Model of analysis of sustainable management of information security of a distributed information system

P.I. Tutubalin[1], E.M. Komissarova[1], N.K. Arutyunova[1]

[1]Kazan National Research Technical University named after A.N. Tupolev, K.Marx St. 10, Kazan, Tatarstan, Russia, 420111

Abstract. The article presents a model of stability analysis of a distributed information system in the sense of sustainable provision of its information security with some means of protection. It is assumed that the information system in question is operating in real time. On the basis of the proposed model, the area of functional security of a distributed information system under the influence of information attacks of the enemy is constructed, while this task is solved from the condition of specified allowed intervals: the probability of ensuring the information security of the system under consideration, as well as the criterion of deterioration of the main indicator of its effectiveness from enemy interference in process of its functioning. In the form of a strict sequence of actions, an algorithm is formulated to implement the proposed model in practice, provided that the information security of a distributed information system is managed reliably.

Keywords: analysis, system stability, system model, information security, distributed system.

1. Introduction

Among open works in which the issues of information security or information protection are affected in one way or another, there are practically no works that deal with issues related to sustainable management of the required level of information security, that is, the bulk of open works do not test the level of information security of certain systems in terms of its sustainable position.

At the same time there is an increase in the need for works related to the resolution of issues of information security and information security. This can be seen from the continuous growth of works aimed at covering the development, design and operation of information systems.

Let us mention some of these works. Firstly, it is possible to single out a large cluster of works devoted to the processing of graphic and video information [1-3], which notes the fact that ever larger and larger volumes of information need to be stored and processed. A special place in the design, development and operation of such systems is occupied by the preliminary practically consistent modeling of the processes in these processes [4-6]. The complex systems considered in these works naturally need reliable protection against interference by third parties in the process of their functioning, as well as the sustainable provision of this protection process.

It is natural to note that in all systems using the models and methods noted in [1-6], it is necessary to apply sufficiently reliable approaches, models and methods to ensure the safety of the information

that is circulated and processed in these systems. In this regard, we recommend that attention be paid to a number of the following papers [7-12], in which the basic principles, approaches and methods are sufficiently thoroughly expounded, which allow both to substantially increase the information security level of a particular system, and to ensure the necessary level of information security of the said system.

In addition to the works [7-12], we will further propose an approach to the stable provision of information security of data in arbitrary distributed information systems, mainly functioning in real time.

2. On stability in a classical and managerially significant sense

In the classical understanding of stability, the following meaning is usually embedded: the ability to return with the passage of time of the system after removing some perturbing influence in a state in which the system remained until the application of the indicated effect on it.

A situation is possible when a certain system **A**, being under the influence of external perturbations or else also internal, is in principle not stable in this sense. But if it is possible to build some control system **B**, which is preemptive, and having a sufficiently high degree of speed, it exerts such influences that extinguish the internal and external influences that excite the system **A**, deriving it from equilibrium in the classical sense of the word of position, then such a system **A`**, already newly formed, can be called stable. In principle, such a state of affairs becomes possible when the control system **A** of the selected control scheme is provided in the prediction mode of its possible behavior to a certain extent (for example, future states of system **A**) under the influence of external controls (environment), internal changes and own control actions resulting from the constructed control subsystem **B**.

In the course of analysing and ensuring the sustainable management of the information security of a distributed information system, it is necessary to adhere to exactly this understanding of sustainability, which is given in the previous paragraph; further, based on this, all arguments are based on building a model for analysing the stability of the information security of distributed information systems.

3. The model of analysis of the stability of information security

Let's pass to the consideration of the model allowing to analyse and form a stable management of information security by some distributed information system.

We assume that the system under consideration can be subject to enemy attacks, while the information security administrator of this system is able to predict the nature and intensity of these attacks.

Considering what has been said, let us pass to the definition of the so-called functional safety domain of the given system.

We introduce the following notations: $\boldsymbol{q}$ is the probability of ensuring the information security of the system in question, $\boldsymbol{\Delta E}$ is a possible reduction in the functional efficiency indicator of the system under consideration from harmful enemy actions in the system operation.

