The approach to concealing data in a distributed system

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

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

Abstract. The article provides a brief description of the methods and tools used to ensure the protection of information in some organization, that is, hiding confidential data. A self-regulating scheme of the operation of the information protection system and a stochastic method providing an increase in the level of information security of the system under operating conditions that provide for the random nature of the environmental impact on the system under consideration are proposed.

Keywords: method, information protection, confidential data, self-regulating system, random impact.

1. Introduction

As practice shows, the growth of volumes of information that circulates in modern society continues. This situation can be explained in many respects by the fact that systems continue to be available to organizations of various sizes and to the mass consumer. At the same time, the issue of ensuring the information security of certain systems is still on the agenda, on the contrary, the issues of ensuring information security and information protection are becoming increasingly important with the growing accessibility of the Internet and the movement of various outlines of information that were not previously posted on the Internet to the Internet.

Various open sources confirm what has been said, I would like to mention only those of them, which, in our opinion, most clearly tell about this. For example, in the work related to the processing of graphic and video information [1-3], it is noted that ever larger volumes of information become available through the means of certain computing public resources, and one can also speak of works highlighting the features of modeling complex systems [4,5], in which the interference of outside parties in this process can significantly reduce the reliability of the results of this process, which is extremely undesirable.

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 you pay attention to a number of the following papers [7-12], in which the basic principles, approaches and methods are sufficiently thoroughly expounded, allowing 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 development and on the basis of the data contained in [7-12], we will propose an approach to data concealment, which is advisable to use in medium and large organizations, services and departments, but this approach can also be used in arbitrary distributed information systems.

Today, certain organizations, services and agencies are interested in reliable concealment of their confidential data (commercial secrets, data for official use, data constituting state secrets). In connection with this, the protection of such data is an actual task included in the list of tasks for the functioning of any modern distributed information system.

2. Well-established approaches to information security

Current practice shows that among the main approaches that are used and proposed by companies engaged in the development and deployment of distributed information systems (including mobile) in the market for the protection of information of a different nature, two main approaches are used to protect information (ensuring its safe circulation in circuits organization):

organization of a virtual private network using technologies based on the use of VPN;

this or that application of means of data encryption and decryption, that is, various cryptographic algorithms.

In practice, usually stop at one of the above solutions, but most often this solution, being cheaper and not optimal from the point of view of the received level of information security of the system.

3. Current trends in the field of information technology

Let's consider modern tendencies of development of information technologies in the average and large organizations of Russia, which can be characterized by the following important distinctive features:

1) Sufficiently rapid and significant expansion of the scope of application of information technology with simultaneous growth in the number of universal functions performed by systems that provide appropriate computing processes;

2) A significant need to maintain the existing technical and technological solutions in the design and implementation of new automated information processing and management systems, as well as ensuring compatibility between them in various operational aspects;

3) The rather high complexity of not only electronic equipment and system application software, but also the logical organization (structures, individual components and interrelations between them) of data processing systems and applications.

It can be added that at the same time there are growing trends in the problem of ensuring the security of subjects of information relationships, protecting their legitimate interests by using information and control systems, information stored and processed in them.

In addition and in addition to what has been said, it should be noted that in the context of constant monitoring and solving the problem of securing information in the automated systems of certain large and medium-sized organizations, it is necessary to correctly solve the issues of protecting personal data in accordance with the current Federal Law "On Personal Data", in which sets out guidelines for carrying out activities related to the protection of personal data.

Based on the results of the work related to the detailed analysis of the implementation and operation of various mobile distributed automated information processing and management systems in Russia, it is possible to single out the following main tasks that need to be addressed when creating secure access to information resources of medium and large organizations in Russia:

1) Creation of conditions for provision of protected access of employees of the organization to resources of the united data bank, up to the federal level.

2) Organization of selective and adaptive access to existing and required application software packages for employees of the organization (Microsoft Office, corporate portal, standard programs, etc.).

3) Formation of conditions for ensuring scalability of the organization's infrastructure and its high-quality service.

