Control of component alterations according with the target efficiency of data processing and control system

V.E. Gvozdev[1], M.B. Guzairov[1], D.V. Blinova[1], A.S. Davlieva[1]

[1]*Ufa State Aviation Technical University, Karl Marx street, 12, Ufa, Russia*

Abstract

In this article we describe the solution to make an estimate of allowed alternations in model components parameters that make up a data processing and control system. They reflect properties of physical and information components of the aforementioned system. This solution is derived according to the limitations of possible changes in integral property that describes the system behavior in different modes of operation. The proposed solution makes it possible to solve not only the direct problem - making a conclusion whether the vulnerability of the data processing system is negligible with respect to alternations in parameters of this systems components but the inverse as well, finding tolerable levels in alterations in systems components parameters from an acceptable level of uncertainty of targeted efficiency. The proposed solution follows known demands: inner properties of the system must be so that customer demands are fulfilled.

Keywords: data processing and control system; system vulnerability; target system efficiency; parameter alternations; uncertainty in systems components

1. Introduction

Nowadays information environment is a key factor in the life of our society, which leads to critical importance of managing the functional vulnerabilities of data processing and control systems. (DPCS) [1]. Concept of "security" is tightly coupled with the concept of "reliability" [2]. Reliability estimate is done by comparison of actual functional properties of the system and base functional properties defined in the development specification. These base functional properties in turn are the reflection of wishes and demands of the users onto the functional properties of DPCS. One of the properties of "general reliability" is survivability, the property of the system to continue functioning under influence of external and internal malicious factors, such factors include alternations in parameters of components of the system [3,4]. The opposite to survivability is vulnerability - a parameter that describes the possibility of the system being damaged by external and internal causes of different nature. These can be functional, economical, management, physical and so on. One of the distinct properties of modern DPCS is that they have infinitely many internal states. This is caused by infinite combinations of input data as well as other external factors that can cause errors of different nature. The cause of these defects are flaws of different types made on certain stages of software lifecycle [5-8]. The latter promotes development of vulnerability research techniques of DPCS by analysis of external behavior of the system [9-11]. This work presents a technique to study the influence of alterations in systems parameters, running in different modes; on it’s vulnerability in cases when the external behavior of the system is defined by the target efficiency property.

2. Target efficiency as indirect property of functional vulnerability

Functional vulnerability is the factor that negatively effects consumer qualities and consumption of resources needed to maintain DPCS.

Target efficiency shows the degree of match between actual functions of the system and it’s target functions [2]. Due to this fact target efficiency can be viewed as integral quality property of DPCS, used in different modes. This quality property shows the correlation between the expected by users behavior and external behavior of the given system. Decline in the target efficiency is an indirect property of deviation of the system from state S_k and base state S_0, in other words it is an indirect vulnerability criteria. Random nature of the target allows the usage of statistical methods to research the target efficiency [3].

In [3] robustness of the system is defined as follows: "...conditional probability of end system state S_k will not deviate from base state S_0 more than a given value ε_0 when event ω happens". The same reference contains formal relations between functional vulnerability and robustness.

$$v_f = 1 - \mathrm{Rob}, \tag{1}$$

where $\mathrm{Rob} = 1 - P[\|S_k - S_0\| < \varepsilon_0 | \omega]$. Here ω is an attribute of unwanted event.

Based on the given definition of robustness relations between robustness and functional vulnerability it is possible to state that there exists a direct dependency between robustness and target efficiency. Existence of such dependency lets us postulate the following: functional vulnerability of the system v_f is contained in tolerable limits $\varepsilon_0^{(v_f)}$, if the probability of deviation of target efficiency property $Э_\Sigma$ does not rise over a base value $\varepsilon_0^{(v_f)}$:

$$\exists P[|Э_\Sigma - Э_\Sigma^{(0)}| < \varepsilon_0^{(Э_\Sigma)}] \Rightarrow v_f < \varepsilon_0^{(v_f)}. \tag{2}$$

Alteration of systems components parameters is the inherent property of any DPCS. Statistical uncertainty as a probability of state parameters being in tolerable intervals comprise the metric property of such alteration. On the other hand change in the parameters is the cause of statistical uncertainty of target efficiency property:

$$v_f = f_1(H_D)\ , \tag{3}$$

$$H_Э = f_2(H_D)\, , \tag{4}$$

Here $H_Э$ is the metric uncertainty characteristic of the target efficiency;

$f_1(\bullet)$ – a direct functional relationship, making a relationship v_f between the metric characteristics of the uncertainty H_D and the state parameters vector components D .

$f_2(\bullet)$ – a direct functional relationship that makes a relationship $H_Э$ between the metric characteristics of uncertainty H_D . The character $f_2(\bullet)$ is defined by the structure of the system.