The expression $\boldsymbol{\Delta E(q)}$ will have a maximum value of $\boldsymbol{\Delta E_{max}}$ in the case where $\boldsymbol{q} = 0$ and the lowest $\boldsymbol{\Delta E_{min}}$ at $\boldsymbol{q} = 1$, respectively. It should be noted that the value of $\boldsymbol{E_{min}}$ is not directly related to the level of information security of the system, since the system may not fulfill its functional load and for reasons far from the information security of the system, but this influence must be taken into account and clearly defined in practical tasks. The general form of the dependence $\boldsymbol{\Delta E(q)}$ is shown in figure 1.

We will assume that $\boldsymbol{r_p}$ and $\boldsymbol{r_a}$, respectively, the duration of the cycle when performing manual and automated control of some considered system. Then we can assume that $\Delta E_{\max} = r_{\mathrm{p}} - r_{\mathrm{a}}$ and $\Delta E_{\min} = \varepsilon$, where the value $\varepsilon \geq r_{\mathrm{a}}$.

Let for the considered system the interval $[\Delta E_1, \Delta E_2]$ is defined, the meaning of which is that the values of its components correspond to the mode of normal functioning, the permissible level of information security.

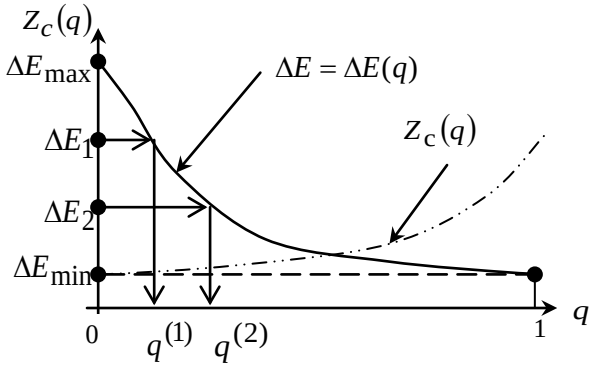

Figure 1. The general form of the dependence **Δ*E*(*q*)**.

We introduce an expression $Z_c(q)$ characterizing the resource costs that should be created to create an information security system for some distributed information system with a probability value ***q*** for it.

In order to find the optimal value of the indicator ***q***, it is proposed to solve the problem of the following form:

$$(\Delta E, Z_c) \to \min_{0<q<1}$$

We shall construct a set of optimal solutions of this problem by minimizing the following linear convolution:

$$L(q,d) = \alpha\Delta E(q) + (1-\alpha)Z_c(q) \to \min_{0<q<1}, \ \alpha \in (0,1).$$

If the functions $\Delta E(q)$ and $Z_c(q)$ are continuous and differentiable, then for the indicated linear convolution one can write the parametric solution in the indicated form: $q^0 = q(\bar{\alpha}), \alpha \in (0,1)$. Then, the values α_1 and α_2 can be calculated as: $\alpha_1 = \arg\left\{ q(\alpha) = q^{(1)} \right\}$ and $\alpha_2 = \arg\left\{ q(\alpha) = q^{(2)} \right\}$.

Accordingly, we form the interval $[q^0(\alpha_1), q^0(\alpha_2)]$, the probability value q^* is selected from it. The chosen choice should be made by the decision maker from the staff of the system in question and the developers of the information security system. In addition to selecting a compromise value q^*, a value $\pm\Delta q$ is selected that limits the guaranteed interval $[q^* - \Delta q, q^* + \Delta q] \subset [q^{(1)}, q^{(2)}]$ change the probability of ensuring the information security of the system.

The level of information security of the system, dictated by the boundaries of the interval, should be ensured with the help of the correct choice and introduction in the practice of its work of appropriate methods and means of software and hardware information protection.

It should be noted that in order to ensure a given level of information security $[q^* - \Delta q, q^* + \Delta q]$, all the selected security measures should be subjected to the procedure of automated testing using the methodology proposed and described in [7-10].

Let us proceed to the formation of a model of the system, which can be under the direct harmful effect of information attacks by a potential adversary.

In the course of the conducted review of the open publication it was revealed almost complete absence of similar models.

