Opportunities to study the characteristics of information systems and manage them using modern technologies

Igor V. Goncharov
Candidate of Technical Sciences, Associate Professor
National Research University of Electronic Technology
Shokin Square, 1, Zelenograd, Moscow, Russia, 124498
goncharov@infobez.org

Nikita I. Goncharov
National Research University of Electronic Technology
Shokin Square, 1, Zelenograd, Moscow, Russia, 124498
st@infobez.org

Alexander V. Dushkin
Doctor of Technical Sciences, Associate Professor
National Research University of Electronic Technology
Shokin Square, 1, Zelenograd, Moscow, Russia, 124498
a_dushkin@mail.ru

Pavel A. Parinov
National Research University of Electronic Technology
Shokin Square, 1, Zelenograd, Moscow, Russia, 124498
pavelparinov03@gmail.com

Abstract: In the conditions of the modern functioning of information and computing systems, including as objects of informatization, the task of proper management and timely decision-making by the operator (network administrator) is urgent. In this paper, as part of expanding the capabilities of the adaptive response module, an approach to the analysis of the presentation and state of the information-computing system using neural networks and wavelet transforms with the aim of adaptive control of the corresponding characteristics is proposed.

Keywords: information computer system, neural network, wavelet transform, external influence, modeling, adaptive response

Introduction

It is first necessary to determine a typical model of conflict interaction between an information system and an intruder. We suggest a model based on hybrid automata formalism that is used to determine the ratios for approximate estimate of probability of security violation and the lower bound of probability of security violation in the IS. The model uses the most basic parameters such as mathematical expectation and variance for the duration of each of the discrete states of the IS and the intruder. The main features of hybrid automata and their application in simulating conflict interaction of systems were considered in the earlier works by the authors [1-5].

1 Simulating conflict interaction between information systems and intruders

Let us suppose that one of the parties (Party A) of the conflict is an information system (IS). The IS operates successfully, if it ensures the security of the information within itself in a set period of time $0 \le t \le T$. The IS itself is constantly in one of the states typical for its operation and functioning under normal conditions. The IS fails, if the security of the information within it is violated, at which point the system transfers to a corresponding critical state. The other party (Party B) of the conflict is an intruder system that aims to violate the security of the information within the IS and thus transfer the IS into the critical state within a set period of time. The intruder system succeeds, if it manages to reach this target. Party B fails, if it does not manage to violate the security of the information within the set period of time $0 \le t \le T$.

Fig. 1 presents two hybrid automata (HA) functioning simultaneously: automaton A and automaton B. For these automata the set of discrete variables $S^D = \{s_a, s_b\}$, which describe the most common states, is presented by two variables, each taking the values $s_a \in Q_A = \{L_A, D_A\}$, $s_b \in Q_B = \{L_B, D_B\}$. State L_A represents the functioning of A until the moment when the intruder takes advantage of the existing vulnerabilities, which results in security violation and transition of the IS to the critical state D_A ("failure" A). State L_B represents the functioning of B that aims to interfere with the operation of A, and lasts for a set period of time after which the intruder fails to breach the security of the information system ("failure" B) and transfers to the state D_B. Transition to D_A and D_B proceeds abruptly and is influenced by $attack\_B$ and $t \ge T$, leading to failure for A and B respectively.

To detail the operation of both parties of the conflict, it is necessary to consider the inner states of the set $L = \{L_A, L_B\}$ as embedded hybrid automata which we will refer to as hybrid automata of active elements (HA AE).