4) Creation of conditions for ensuring the necessary level of reliability of the system, as well as ensuring the possibility of distributing and redistributing the load on it.

5) The solution obtained during the implementation of these tasks should be modern, convenient, technological and cost-effective.

6) Also important is the need to provide long-term support for the decision of the manufacturer.

To date, the de facto standard is the development, implementation and use in medium and large organizations, within corporate needs, of tablets - so-called secure access terminals. These, in fact, mobile access terminals are designed to provide and facilitate the circulation of employees of medium and large organizations of Russia to the information resources of single information and telecommunication systems, as well as to integrated databases.

So, for example, employees of various divisions of law-enforcement bodies and law-enforcement bodies have the opportunity, through protected departmental tablets, to obtain separated access to data stored in an integrated federal-level data bank.

It should be noted that the organization of this access is strictly in accordance with modern requirements of regulatory documents in the field of information security and information protection.

If we briefly characterize the tablet of protected terminal access of the main information and analytical center of the Ministry of Internal Affairs of Russia, then this tablet, made in a protected case, is an autonomous field information system that operates on the principle of client-server architecture.

As part of this system, the following subsystems and modules can be distinguished:

1) server subsystem located within the controlled area of the main information and analytical center of the Ministry of Internal Affairs of Russia, and includes in its composition:

• transparent terminal access subsystem;

• Certified SecretNet security servers and the Active Directory domain controller.

• Fault-tolerant firewalling subsystem, mainly based on the VipNET component base;

• Fault-tolerant subsystem of cryptographic protection, based on the use of VipNET tools;

• an extended subsystem of information security monitoring and control implemented by means of MaxPatrol software hardware;

• integrated subsystem of content filtering of the network, which is implemented with the help of specialized software Aladdin eSafe;

• an autonomous subsystem of anti-virus protection.

2) the employee's automated workplace in the information center of the main information and analytical center of the Ministry of Internal Affairs of Russia;

3) terminal stations of employees of the main information and analytical center of the Ministry of Internal Affairs of Russia.

Let's note one more aspect connected with work of average and large corporate information systems, namely application of the best world practices on support of information services. Here it should be noted the experience of ITIL - the library of the information technology infrastructure.

In the practice of medium and large mobile distributed automated information processing and control systems, the experience presented in ITIL will be very useful.

Here are a few examples of information subsystems of the Ministry of Internal Affairs, which provide for work with information that should be hidden, unauthorized access to which should be prohibited.

Next, a number of complexes are listed that can be used by the Ministry of Internal Affairs personnel to conduct various special operations.

So, depending on the objectives pursued, the following complexes can be used:

• access of mobile users to various information resources can be provided with the help of mobile access subsystem "Radius";

• police officers for operatively protected access to various data banks can be equipped with hardware and software systems "Bars", which are devices for individual and personal access to data;

• special requirements are imposed on those information subsystems that are applied during the liquidation of the consequences of emergencies and the prevention of terrorist actions; in these conditions it is proposed to use the hardware-software complexes "ZUBR"; Also these complexes can be applied in the organization of training of the Ministry of Internal Affairs employees; and for information support of various outreach activities;

• the next extremely important aspect of information processing is the provision of processing of information containing information constituting state secrets, for this purpose special hardware and software systems "Pantsir" can serve;

• the collection and storage of data in large organizations provides for the presence of software packages similar in their characteristics to the program complex "Integrated Data Bank of the New Generation". This complex is designed to ensure the activities of territorial and regional divisions of the internal affairs bodies, in fact, it can perform the functions of a regional or even federal automated information system.

4. A stochastic approach to increasing cryptographic stability

In order to further increase the level of information security of the listed information protection and information security tools, stochastic methods for ensuring information security and information protection can be implemented in them.

In our opinion, it was correct and, ultimately, more profitable to implement some self-regulatory method of information protection, which would mean, in practice, depending on the operating conditions of the information system, the use of one of the two methods noted above. At the same time, during the operation of some information system, there should exist the possibility of an alternation of protection methods based on a certain stochastic one on another.

