graph of the differential sensitivity function depending on the scale factor when $t_0=0.8$, $\beta=4$.

6. Conclusion
Thus, in the work the questions of construction of risk-models of violation of the qualities of relevance and value of information in infocommunication systems of special purpose are considered. Particular attention is paid to the connection between the qualities of relevance and the value of information obtained as a result of the operation of infocommunication systems of a special purpose. Analytical expressions for the risk and damage function in the time range in special-purpose infocommunication systems are obtained, which can serve as a mathematical basis for risk assessment. An analytical expression is obtained for assessing the chance of obtaining up-to-date information in the operation of infocommunication systems up to the time when information quality is upsetting. An analytical ex-
pression for estimating the chance can be used to calculate the effectiveness of a special-purpose information communication system. The obtained analytical expressions can be useful for assessing the viability of information communication systems for special purposes.

References
1. Ostapenko A G, Ermilov E V and Kalashnikov A O 2013 Innovative development trends and information risks of IT sector development in the context of critical facilities provision Information and Security 3 pp 323-334
2. Ostapenko A G, Karpeev D O and Plotnikov D G 2009 Prospects for the development of the methodology of risk analysis of systems Information and Security 3 pp 419-424
3. Ostapenko A G, Plotnikov D G, Makarov O Yu, Tikhomirov N M and Yurasov V G 2013 Viability of attacked distributed systems: assessment of risks of fatal component failures (Voronezh: Scientific book) p 160
4. Ostapenko A G, Ermilov E V and Kalashnikov A O 2013 Risks of damage, the chances of utility and resilience of the components of automated systems under the impact of information threats on them Information and Security 2 pp 215-218
5. Ostapenko A G, Kalashnikov A O, Ermilov E V and Korneeva N N 2014 Formalization of the risk management process in the information technology infrastructure of a critical facility Information and Security 2 pp 164-179
6. Davydov A A 2010 Distribution of the rates of innovative development of the countries of the world Official site of the ROS p 11
7. Ostapenko A G, Plotnikov D G, Ostapenko O A and Maslikhov P A 2012 Loglogistic distribution of damage: the calculation of the risk of ITCS based on the risk parameters of its components Information and Security 3 pp 425-428
8. Ostapenko A G, Ermilov E V and Kalashnikov A O 2013 Risks of damage, the chances of utility and resilience of the components of automated systems under the impact of information threats on them Information and Security 2 pp 215-218
9. Ostapenko G A, Plotnikov D G and Rogozin A S 2013 The vitality of elements of critical information infrastructures: an analytical assessment with allowance for possible damages Information and Security 3 pp 353-364
10. Ostapenko G A, Plotnikov D G, Shcherbakova N Yu and Zarubin V S 2013 On the issue of assessing the damage and resilience of attacked distributed information systems: the development of methodological support Information and Security 1 pp 141-142
11. Ostapenko G A, Plotnikov D G and Meshkova E A 2010 Methodical and algorithmic support of calculation of risk parameters for components of distributed systems Information and Security 3 pp 335-350
12. Ostapenko G A, Plotnikov D G, Batishchev R V and Goncharov I V 2010 Distributed systems: methodologies for assessing effectiveness under attack conditions Information and Security 3 pp 359-366
13. Ostapenko A G, Plotnikov D G, Makarov O Yu, Tikhomirov N M and Yurasov V G 2013 Viability of attacked distributed systems: an assessment of the risks of fatal component failures (Voronezh: Scientific book) p 160
14. Ostapenko G A and Plotnikov D G 2012 On the issue of assessing the survival of information systems of an innovative nature Information and Security 3 pp 413-417
15. Parinov A V, Parinova L V and Yurasov V G 2013 Risk-assessment of mortality of innovative projects: scientific and methodological basis Information and Security 3 pp 423-426
16. Parinov A V Parinova L V and Zaryaev A V 2014 Risk management of innovative projects Information and Security 4 pp 602-605
17. Ostapenko A G 2010 Function of the possibility in assessing the risks, chances and effectiveness of systems Information and Security 2 pp 17-20
18. Ostapenko A G, Karpeev D O and Plotnikov D G 2009 Prospects for the development of the methodology of risk analysis of systems Information and Security 3 pp 419-424
19. Ostapenko G A, Plotnikov D G, Shcherbakova N Yu and Barannikov N I 2013 Models of survivability of the attacked distributed information system: risk-formalization with allowance for possible damage Information and Security 1 pp 63-68
20. Ostapenko G A, Plotnikov D G, Batishchev R V and Goncharov I V 2010 Distributed systems: methodologies for assessing effectiveness under attack conditions Information and Security 3 pp 359-366
21. Popov E A and Ostapenko G A 2014 Dos-attacks on innovative state distributed information systems: risk analysis in case of irregular distribution of damage Information and Security 3 pp 456-459
22. Rad'ko N M, Parinova L V, Pasternak Yu G, Razinkin K A and Tikhomirov N M 2013 Some assessments of risks, chances and survivability of networks in the context of information attacks of a viral nature Information and Security 4 pp 498-499
23. Ostapenko G A, Bursa M V and Tolstoy N N 2013 Risk-model of the innovative project, functioning in the face of threats of ddos-attacks Information and Security 3 pp 443-444
24. Ivankin E F, Mashin S V and Losev O A 2012 Virus attacks on the information resources of innovative projects: risk management Information and Security 3 pp 401-406
25. Dushkin A V, Novoseltsev V I and Sumin V I 2016 Methodological bases of construction of the protected automated systems: the monography (Voronezh: Scientific book) p 76
26. Balan V P, Dushkin A V, Novoseltsev V I and Sumin V I 2016 Risk and reflection: monograph (Moscow: Hot line – Telecom) p 136
27. Balan V P, Dushkin A V, Novoseltsev V I and Sumin V I 2015 Conflict Management (Moscow: Hot line – Telecom) p 144
28. Dushkin A V, Kravchenko A S, Novoseltsev V I, Smolentseva T E and Sumin V I 2014 Mathematical models and information processes of complex object control: Monograph (Voronezh: Scientific book) p 125
29. Barkalov S A, Dushkin A V, Kolodyazhny V I and Sumin V I 2017 Introduction to system analysis: Monograph (Moscow: Hot line – Telecom) p 234
30. Barkalov S A, Dushkin A V, Kolodyazhny S A and Sumin V I 2017 Introduction to the system design of intellectual knowledge bases: monograph (Moscow: Hot line – Telecom) p 108
31. Novoseltsev V I, Kochedykov S S and Orlova D E 2017 Tensor analysis of Crohn and its applications: monograph (Voronezh: Scientific book) p 220
32. Sumin V I, Dushkin A V and Kravchenko A S 2014 Modeling of systems (Voronezh: Scientific Book) p 222