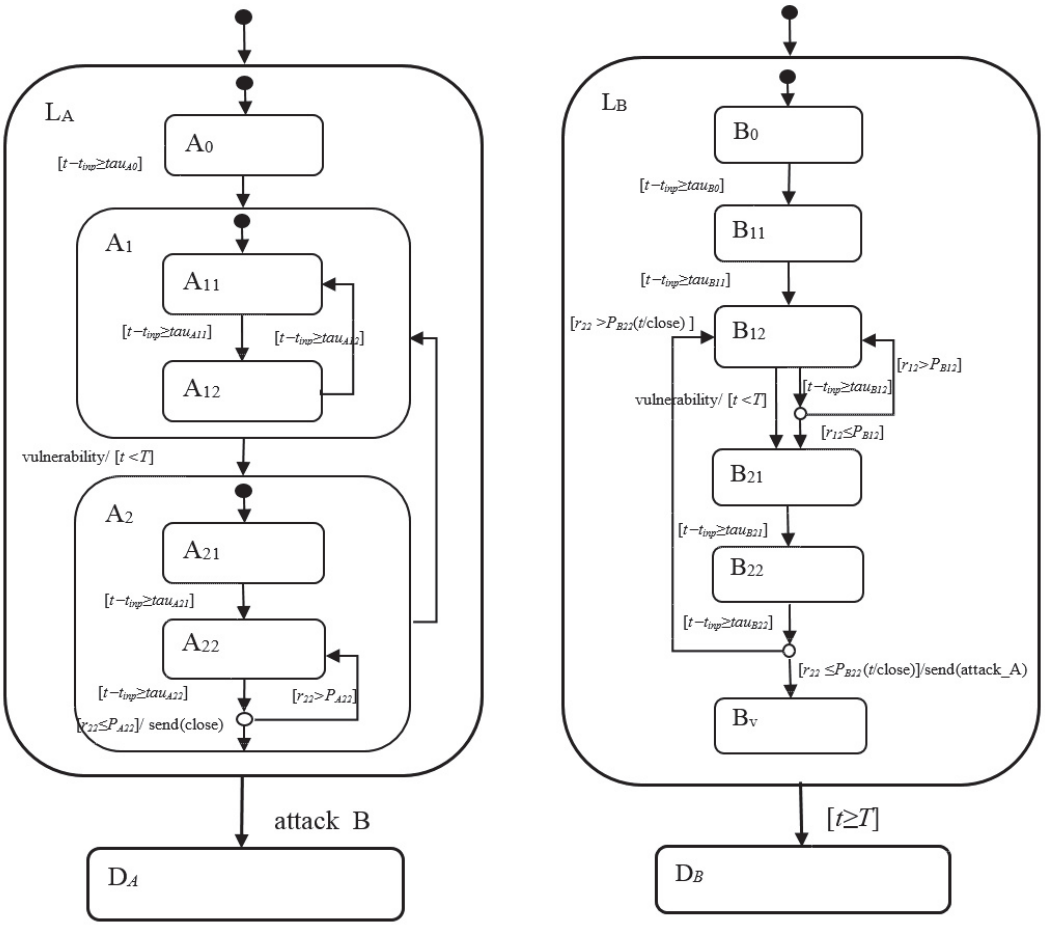

Figure 1 – A model of conflict interaction between the information system and the intruder based on hybrid automats

The subset of symbols $Q_{A0}^L = \{A_0\}$ consists of the symbol of the state that is responsible for getting system A into operation. The subset of symbols $Q_{A1}^L = \{A_{11}, A_{12}\}$ represents the system's operation under normal conditions. The symbols are embedded into general state A_1, which means that "system A is secure from all known vulnerabilities". The subset of symbols $Q_{A2}^L = \{A_{21}, A_{22}\}$ represents the functioning of the system after a new vulnerability was found or appeared. The symbols are embedded into general state A_2, which means that "system A is insecure from a known vulnerability". The transition from state A_1 to state A_2 is influenced by the event "vulnerability" under the condition that this vulnerability appears in the period of time $[t,T)$, set for conflict interaction between systems. To describe the way new vulnerabilities appear, we used a model of external random flow of events. Transition from state A_2 back to state A_1 is possible, if the

system manages to eliminate the vulnerability in A_2. For active elements of party B the following states and transitions should be introduced when modelling the events of a typical conflict. The subset of symbols $Q_{B0}^{L} = \{B_0\}$ consists of the symbol of the state that is responsible for getting system B into operation. The preparatory actions do not repeat. The subset of symbols $Q_{B1}^{L} = \{B_{11}, B_{12}\}$ represents the states of system B when it searches for and identifies the vulnerabilities, system A being in state A_1 (system A is secure from all known vulnerabilities). State B_{11} determines the functioning of the system aimed at gathering information about system A (analysis of the organisation principles, technical tools, and software, and rights and qualifications of the users and operating personnel). State B_{12} determines the way system B searches for vulnerabilities when system A operates under normal conditions. Probability P_{B12} is set by the operator of local behaviour as the probability of identification of a vulnerability when system A operates under normal conditions. It is time-independent. The model shown in Fig. 1 describes the main transition type as well as another type of transition from B_{12} into the following group of discrete states. The latter is determined by the event "vulnerability" (identification of a new vulnerability) happening in the period of time $[t, T)$. We assume that systems A and B receive the information about a new vulnerability at the same time. The subset of symbols $Q_{B2}^{L} = \{B_{21}, B_{22}\}$ represents the functioning of system B after a new vulnerability was detected. State B_{21} determines the actions performed to analyse the detected vulnerability and utilise it. The state is limited in time. State B_{22} activates the utilisation of the vulnerability in order to violate the security of system A. The subset of symbols $Q_{Bv}^{L} = \{B_v\}$ consists of the symbol of the state when the security of information in system A is successfully violated. The transition to the critical state is followed by the event attack_A, which transfers the HA of party A from state L_A into eigen state D_A. State B_v is absorbing for this model. Transition from state B_{22} back to state B_{12} is performed, if system B fails to utilise the detected vulnerability.

2 Assessing the probability of information security violation

Here we present the analytical relations obtained in the analysis of the probability of success of party B [1-5] in a situation when it does not receive any external information about new vulnerabilities.

Analytical relation based on Gaussian approximation for a random variable $\tau_{b,1}$:

$$P_{Bga}^{(1)} = \Pr(0 < \tau_{B,1} < T) = \int_0^T N(u, m_{B,1}, d_{b,1})du = \\ = F\left(\frac{T - m_{B,1}}{\sqrt{d_{B,1}}}\right) - F\left(\frac{-m_{B,1}}{\sqrt{d_{B,1}}}\right), \\ F(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} N(v, 0, 1)dv\,. \tag{1}$$

where $N(u, m, d)$ is the Gaussian probability density distribution with corresponding parameters.

To estimate the lower probability of security violation, Chebyshev's inequality can be used [1-5]. The estimate can also be specified using the Vysochanskij-Petunin inequality, assuming that the distribution density of composition $\tau_{b,1}$ is unimodal:

$$P_{Bvp} = \Pr\left[\tau_{B,1} < T\right] \geq \Pr\left[\left|\tau_{B,1} - m_{B,1}\right| < T - m_{B,1}\right] = \\ = \Pr\left[\left|\tau_{B,1} - m_{B,1}\right| < \frac{T - m_{B,1}}{\sqrt{d_{B,1}}}\sqrt{d_{B,1}}\right] \geq \\ \geq 1 - \frac{4}{9\rho^2} = 1 - \frac{4d_{B,1}}{9(T - m_{B,1})^2}, \quad \rho = \frac{T - m_{B,1}}{\sqrt{d_{B,1}}} \geq \sqrt{\frac{8}{3}} \tag{2}$$

It is, however, much more difficult to estimate the probability of success of system B, if within the set period of time it receives information about a new vulnerability. The authors obtained analytical relations for this estimate as well, introducing a number of assumptions and approximations, but these results are out of the scope of the present paper.