At the first step of constructing such a model, we confine ourselves to a simplified functional model of such a system. In this case, we base the model on the formalism of Markov processes, in which the set of states is discrete, and it is also assumed that time flows continuously.

We will assume that the system under consideration can be in the following two states: S_0 - the system is functioning normally, its information security level is estimated as satisfactory; S_1 - the system suffers damage, being under the influence of some information attacks of a potential adversary.

We assume that the attack flow can be regarded as approximately Poisson and can be characterized by the intensity **λ**.

In the event that an attack is detected on the system, then there are regulated actions to track its impact on the system. We will assume that in view of the fact that there is uncertainty in the direction and possible consequences of the attack, the regulatory actions will require the expenditure of time subject to a random law. For simplicity of the initial description of the model, we will assume that this law is indicative with its characteristic parameter **μ**, which should be interpreted as the recovery rate of a given level of information security of the system, figure 2.

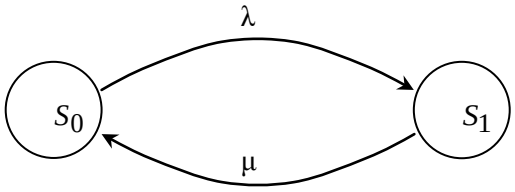

Figure 2. The nature of the interaction of the distinguished states of the system.

We take the following notation: $P_i(t)$ - the probability of finding the system at time ***t*** in the state $S_i, i = \overline{(0,1)}$. The above probabilities can be determined from the following mathematical model, which is built on the basis of the graph, which is shown in Figure 2:

$$\dot{p}_0 = -\lambda \cdot p_0 + \mu \cdot p_1; \tag{1}$$

$$\dot{p}_1 = \lambda \cdot p_0 - \mu \cdot p_1, \quad t \geq t_0; \tag{2}$$

$$p_0(t) + p_1(t) = 1, \quad t \geq t_0; \tag{3}$$

$$p_0(t_0) = p_{00}, \quad p_1(t_0) = p_{10}. \tag{4}$$

The next step is to determine the equilibrium position of the system $p^* = (p_0^*, p_1^*)$. To this end, well-known approaches can be used, as a result of which we obtain the following expressions:

$$p_0(t) = \frac{\mu}{\lambda+\mu} + \left(p_{00} - \frac{\mu}{\lambda+\mu} \right) \cdot e^{-(\lambda+\mu)(t-t_0)};$$

$$p_1(t) = \frac{\lambda}{\lambda+\mu} - \left(p_{10} - \frac{\lambda}{\lambda+\mu} \right) \cdot e^{-(\lambda+\mu)(t-t_0)}. \tag{5}$$

From (5) it follows that the equilibrium point (p_0^*, p_1^*) of system (1) - (4) is in its way asymptotically stable in the sense of Lyapunov, and it is independent of the values of the parameters t_0, p_{00}, **λ** and **μ**.

Thus, it can be argued that a system that is described by the model (1) (4) and operates on a sufficiently long time interval does not require stabilizing stability management in the sense that is given in this paper.

The parameter **μ** itself, which is included in the model (1) - (4), will be used directly to solve the problems of ensuring the required level of information security of the system, which should not exceed the limits specified by the interval $[q^* \pm \Delta q]$.

So, it is known that

$p_0^* = p_0(\infty)$, $p_1^* = p_1(\infty)$.

We require that the following inequalities hold:

$$q^* - \Delta q < p_0^*(\mu) < q^* + \Delta q. \tag{6}$$

To satisfy inequalities (6) it is necessary and sufficient that:

$$\frac{(q^* - \Delta q)\lambda}{1 - q^* + \Delta q} < \mu < \frac{(q^* + \Delta q)\lambda}{1 - q^* - \Delta q}. \tag{7}$$

We introduce the following notation:

$$l_1 = \frac{q^* - \Delta q}{1 - q^* + \Delta q}; \quad l_2 = \frac{q^* + \Delta q}{1 - q^* - \Delta q}; \quad \mu_н = \frac{\lambda \cdot q^*}{1 - q^*}. \quad (8)$$

Otherwise, inequalities (8) can be written in a relatively shortened form, for example: $l_1 < (\mu/\lambda) < l_2$ on their basis, it is convenient to obtain a set of admissible values for the control of the information security level of the parameter **μ**. This set is represented in figure 3 and from it follows the following: the increase in the intensity **λ** of the information attacks of a potential adversary on some distributed information system under consideration should be reflected in the growth of the corresponding intensity of control and restoration of the information security systems of the system **μ**.