It should also be noted that the process of self-regulation associated with the choice of a specific method of protecting information at one time or another should be built with the involvement of stochastic laws.

A particular version of the self-regulatory method associated with using at some point in time either VPN technology or data encryption / decryption can be considered. Generally speaking, this has a fairly simple and reliable basis, namely that VPN technology, in the end, also relies on the use of certain cryptographic algorithms, and correspondingly, the corresponding encryption / decryption schemes.

At the same time, it should be noted that the number of methods between which a choice can be made in the functioning of the system can be significantly more than two, then this will be demonstrated.

With this in mind, in our opinion, a very rational approach can stop at an alternating stochastically-oriented use for encrypting and decrypting data circulated and stored in the information system, various cryptographic algorithms and encryption schemes-decryption.

Let us explain what has been said. The proposed approach takes place in connection with the fact that the selection of key cryptographic information of different implementations of even one cryptographic algorithm is substantially different. At the same time, the success of the cryptanalyst's activity largely depends on the chosen method of cryptanalysis of data, which he applies directly based on the assumption of some method of data encryption. Accordingly, any increase in uncertainty in the choice of the method of cryptanalysis, leads to the fact that the level of information security of the system and its protection from unauthorized influences on its resources increase. The noted property of the information system is extremely desirable, it should be aimed at the developers of such systems, as well as those involved in their direct implementation.

Let's consider the practical scheme of application of the stochastic approach for increase of a cryptographic firmness of the data transferred and stored in an information system.

The idea of the scheme used in this approach is that additional uncertainty is introduced into the system about certain methods of its organization, this uncertainty is created due to the fact that certain information protection means are included or excluded from the system, while these Inclusion or exclusion from work occurs in a random, stochastic manner.

Let us consider in more detail what has been said. The implementation of this idea is based on the theory-game model, which is given in [10].

Let the process of encryption, transmission and decryption of data in the information system and their interception and cryptanalysis by the enemy be considered as a game of two conflicting sides **A** and **B**. Let us assume that **N** implementations of cryptographic algorithms are involved and used in this process.

In this case, in principle, two situations can be singled out:

a) the availability of an opportunity - the use of cryptographic algorithms by party **A**, which is reliably known to party **B**;

b) a list of cryptographic algorithms used by party **A** and they, that is, the principles of their implementation, are hidden from side **B**.

Next, the situation marked by a) is considered, the situation corresponding to the letter b) is certainly unfavorable for side **B**.

We denote by $\boldsymbol{A_i}$ and $\boldsymbol{B_j}$ the strategies of the parties opposing the conflict situation, which consists in the fact that side **A** uses the ***i***-th method of data encryption in the transmitted messages, and side **B** makes attempts to cryptanalysis of intercepted messages using the ***j***-th method, $i \in \overline{1,N}$, $j \in \overline{1,M}$.

We will consider strategies $\boldsymbol{A_i}$ and $\boldsymbol{B_j}$ as mixed, described by probabilities $\boldsymbol{p_i}$ and $\boldsymbol{q_j}$ of their use by parties **A** and **B**. These probabilities must satisfy the following conditions:

$$\sum_{i=1}^{N} p_i = 1, \ \sum_{j=1}^{M} q_j = 1 \tag{1}$$

The pay matrix of the game is denoted as:

$$\Gamma = [\gamma_{ij}]_{N\times M} \tag{2}$$

elements of which have the sense of losing side **A**, provided that it applies strategy $\boldsymbol{A_i}$, and party **B** - strategy $\boldsymbol{B_j}$.

We denote by $\boldsymbol{v}$ the game price describing the average loss of side **A** when using the set of probabilities $\boldsymbol{p_1}$, $\boldsymbol{p_2}$, ..., $\boldsymbol{p_N}$ as its mixed strategy of behavior. These probabilities are inherently reflective of the frequency of use of the corresponding pure strategies of party **A**.