3 Results of the experiment

We examined the possibility of using the obtained analytical relations by means of various types of distributions for the duration of each of the systems' states. In a series of statistical experiments, including 1,000 tests each, we considered various combinations of distribution laws, their parameters, and the probability of returning and repeating the tests. The obtained results were summarised as the dependencies of the probability of success P on the relation $\rho o = (T - m_{B,1})^2 / d_{B,1}$. A few examples of such dependencies are shown in Figure 2.

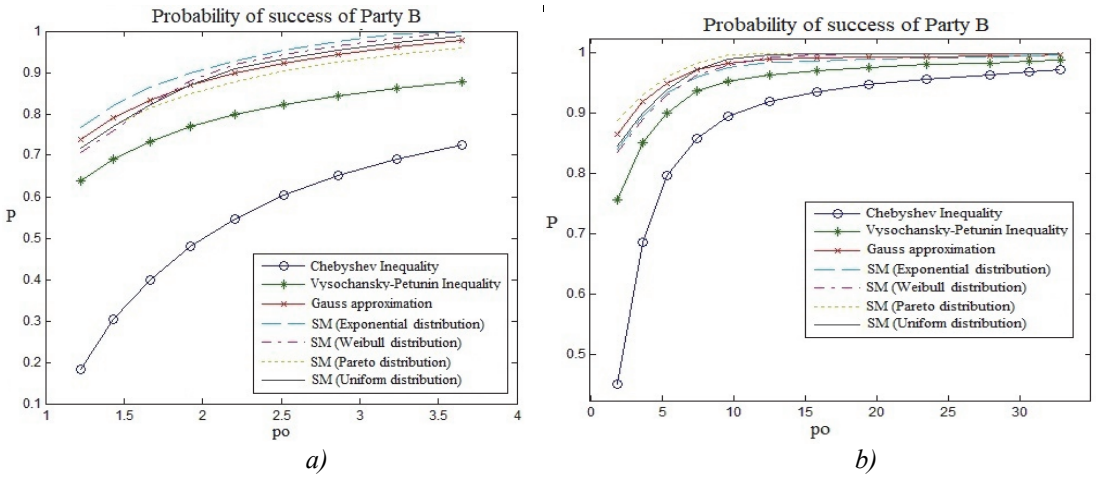

Figure 2 - Comparison of the obtained estimates with the results of simulation modelling

Fig. 2 demonstrates that using analytical relations based on Vysochanskij–Petunin inequality and Gaussian approximation allows for precise estimate of the lower probability and approximate estimates of probability of information security violation under the condition of ambiguity of probability density distribution within the duration of the respective states of the information system and the intruder system. Analytical relation based on Chebyshev's inequality yields rougher estimates. The precision of the analytical relations in each case is determined by preset parameters and the use of assumptions. Without specific assumptions, the margin of error introduced by the said analytical relations is offset by the possible errors of selecting the distribution law that may occur when the relations are strictly set.

The dependencies calculated for a specific IS and shown in Fig. 2 allow us to conclude that the larger the value of the parameter ρo , characterising the relative average difference between the duration of the conflict and the time needed for security violation, the higher the probability of security breach in the observed information system. This means that for preventive influence, time is more important than the probability of failure at the later stages of vulnerability search and utilisation.

As a special case of determining changes in the parameters of an information system that is under the influence of external influences, modelling of information-psychological impact (IPI) using neural networks in [1-9] is considered. The use of a neural network algorithm is an effective tool for modelling and studying an information system that is under the influence of external factors [10-15]. Depending on the tasks to be solved, information systems can have numerous parameters and characteristics [16-21]. In [6-9], an approach was considered for predicting the parameters and characteristics of an information system using a wavelet transform.

Consider a model of the process of detecting changes in the states of an information system using neural networks and wavelet transform.

If the information system is located under external influences, the effects are directly on its components (subjects, nodes, etc.). The process of exposure to an information system includes the following components: impact on components, providing the functions of an information system, determining a result of an impact, analysis of a result of an impact, response to a result of an impact [6-9]. Figure 3 shows a model of the process of influencing the components of an information system.

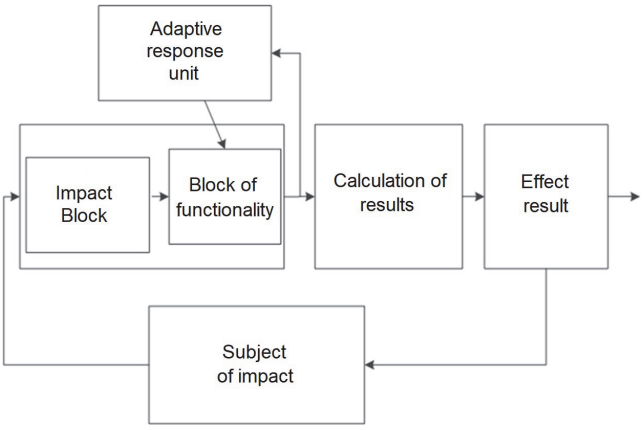

Figure 3 – Model of the process of implementing the impact on the components of the information system

Consider the components of the model of the process of influence on the information system.