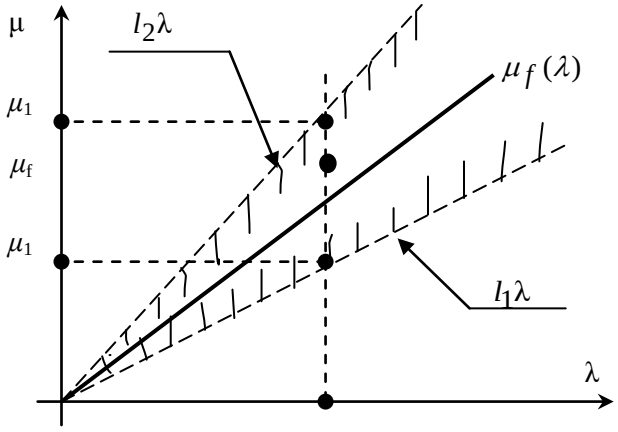

Figure 3. Set of admissible values for the control parameter of the information security level **μ**.

Summarize the above in the form of a sequential algorithm for managing the information security of the system and in which we will include the following steps:

1) systematic collection, accumulation and processing of data on information attacks on the system, finding a value λ_f that should characterize the actual intensity of attacks on the system, while finding the value λ_f should occur over the period of system operation time;

2) determination of values μ_1 и μ_2 and intensity **μ** of control and restoration of information security systems of the system that correspond to the boundary conditions for the solution of the problem in accordance with formulas (7) and (8);

3) the implementation by the chief administrator of information security (the decision maker) is a sequential choice of value $\mu_ф \in (\mu_1, \mu_2)$, while the DM should be guided by the capabilities of the system's personnel and the available means of ensuring information security;

4) finding a sequence $\theta_1, \theta_2, \theta_3, \ldots$ of temporary control points for unauthorized access to the system, as well as the accompanying restoration of possible damage, using the formula:

$$\theta_r = -\frac{1}{\mu_ф} \ln \xi_r, \quad r = 1,2,3\ldots,$$

where ξ_r is a random number uniformly distributed in the interval (0;1).

At the final stage of the proposed methodology, it is proposed to adhere to the principle for the protection of information, which is based on some stochastics [7-11]. We use for this purpose the distribution function of the random duration of the time interval **T** between two neighboring checks and the subsequent possible restoration of the system's information security:

$$F(t) = P\{T < t\} = 1 - e^{-\mu t}$$

and also we will use the following condition:

$$F(\theta_r) = \xi_r, r = 1,2,\ldots$$

to form a set of values $\theta_1,\theta_2,...$, which due to this will be distributed according to the exponential law with a given distribution parameter **μ**.

In our opinion, a random strategy for monitoring and restoring the actual level of information security of the system is more effective than such deterministic strategies as periodic diagnostics and restoration of information security tools; control and restoration of information security means by alternating changes of information security administrators of the system; carrying out of complex diagnostics at each change of administrators of information safety.

The most obvious drawback is that a potential enemy, knowing their time parameters, can organize information attacks in those intervals of time in which a complete or partial verification of the information security of the system will be conducted.

Note that in order to simplify the work of the decision maker in step 3) when choosing a value $\mu_f \in (\mu_1,\mu_2)$, it is possible to use the results of solving the following optimization problem:

$$p_1^*(\mu) = \frac{\lambda_\phi}{\lambda_\phi + \mu} \to \min_{\mu\in(\mu_1,\mu_2)},$$
$$C(\mu) = c\mu \to \min_{\mu\in(\mu_1,\mu_2)}. \quad (9)$$

In problem (9), the first criterion is designed to ensure the preservation of the equilibrium position of the system under consideration in the information attacks of a potential adversary.