The above probabilities can be determined taking into account the conditions (1) from the solution of the linear programming problem:

$$\mathrm{K}_1 = \nu \to \min \tag{3}$$

$$\sum_{i=1}^{N} p_i \gamma_{ij} \le \nu , \ j = \overline{1,M} . \tag{4}$$

$$\sum_{i=1}^{N} p_i = 1, \ 0 \le p_i \le 1 , \ i = \overline{1,N} . \tag{5}$$

Criterion (3) indicates that side **A** in this game aims to minimize its losses (loss) obtained during the conflict with side **B**.

5. Examples

5.1. Example 1

Let us consider an example of using the proposed method on the basis of data on the stability of cryptographic algorithms from [7-10]. It should be noted that in those cases when the cryptanalyst correctly selects the algorithm for hacking the key cryptographic information, then the resistance is determined on the basis of fast methods of selecting key cryptographic information, and if the analyst has chosen an incorrect cryptographic analysis algorithm, the speed of determining the key cryptographic information is found from the condition of use the method of full search, which is slower than in 10^{10} in comparison with the optimized methods of finding the key cryptographic information formations [12], with the increase in the length of key cryptographic information, the slowdown in the work of the full-scan method in comparison with optimized methods is substantially increased.

It should be noted that in the field conditions of the above-mentioned complexes, cryptanalysts may have at their disposal insignificant computational means for selecting key cryptographic information. Therefore, the choice of the correct algorithm for selecting key cryptographic information that takes into account the supposed implementation of the encryption-decryption method is a very significant factor for the cryptanalyst to accelerate the achievement of its goals, and therefore the stochastic approach to choosing concrete applied implementations of cryptographic algorithms is an important tool for ensuring and improving the level of information security all kinds of field complexes.

Taking into account the foregoing and stability estimates for the implementation of cryptographic algorithms from [11], we will compile a payment matrix for the game, which, by its elements, will mean the inverse resilience of a particular implementation of the cryptographic algorithm, provided the cryptanalyst used by the cryptanalyst against it selects key cryptographic information. Thus, the matrix of the form (2) in the conditions of the example takes the form:

$$\Gamma = \begin{bmatrix} 10^{-10} & 1 \\ 1 & 10^{-10} \end{bmatrix}$$

This matrix game in mixed strategies has, according to well-known works on game theory, the following solution:

$$\left(p_1^*; p_2^*\right) = (0{,}5; 0{,}5)$$

As it is not difficult to notice - the price of the game will be almost twice lower in comparison with the case of choosing one of the two pure strategies, that is, using a predetermined implementation of the cryptographic algorithm. This example demonstrates the expediency and effectiveness of applying the stochastic approach in the selection of key cryptographic information using both field and stationary information systems in the framework of activities, both internal affairs bodies and other departments and medium and large organizations.

To implement the procedure for determining (playing) the next cryptographic algorithm, which should be used at the moment in the information system, the methodology described in [11,12] can be applied.

5.2. Example 2

As in any other distributed information system, there is a significant number of communication lines in the mobile distributed control system, which in each specific case of the system implementation can be represented as wired channels (for example, twisted pair, fiber) or wireless (radio channels, Wi- Fi). In the real world, a mobile distributed control system can be subject to accidental and deliberate actions from the side of the possibly enemy. These actions, including, may adversely affect the operation of its communication channels. At the same time, it should be noted that the likely enemy can conduct his attacks not only from static ground objects, but also from mobile platforms, the position and coordinates of which can vary significantly over time. The latter statement makes it difficult to identify the dislocation of a credible adversary and to eliminate its means of influencing the communication channels of a mobile distributed control system, and also encourages the use of effective methods and means of protecting communication channels of existing mobile distributed control systems for various purposes. Such methods and means can include various noise-resistant codes, including, in particular, majorization principles, as well as communication systems characterized by adaptation using pseudo-random adjustment of the operating frequency and the use of broadband signals.