The block of influence shown in Figure 4 on the components of the information system is a single-layer perceptron [2-9]. As an input signal, the characteristics of the means that affect are taken. We represent the input vector as $S = \{S_1, S_2, ..., S_l\}$, where the weights correspond to the effectiveness of the means of action. Artificial neuron, for property $Sub_i(Char_m)$, calculates a weighted sum of input signals. With an artificial neuron, the means of influence are compared with weight $Ef_{i,m,j}$ weighted sum of input signals. Then an output signal is generated. $res_{i,m}$, by comparing the result with a threshold value P, which is generally different for each property [2-9]. Thus, we obtain the output vector $OUT_B = \{res_{1,1}, res_{1,2}, ..., res_{n,k}\}$, which forms the meaning of the impact. The vector is calculated by the expressions: $NET_B = S^T \cdot Ef$,

$$OUT_B = f(NET_B),$$

where $f(NET_B)$ represents a threshold function:

$$f(NET_B) = \begin{cases} res_{i,m}, & \text{если } NET_B > P \\ 0, & \text{если } NET_B < P \end{cases}.$$

Presented in Figure 4, the information system function support block is a single-layer perceptron, which works similarly to the perceptron of the block of influence on information system components. We represent the input signal as a vector $B = \{B_1, B_2, ..., B_p\}$, where weights correspond to the efficiencies $Ef'_{i,m,j}$ means of providing functions $Ef_{i,m,j'}$ information system for properties $Sub_i(Char_m)$. Then the output signal is formed (measures to eliminate the effects) $res'_{i,m}$, by comparing the result with a threshold value P' [2-9].

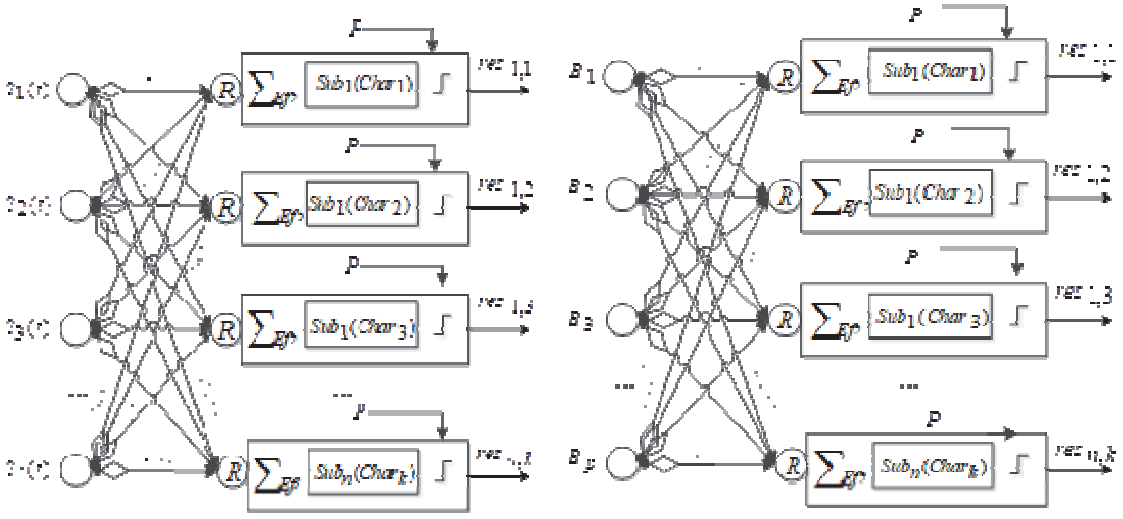

Figure 4 – From left to right: impact block, block providing functions and tasks for the purpose of the information system

Matrix $\mathrm{Re}l$ reflects the relationship of impact and functions solved by the components of information systems and describes the presence of dangerous effects on the information system. Vector values B are determined by the matrix $\mathrm{Re}l$. Matrix Columns $\mathrm{Re}l$ define sets of means of influence, which are intended for the properties of the components of the information system. The lines reflect the inclusion or deactivation of the means of ensuring the functions of the information system. For example, the matrix $\mathrm{Re}l = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ means that when affecting a property $Sub_1(Char_1)$ funds included B_1 и B_2, but on the property $Sub_1(Char_2)$ – only B_2 [2-9]. So the output vector $OUT_{ОИБ}$ of the system for ensuring the functions of the information system will be determined by the following expressions:

$$B = OUT_{ОИБ} \cdot \mathrm{Re}l, \; NET_{ОИБ} = B^T \cdot Ef', \; OUT_{ОИБ} = f'(NET_{ОИБ}),$$

$$f'(NET_{ОИБ}) = \begin{cases} res'_{i,m}, & \text{если } NET_{ОИБ} > P' \\ 0, & \text{если } NET_{ОИБ} < P' \end{cases}.$$

In general, the operation of artificial neurons depends on threshold functions $P(t)$ and $P^{'}(t)$. Figure 5 presents a model of the impact process on an information system based on a recurrent neural network, taking into account the work of the adaptive control unit [2-9].