The physical meaning of the value p_1^* can be extracted as follows, namely: the value p_1^* determines the average percentage of attacks missed by the means of protecting the information of the system from the potentially carried out by the enemy.

Note that in the meaning of the parameter ***c***, which is used in the second criterion of this problem (9), the average cost of checking and restoring the system is invested with a single violation of the information security state of the system. In this case, the function $C(\mu)$ should be interpreted as a characteristic of the unit cost of inspections and regulatory measures to restore the system, in the case of a given intensity of attacks on it.

4. An example of an approach to providing information security management process of an information system

As an example, consider some process of managing the information security of a mobile distributed control system. The characteristic features of these systems are that the time of their functioning is usually limited by a finite interval of time $[t_0,t_k]$, and also by some area of their functioning [10-12]. They are also subject to systematic information attacks, the nature of which can be described using model (1) - (4), where $t \in [t_0,t_k]$.

Let us investigate the nature of the function $p_0(t)$, formula (5), on the time interval $[t_0,t_k]$ under the following initial conditions: $p_0(t_0) = p_{00}$ the admissibility of the level of information security of the system in the interval $[q^* \pm \Delta q]$.

It follows from relation (5) that:

$$p_{00} < \frac{\mu}{\lambda + \mu}$$

$p_0(t)$ increases on the interval $[t_0,t_k]$. Let the system make a reference to the nominal control action, which is given by the following expression:

$$\mu_f = \frac{\lambda q^*}{1 - q^*}.$$

Then

$\frac{\mu_f}{\lambda+\mu_f} = q^*$; $\lambda + \mu_f = \frac{\lambda}{1-q^*}$.

As a result, we get:

$$p_0(t) = q^* + \left(p_{00} - q^*\right) e^{-\frac{\lambda\cdot(t-t_0)}{1-q^*}}, \; t \in [t_0, t_k]. \quad (10)$$

We note that for $q^* < p_{00} < q^* + \Delta q$ function (10) decreases. If the inequality $q^* - \Delta q < p_{00} < q^*$ is satisfied, then the function $p_0(t)$ will increase with increment of its argument. In the event $p_{00} = q^*$ that we get that $p_0(t) \equiv q^*$.

The behavior of the function $p_0(t)$ on the interval $[t_0, t_k]$ for various values $p_{00} \in [q^* \pm \Delta q]$ is clearly shown in figure 4.

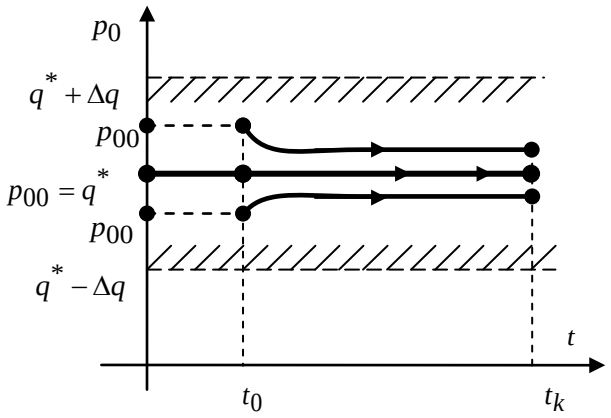

Figure 4. The behavior of the function $p_0(t)$ on the interval $[t_0, t_k]$ for various values $p_{00} \in [q^* \pm \Delta q]$.

So, if the norms $\| x(t_0) \|$ and $\| x(t) \|$ are defined as follows: $| p_{00} - q^* | \le \Delta q$ and $| p_0(t) - q^* | < \Delta q$ then the completely defined system (1) - (4) will be technically stable in the described sense on the time interval $[t_0, t_k]$.

The value of the function $p_0(t)$ at the instant of time $t = t_k$ is determined directly using the formula (10) as an expression of the form:

$$p_0(t_k) = q^* + (p_{00} - q^*) e^{-\frac{\lambda\cdot(t_k - t_0)}{1-q^*}}$$

Now consider the case under which $p_{00} \le q^* - \Delta q$. There will be some time interval $[t_0, t_1]$ in which the information security level indicator of the system $p_0(t)$ will not satisfy the level specified for it $[q^* \pm \Delta q]$, is shown in figure 5.