In addition to raising the level of information security for particularly important military, high-tech and special systems that can be classified as a class of mobile distributed control systems with an increased level of security, it can be achieved just by applying the method of stochastic change of information protection means.

For example, in some mobile distributed control systems, means of protection of communication channels are used within the framework of the stochastic approach, which will be conditionally designated as the following list of pure strategies:

A_1 - pseudo-random adjustment of the working frequency of the communication channel;

A_2 - data transmission by means of broadband signals.

In turn, it is known that from the side of a possible adversary, in order to distort the transmitted data of a mobile distributed control system, the following means of attack can be used, which by analogy is designated in the form of a list of his pure strategies:

B₁ - jamming station;

B₂ - station interference in part of the band;

B₃ - station of tracking jamming.

Following [13], the list of introduced pure strategies and formula (2), we construct a payment matrix for the game, describing the conflict between the protection system of the communication channels of the mobile distributed control system and the enemy, which will take the following form:

$$\Gamma = \begin{array}{c|ccc} & B_1 & B_2 & B_3 \\ \hline A_1 & 1{,}5\cdot 10^{-3} & 1{,}5\cdot 10^{-2} & 1{,}7\cdot 10^{-2} \\ A_2 & 2{,}8\cdot 10^{-2} & 2{,}8\cdot 10^{-3} & 10^{-10} \end{array}$$

where each element determines the probability of interference in the communication channels of the mobile distributed control system under the action of the enemy in the ***j***-th strategy and the choice to protect the i-th strategy.

It is reliably known from [13] that the implementation of strategy **A₁** is twice more energy-consuming compared to strategy **A₂**, then along with criterion (3) determining the price of the game, one can consider the criterion of energy costs, which will be written in the following form:

$$R = p_1 + 2p_2 \to \min\,, \qquad (6)$$

where the probabilities $\boldsymbol{p_1}$ and $\boldsymbol{p_2}$ determine the mixed behavior strategies **A₁** and **A₂**.

Limitations (4) and (5) under the conditions of the example will take the form:

$$\begin{aligned} &1{,}5\cdot 10^{-3} p_1 + 2{,}8\cdot 10^{-2} p_2 \le \nu, \\ &1{,}5\cdot 10^{-2} p_1 + 2{,}8\cdot 10^{-3} p_2 \le \nu, \qquad (7) \\ &1{,}7\cdot 10^{-2} p_1 + 10^{-10} p_2 \le \nu. \end{aligned}$$

$$p_1 + p_2 = 1\,,\ 0 \le p_1 \le 1\,,\ 0 \le p_2 \le 1\,. \qquad (8)$$

To solve the formulated linear programming problem, we apply the linear convolution of the criteria taking into account expressions (3) and (6), which will take the following form:

$$L(\alpha, p_1, p_2,) = \alpha\nu + (1-\alpha)(p_1 + p_2) \to \min\,. \qquad (9)$$

During the computational experiment to solve the problem described by the mathematical model (9), (7), (8), with the change in the convolution parameter, the following Pareto optimal solutions were obtained, which were summarized in table 1.

Table 1. Pareto optimal solutions of the model (9), (7), (8), obtained with the change step of the convolution parameter $\Delta\alpha = 0{,}1$.

Number	α	p_1	p_2	v
1	0	0,153	0,847	0,0026
2	0,1 - 1	1	0	0,017

If option # 1 is chosen as the solution from Table 1, the application of the means of protection of the communication channels of some mobile distributed control system can be played using and based on the Monte Carlo method for a specified time of the system.

5.3. Example 3

To date, the means of attacking information systems are quite diverse. Of particular interest are radio viruses, which can be introduced via wireless networks into the work of distributed information structures. It is natural to assume that radio viruses can pose a significant danger to the operation of all possible mobile distributed control systems, since in their overwhelming majority of cases communications facilities using radio channels are included.

Let's consider a completely possible conflict in practice between the information security system of the communication channels of a mobile distributed automated control system, which includes a set of four antiviruses, and a probable enemy, which has three radio viruses in service.