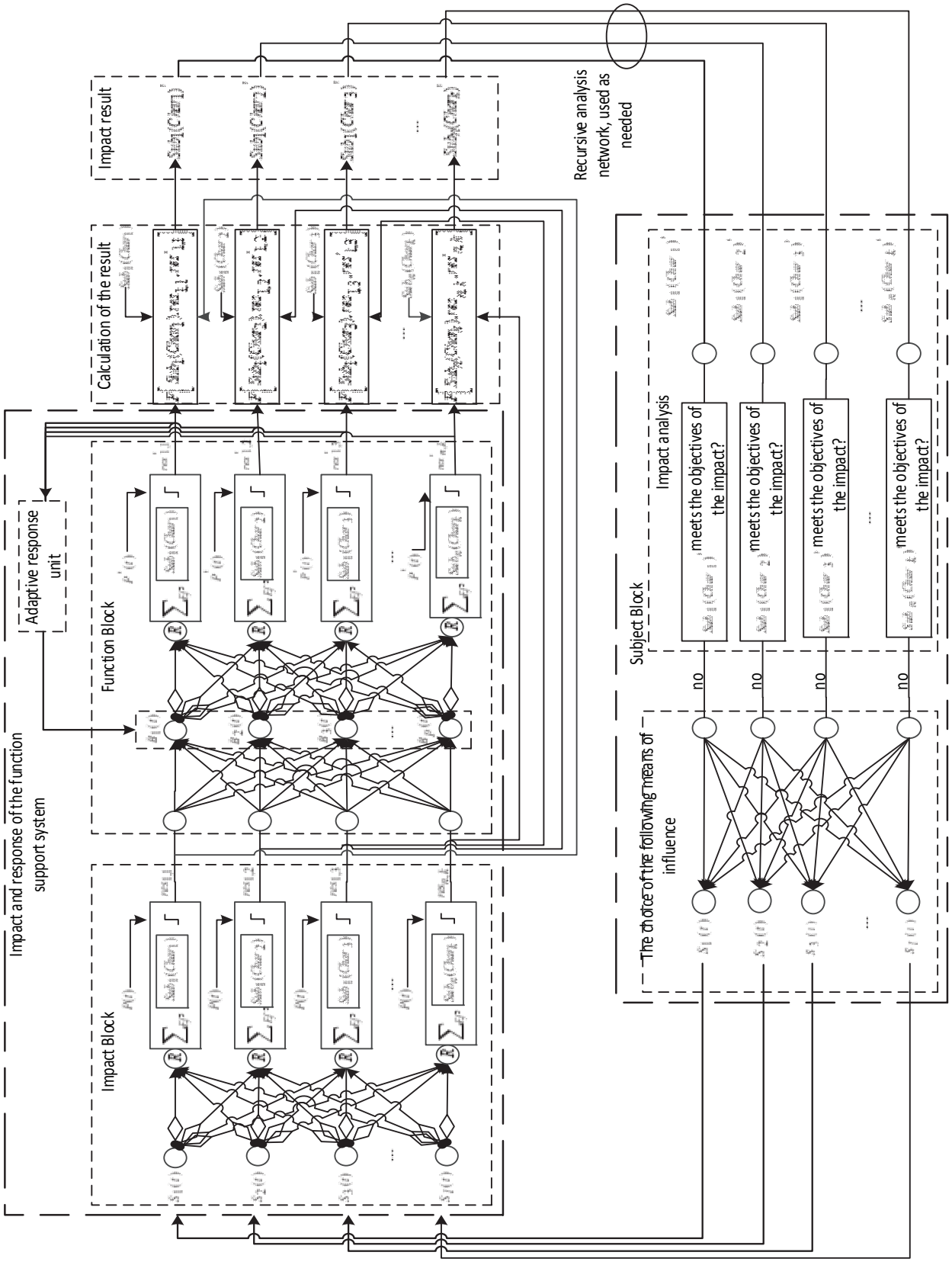

Figure 5 – A model for describing the process of influencing an information system based on a recurrent neural network

The adaptive response unit serves to determine the prerequisites for changes in the state of the information system and activates the means to eliminate or compensate for these prerequisites or directly the changes themselves. Thus, the input of the adaptive response unit receives signals about the prerequisites for changes, and the output of this unit generates signals to enable the appropriate means to eliminate or compensate for these prerequisites or directly the changes in the information system [2-9].

Using the mathematical apparatus of the wavelet transform, it is possible to control the regulation of changes in the states of the information system.

Imagine the state of an information system using a state function that describes its properties at a certain point in time. To do this, we represent the totality of all the properties of an information system in the form of a convolution function of a sequence of functions that are the properties of components [2-9].

Let us consider a simple case in which single rectangular pulses are functions of the properties. The amplitude of these pulses will depend on the value of the corresponding properties of the component of the information system. The pulse duration will be taken continuously for all subsequent representations. For example, the state of information system A corresponds to a sequence of pulses, which is presented in Figure 6. The state function of information system A is shown in Figure 7.

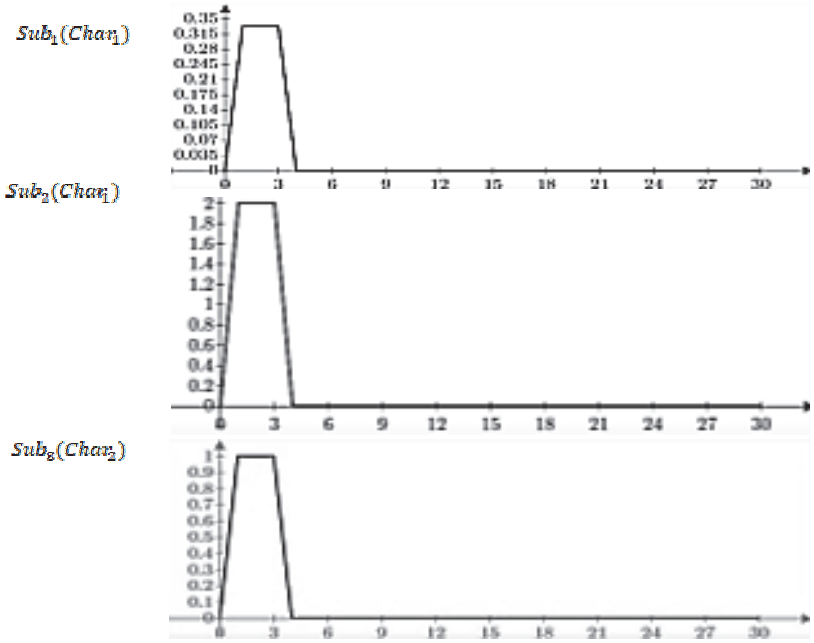

Figure 6 – Functions of the subject properties of the information system

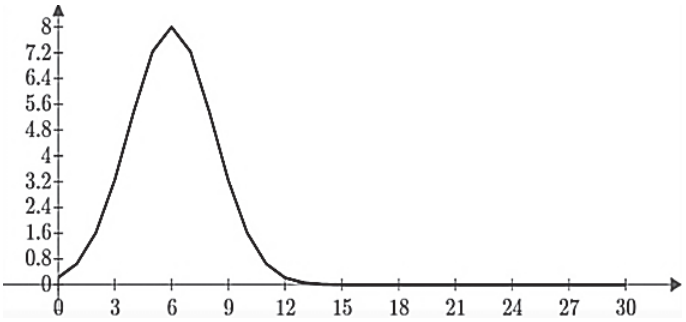

Figure 7 – Function of the state of the information system

$$Obj_A = \begin{pmatrix} 1/3 & 0 \\ 2 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} \tag{2.4}$$

Approximating this function, we can assume that the state function of the information system is a bell-shaped impulse in a two-dimensional representation. This function takes place for information systems having at least three properties that can be described by single rectangular pulses [2-9].