Then, in this case, the information security management of the system will consist in finding the value of **μ**, which would ensure the minimum length of the interval $[t_0, t_1]$, that is, would approach the level of information security to the value $(q^* + \Delta q)$ as quickly as possible. But it also requires that the average cost of measures to ensure the information security of the system would be as close as possible to the minimum, which can be achieved by using the following integral criterion:

$$W_1(\mu) = \int_{t_0}^{t_k} \left[(q^* + \Delta q) - p_0(t) \right] dt \to \min_{\mu \in (\mu_1, \mu_2)}. \tag{11}$$

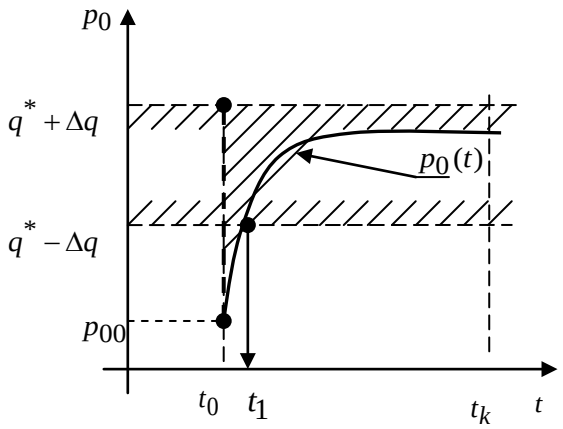

Figure 5. The level of information security of the system does not meet the requirements.

The physical meaning of criterion (11) corresponds to the area of the shaded area, which is shown in figure 5.

The criterion of cost optimization when choosing the actual value of **μ** will be written in the following form:

$$W_2(\mu) = c(t_k - t_0)\mu \to \min_{\mu \in (\mu_1, \mu_2)}. \tag{12}$$

Criterion (12) adequately reflects the average cost of diagnostics and restoring information security of the system on the interval of its operation $[t_0, t_k]$. We note that criterion (12) increases with increasing value of the argument **μ**.

The optimization problem (11), (12) can be solved using a formalism based on the use of a simple linear convolution:

$$L(\mu, \alpha) = \alpha W_1(\mu) + (1 - \alpha) W_2(\mu) \to \min_{\mu \in (\mu_1, \mu_2)},$$

where $\alpha \in (0,1)$.

Since the functions $p_0(t)$ and $W_1(\mu)$ do not correspond to the linearity conditions, the problem (11), (12) must be solved with the help of the corresponding special numerical methods.

Among the complexities of solving the problem in hand, we can note the procedure for determining the boundaries of the interval (α_1, α_2), which is used to enumerate the values of the convolution parameter **α** and, at which the required parameter $\mu \in (\mu_1, \mu_2)$.

Suppose that the decision maker has chosen a value $\mu^* \in (\mu(\alpha_1), \mu(\alpha_2))$. Based on this, a control point is determined t_1 (see figure 5), before the transition from which the system, from the moment of time t_0, the specified level of information security of the system is not reached.

$$t_1 = \arg\{ p_0(t, \lambda_f, \mu^*) = q^* - \Delta q \}. \tag{13}$$

To find the probability $P(t_0, t_1)$ that information attacks will take place over a distributed system over time $[t_0, t_1]$, consider the connection graph of the system states, which is shown in figure 6.

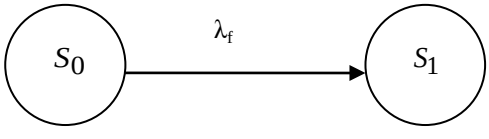

Figure 6. The graph of the connection of states of the system.

The graph in figure 6 corresponds to the following model:

$\dot{p}_0 = -\lambda_f p_0$, $p_0(t_0) = p_{00}$.

Solving the Cauchy problem corresponding to this model, we obtain the following solution:

$$p_0(t) = p_{00} e^{-\lambda_f (t - t_0)};$$
$$P(t_0, t_1) = p_{00} e^{-\lambda_f (t_1 - t_0)}; \quad (14)$$

where the control point t_1 is determined from the expression (13).