Initially, it is known that for each antivirus there are defined the so-called integral characteristics that determine the necessary computational resources for its operation, which are given in table 2.

Table 2. Characteristics of the costs of computing resources for the normal operation of antivirus software.

Antivirus number	Resource capacity
1	10
2	20
3	15
4	8

We will assume that the choice of the antivirus is carried out within the framework of the stochastic approach, that is, the choice of the antivirus with the corresponding number determines the strategy for protecting the mobile distributed control system, and the application of the radio virus, with its defining number, corresponds to the opponent's strategy.

Thus, given the above, let the payment matrix of the game take the following hypothetical form:

$$\Gamma = [\gamma_{ij}]_{4\times 3} = \begin{array}{c} \\ A_1 \\ A_2 \\ A_3 \\ A_4 \end{array} \begin{array}{c} \begin{array}{ccc} B_1 & B_2 & B_3 \end{array} \\ \begin{bmatrix} 23 & 34 & 45 \\ 12 & 56 & 42 \\ 18 & 11 & 46 \\ 68 & 20 & 21 \end{bmatrix} \end{array},$$

where the values γ_{ij} determine the conventional damage received by the mobile distributed control system under the action of the enemy in the ***j***-th strategy and the choice to protect the ***i***-th strategy.

By analogy with the second example, we write down the mathematical game model of the conflict, represented by a series of the following expressions:

1) The criterion of computational resources costs for the use of one or another anitvirus:

$$R = 10p_1 + 20p_2 + 15p_3 + 8p_4 \to \min \tag{10}$$

2) Game Restriction System:

$$\begin{aligned} &23p_1 + 12p_2 + 18p_3 + 68p_4 \le v, \\ &34p_1 + 56p_2 + 11p_3 + 20p_3 \le v, \\ &45p_1 + 42p_2 + 46p_3 + 21p_3 \le v, \end{aligned} \tag{11}$$

$$p_1 + p_2 + p_3 + p_4 = 1,\ 0 \le p_i \le 1,\ i = \overline{1{,}4}\,. \tag{12}$$

3) The final linear convolution criteria - the price of the game and the costs of computing resources necessary for the normal operation of the selected antivirus software:

$$L(\alpha, p_1, p_2, p_3, p_4) = \alpha v + (1-\alpha)(10p_1 + 20p_2 + 15p_3 + 8p_4) \to \min \tag{13}$$

The optimal Pareto solution of the problem described by the mathematical model (13), (10) - (12), with the change step of the convolution parameter is summarized in table 3.

Table 3. Pareto optimal solutions of the model (13), (10)-(12), obtained with the change step of the convolution parameter $\Delta\alpha = 0{,}1$.

Number	α	p_1	p_2	p_3	p_4
1	0	0	0	0	1
2	0,1 – 0,9	0,68	0	0	0,32
3	1	0	0,45	0,17	0,36

As a solution, option No. 2 or No. 3 may be chosen, but it is clear that in the second variant two protection measures will be used, and in the third three.

6. Conclusions

In this article, in our opinion, the approach worthy of attention to the concealment of data circulating and stored in distributed systems was presented.

The most interesting and relevant this approach is for systems that are distributed in space, contain elements and modules, both software and hardware, which can change their position and role occupied in the system.

In conclusion, it should also be noted that a method based on stochastic use of protection strategies can be applied not only, for example, in mobile distributed control systems, but also other widely used information systems.

We also believe that the proposed method has the potential for further development, for example, the number of defense system strategies can be significantly increased through their pairwise or multiple combination. At the same time, criteria that determine the quality of selected combinations from the point of view of their effectiveness in providing information security of the protected information system can be additionally introduced into consideration.

7. 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 / I.M. 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).

[13] Gremyachensky, S.S. Introduction to the game-theoretic analysis of radio-electronic conflict of radio communication systems with radio-suppression means and some estimates of the results of the conflict / S.S. Gremyachensky, V.I. Nikolaev. – Voronezh: VNIIS, 1995. – 46 p. (in Russian).