During the process of influencing the information system, its properties change, which leads to a change in the matrix of its properties and, accordingly, to a change in the state function. The change in the state function reflects the sequence of states that the information system receives at the appropriate time intervals during which the information system is exposed [2-9].

Imagine the transition of an information system from state A to the following states in the course of the impact on it, which is a set of tools S_1, S_2, S_3. This effect is gradually implemented by the enemy:

$$(Obj_A, S_1) = \begin{pmatrix} 1.5 & 0 \\ 1.3 & 1.3 \\ 0 & 0.7 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} = Obj_{A2}, \qquad (Obj_{A2}, S_2) = \begin{pmatrix} 0.5 & 0 \\ 0 & 1.2 \\ 0 & 2.23 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} = Obj_{A3}$$

$$(Obj_{A3}, S_3) = \begin{pmatrix} 1 & 0 \\ 0 & 1.2 \\ 0 & 0 \\ 0.6 & 1 \\ 0 & 1 \end{pmatrix} = Obj_{A4}$$

Let us assume that every 30 intervals, the state of the information system is monitored. During this period, a successful stage of influence on the information system is carried out [2-9]. Then, the dynamics of the state function A of the information system will take the form A, shown in Figure 8.

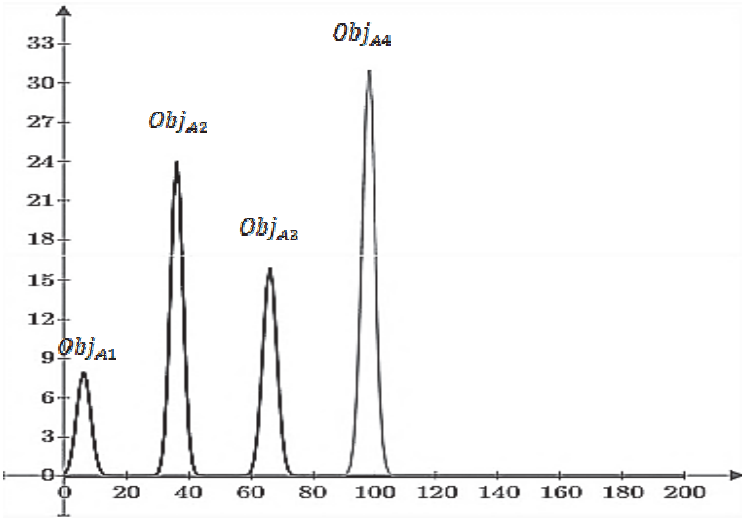

Figure 8 – Dynamics of changes in the function of states of the information system under the influence

Using the wavelet transform, you can visualize an analysis of the state of the information system. Wavelet spectrum $S(a,b)$ is a function of two arguments, where is the time scale, which is similar to the period of oscillations, and b similar to the signal offset along the time axis. At $a = a_0$ the function characterizes the time dependence, with $b = b_0$ the function characterizes the frequency dependence (for $b = b_0$). Since the studied signals in this work are single pulses, the wavelet spectrum of a single pulse of duration τ, which is concentrated in a neighborhood of a point $t = t_0$ has the greatest value in the vicinity of the point with coordinates $a = \tau, b = t_0$ [2-9].

We calculate the wavelet spectrum of the state of the information system using the basic Mexican hat wavelet. $MHAT(t,a,b) = \left(1 - 2\left(\frac{t-b}{a}\right)^2\right) \cdot \exp\left(-\left(\frac{t-b}{a}\right)^2\right)$, the analytical representation of the wavelet transform takes the form

$$S(a,b) = \frac{1}{\sqrt{a}} \cdot \int_{-\infty}^{\infty} u(t) MHAT(t,a,b) dt \ .$$

Figure 9 shows a graph of a two-parameter spectrum as a surface in three-dimensional space $WS_{a,b} = S(a,b)$. In Figure 10, this graph is presented as iso levels on the plane.