As a recommendation, it can be noted that the indicators (13), (14) can be used to select additional routine maintenance of information security on the time interval $[t_0, t_1]$.

5. Conclusions

In this article, in our opinion, a model of stability analysis of a distributed information system, worthy of attention in the sense of sustainable provision of its information security by some means of protecting information, was presented.

This model of analysis is most applicable for systems that are distributed in space, contain various elements and modules, both software and hardware, capable of changing their position in space.

The proposed method for constructing and analyzing the area of functional security of a distributed information system under the influence of enemy information attacks has a broad focus of its application in the practice of operating.

6. References

[1] Mokshin, V.V. Recognition of vehicles based on heuristic data and machine learning / V.V. Mokshin, I.R. Sayfudinov, A.P. Kirpichnikov, L.M. Sharnin // Bulletin of Kazan Technological University. – 2016. – Vol. 19(5). – P. 130-137. (in Russian).

[2] Mokshin, V.V. Definition of vehicles on road sections by the Haar classifier and the LPB with Adaboost and road markings / V.V. Mokshin, A.P. Kirpichnikov, I.M. Yakimov, I.R. Sayfudinov // Bulletin of Kazan Technological University. – 2016. – Vol. 19(18). – P. 148-155. (in Russian).

[3] Mokshin, V.V. Tracking objects in the video stream by significant features based on particle filtering / V.V. Mokshin, A.P. Kirpichnikov, L.M. Sharnin // Bulletin of Kazan Technological University. – 2013. – Vol. 16(18). – P. 297-303. (in Russian).

[4] Yakimov, I.M. Modeling of complex systems in the imitation environment. AnyLogic / IM. Yakimov, A.P. Kirpichnikov, V.V. Mokshin // Bulletin of Kazan Technological University. – 2014. – Vol. 17(13). – P. 352-357. (in Russian).

[5] Tutubalin, P.I. The Evaluation of the cryptographic strength of asymmetric encryption algorithms / P.I. Tutubalin, V.V. Mokshin // Second Russia and Pacific Conference on Computer Technology and Applications (RPC), 25-29 Sept. 2017, Vladivostok, Russia. – 2017. – P. 180-183. DOI: 10.1109/RPC.2017.8168094.

[6] Yakimov, I. The comparison of structured modeling and simulation modeling of queueing systems / I. Yakimov, A. Kirpichnikov, V. Mokshin, Z. Yakhina, R. Gainullin // Communications in Computer and Information Science (CCIS). – 2017. – Vol. 800. DOI: 10.1007/978-3-319-68069-9_21.

[7] Moiseev, V.S. A probabilistic dynamic model for the functioning of active protection software for mobile distributed ACS / V.S. Moiseyev, P.I. Tutubalin // Information technology. – 2013. – Vol. 6. – P. 37-42. (in Russian).

[8] Tutubalin, P.I. Optimization of selective control of the integrity of information systems / P.I. Tutubalin // Information and Security. – 2012. – Vol. 15(2). – P. 257-260. (in Russian).

[9] Moiseev, V.S. General model of a large-scale mobile distributed ACS / V.S. Moiseyev, P.I. Tutubalin // Nonlinear World. – 2011. – Vol. 9(8). – P. 497-499. (in Russian).

[10] Tutubalin, P.I. Application of models and methods of stochastic matrix games for ensuring information security in mobile distributed automated control systems / P.I. Tutubalin // Nonlinear World. – 2011. – Vol. 9(8). – P. 535-538. (in Russian).
[11] Tutubalin, P.I. The main tasks of the applied theory of information security ASU / P.I. Tutubalin // Scientific and Technical Herald of Information Technologies, Mechanics and Optics. – 2007. – Vol. 39. – P. 63-72. (in Russian).
[12] Moiseev, V.S. A two-criteria game-theoretic model with a given ordering of mixed strategies / V.S. Moiseyev, A.N. Kozar, P.I. Tutubalin, K.V. Bormotov // Bulletin of the Kazan State Technical University A.N. Tupolev. – 2005. – Vol. 1. – P. 40-45. (in Russian).