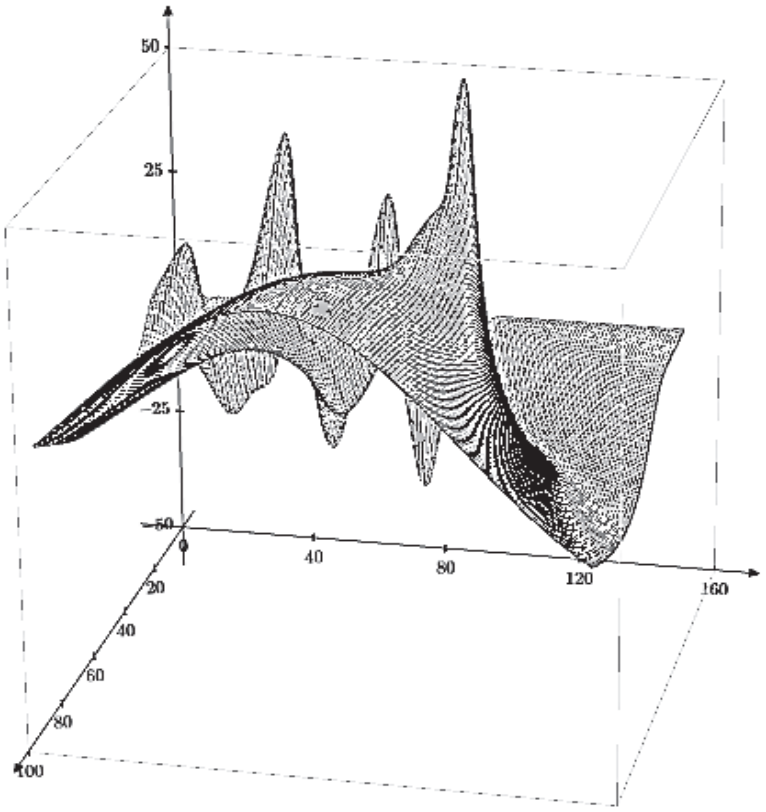

Figure 9 – Wavelet spectrum of the state change of an information system that is under the influence

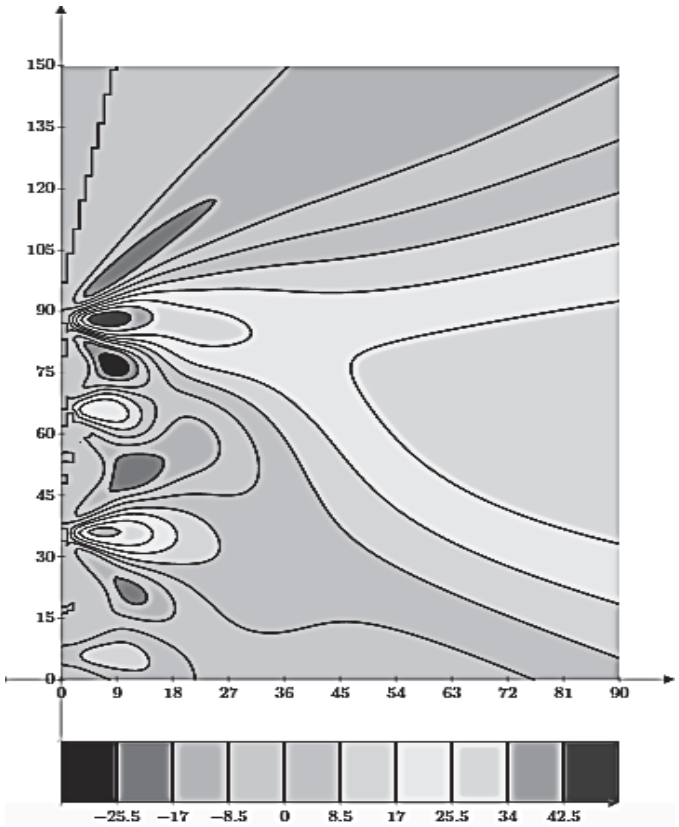

Figure 10 – Representation of the wavelet spectrum of the state change of an information system that is under the influence, using iso levels on the plane

The values of the elements of the matrix of states of the information system, in real conditions, are functions that reflect the properties of the system. Signals that correspond to the properties in this case will have a more complex form, this will determine a new type of state function of the information system and other ways of obtaining the wavelet spectrum. This may be applicable to the analysis of applied means of influence, to the result of changes in the states of the information system [2-9].

The constructed dependency graphs will allow adequate control to be carried out according to a given criterion.

The result of exposure to the information system $Obj^{'}$ will be determined by the function, which is the work of the impact unit, the unit for ensuring the functions of the information system, the adaptive response unit and the initial state Obj information system:

$$Obj^{'} = F(Obj, OUT_{B}, OUT_{ОИБ}),$$

where $F(x)$ - function of the resulting impact, which reflects the properties of the information system [2-9].

An analysis of the state of the information system after exposure can be made, and a decision can be made, based on the data obtained, on the need for further exposure, this makes the proposed neural network recursive, Figure 5.

Conclusion

Thus, a possible approach to the study of the characteristics of the information system under influence and their management using neural networks and wavelet transforms based on determining the relationship between the modified state of the information system and the possibility of dynamic analysis of effects is considered.

References

[1] A.S. Vyalykh, S.A. Vyalykh, A.A. Sirota. Neural network information processing algorithm for predicting software reliability // Bulletin of Voronezh State University «System analysis and information technology». Voronezh, 2013. №2. p.p. 140-143.

[2] A.V. Dushkin, I.V. Goncharov. N.I. Goncharov, S.S. Kochedykov and ets. Probabilistic Modeling in System Engineering / Edited by A.I. Kostogryzov // UK, London: IntechOpen, 2018. P. 278. – DOI: 10.5772/intechopen.71396.

[3] N.I. Goncharov, I.V. Goncharov, P.A. Parinov, A.V. Dushkin, M.M. Maximova. Modeling of Information Processes for Modern Information System Security Assessment // 28-31.01.2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). 2019. p.p. 1758-1763. – DOI: 10.1109/EIConRus.2019.8656828.

[4] N.I. Goncharov , A.V. Dushkin , I.V. Goncharov, P.A. Parinov. Simulation and evaluation of conflict interactions in information systems // International Conference «Applied Mathematics, Computational Science and Mechanics: Current Problems», 17-19.12.2018, Voronezh, Russian Federation. IOP Conf. Series: Journal of Physics: Conf. Series 1203 (2019) 012063. – DOI:10.1088/1742-6596/1203/1/012063.

[5] A.S. Dubrovin, A.V. Parfiryev, A.V. Dushkin, L.V. Stepanov. Control of unmanned aerial vehicles based on the detection algorithm // International Scientific Conference on Informatics: Problems, Methodologies and Technologies, 8-9.02.2018, Voronezh, Russian Federation. IOP Conf. Series: Journal of Physics: Conf. Series 1202 (2019) 012014. – DOI: 10.1088/1742-6596/1202/1/012014.

[6] I.V. Goncharov, N.Yu. Demyanenko, Ya.S. Mishina. The ability to simulate the process of information-psychological effects using neural networks // XIII International Scientific and Methodological Conference «Computer Science: Problems, Methodology, Technologies». Voronezh. 2013. p.p. 124-130.

[7] A.V. Dushkin, A.V. Porfiriev, V.I. Sumin. Algorithm of measurement information processing for hardware and software complex capture and automatic tracking of unmanned aerial vehicle // Proceedings. 2017 2nd International Ural Conference on Measurements (UralCon). South Ural State University (national research university), Chelyabinsk, Russian Federation, October 16-19, 2017. // IEEE, 2017, p. 199-204. – DOI: 10.1109/URALCON.2017.8120710.

[8] I.V. Goncharov, N.Yu. Demyanenko, Ya.S. Mishina. Formalization of the process of information-psychological impact // Bulletin of Voronezh State University, System Analysis and Information Technologies. 2012. №2. p.p. 36-41.

[9] P.A. Parinov, I.V. Goncharov, N.I. Goncharov, O.V. Raikov. Opportunities for the study of the characteristics of information computer systems and their management // Bulletin of the Voronezh State University, System analysis and information technology. Voronezh. 2017. №3. p.p. 65-71.

[10] A.V. Dushkin, T.I. Kasatkina, V.I. Novoseltsev, S.A. Ivanov. An improved method for predicting the evolution of the characteristic parameters of an information system // International Conference «Applied Mathematics, Computational Science and Mechanics: Current Problems» 18-20.12.2017, Voronezh, Russian Federation. IOP Conf. Series: Journal of Physics: Conf. Series 973 (2018) 012031. – DOI: 10.1088/1742-6596/973/1/012031.

[11] A.V. Dushkin , T.I. Kasatkina , V.A. Pavlov, R.R. Shatovkin. Algorithm for predicting the evolution of series of dynamics of complex systems in solving information problems // International Conference «Applied Mathematics,

Computational Science and Mechanics: Current Problems» 18-20.12.2017, Voronezh, Russian Federation. IOP Conf. Series: Journal of Physics: Conf. Series 973 (2018) 012031. – DOI:10.1088/1742-6596/973/1/012035.
[12] P.A. Parinov, I.V. Goncharov. Models of information-psychological impact // Bulletin of Voronezh State University, System analysis and information technology. Voronezh. 2014. №4. p.p. 19-25.
[13] S.S. Kochedykov, A.V. Dushkin, P.V. Markin. Express Assessment Method for the Risk of Impaired Functional Stability Information and Communication System in Conditions Cyber Attacks // 28-31.01.2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). 2019. p.p. 1754-1757. – DOI: 10.1109/EIConRus.2019.8657323.
[14] S.S. Kochedykov, E.V. Grechishnikov, A.V. Dushkin, D.E. Orlova. The mathematical model of cyber attacks on the critical information system // International Scientific Conference on Informatics: Problems, Methodologies and Technologies, 8-9.02.2018, Voronezh, Russian Federation. IOP Conf. Series: Journal of Physics: Conf. Series 1202 (2019) 012013. – DOI:10.1088/1742-6596/1202/1/012013.
[15] I.V. Goncharov, N.A. Korovin, N.I. Goncharov. Determination of characteristics of signals in the channel of spurious electromagnetic radiation of computer equipment using a USB interface // Bulletin of Voronezh State University, System analysis and information technology. Voronezh. 2014. №1. p.p. 52-64.
[16] D.A. Gubanov, D.A. Novikov. Models of distributed control in social networks // Control systems and information technology. 2009. №3.1(37). p.p. 124-129.
[17] A.V. Dushkin, S.S. Kochedykov, V.I. Novoseltsev. Tool and algorithmic diagnostic devices of operability of actuation mechanisms of automated control systems // Proceedings. 2017 2nd International Ural Conference on Measurements (UralCon). South Ural State University (national research university), Chelyabinsk, Russian Federation, October 16-19, 2017. IEEE, 2017. p.p. 193-198. – DOI: 10.1109/URALCON.2017.8120709.
[18] A.V. Parfiryev, I.N. Ischuk, A.V. Dushkin, T.S. Buriak, N.A. Popova. The Software Implementation of the System of Automatic Observation of Ground Objects Based on Correlation Analysis // 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). 2019. p.p. 1749-1753. – DOI: 10.1109/EIConRus.2019.8656636.
[19] A.V. Dushkin, S.S. Kochedykov, A.N. Noev and I.A. Gubin. Method of optimum channel switching in equipment of infocommunication network in conditions of cyber attacks to their telecommunication infrastructure // International Conference Information Technologies in Business and Industry 2018. IOP Conf. Series: Journal of Physics: Conf. Series 1015 (2018) 032101. – DOI:10.1088/1742-6596/1015/3/032101.
[20] V.I. Sumin, A.V. Dushkin, T.E. Smolentseva. Mathematical Models to Determine Stable Behavior of Complex Systems // International Conference Information Technologies in Business and Industry 2018. IOP Conf. Series: Journal of Physics: Conf. Series 1015 (2018) 032136. – DOI: 10.1088/1742-6596/1015/3/032136.
[21] V.I. Sumin, A.V. Dushkin, E.V. Grechishnikov, S.V. Ivanov. Determining the reliability of network information systems // International Conference «Applied Mathematics, Computational Science and Mechanics: Current Problems», 17-19.12.2018, Voronezh, Russian Federation. IOP Conf. Series: Journal of Physics: Conf. Series 1203 (2019) 012083. – DOI:10.1088/1742-6596/1203/1/012083.