From (3) and (4) it can be concluded that, from the limitations on the statistical uncertainty of the system's target efficiency, there is a limitation on the value of the statistical uncertainty of the system state parameters. In other words, if the limitations on the variability (the uncertainty characteristic) of the average target efficiency's index are kept, then it can be argued that the vulnerability of the system is within the permissible limits.

3. Task statement and assumptions

The initial data of the problem are:

(A) Description of the system states set $S_i\,(i = \overline{1;N})$, with each state matching the characteristics of the target efficiency $Э_i$;
(B) The same characteristics of the statistical uncertainty of the target efficiency for each states $H_i(Э)$;
(C) A system model that characterizes the relationships λ_{ij} between the states i and j $(i, j = \overline{1;N}, i \neq j)$;
(D) A rule that allows us to estimate the average proportion of the time $p_i(i = \overline{1;N})$ the system is in the i-th state;
(E) Uncertainty characteristics of relations $H_{ij}(\lambda)$;
(F) The rule for estimating the average target efficiency $Э_\Sigma$ as a function of $Э_i$ and p_i :

$$Э_\Sigma = \varphi(Э_i, p_i)\, ; \tag{5}$$

(G) The rule for estimating the statistical uncertainty characteristics of the average target efficiency $H_Э$ based on $H_i(Э), H_{ij}(\lambda)$:

$$H_Э = f_2(H_i(Э), H_{ij}(\lambda)) \tag{6}$$

Note that in (5) components $H_i(Э), H_{ij}(\lambda)$ are the components of the state parameters vector (see (H)).

(H) Limitations on the variability $\Delta H_Э$ of the uncertainty characteristic of the average target efficiency $\varepsilon_0^{(Э_\Sigma)}$.

It is required: to estimate the limits on the possible values of uncertainty characteristics $\Delta H_i(Э), \Delta H_{ij}(\lambda)$ based on the limitation on the values $\Delta H_Э$ of the uncertainty characteristic of the average target efficiency.

Assumptions:

(A) The apparatus of Markov processes is used as a basis for modeling the state of DPCS [12];
(B) Intervals $Э_i \in [Э_i^{(l)}, Э_i^{(u)}]$; $\lambda_{ij} \in [\lambda_{ij}^{(l)}, \lambda_{ij}^{(u)}]$ are used as characteristics of the statistical uncertainty of the target efficiency $H_i(Э)$ and relationships $H_{ij}(\lambda)$ accordingly. The index "l" corresponds to the lower limit of the interval; index "in" - the upper;
(C) Linear convolution is used as an estimate of the target efficiency

$$Э_\Sigma = \sum_{i=1}^{N} p_i \cdot Э_i\, , \tag{7}$$

which is the average value of the target efficiency;
(D) Probability is a uncertainty characteristic of the target efficiency

$$H_Э = P[a^{(н)} < Э_\Sigma < a^{(в)}]\, , \tag{8}$$

where, $a^{(l)}$, $a^{(u)}$ are determined by (Fig. 1):

$$P[0 < Э_\Sigma \le a^{(н)}] = P[a^{(в)} < Э_\Sigma < \infty] = \varepsilon_0^{(Э_\Sigma)} / 2\, . \tag{9}$$

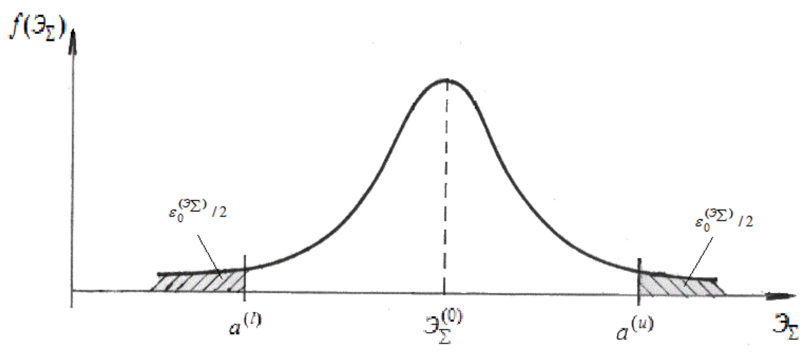

Fig. 1. The graphical illustration to the problem of estimating confines on the of uncertainty characteristics values of the target efficiency.

In Fig. 1 $Э_{\Sigma}^{(0)}$ corresponds to the basic values $\{Э_i\},\{\lambda_{ij}\}$.

4. Solution for the task[1]

The basis solution for the task is the construction of the dependence (6), which connects the statistical characteristics of the uncertainty of the average target efficiency of the system with the statistical characteristics of the uncertainty of the components of the system model. The basis for constructing the dependence (6) is a statistical experiment, the scheme of which is shown in Fig.2.

Specifying a model (graph) linking the states of the system (nodes) and transitions (edges) between states

↓

Specifying the statistical uncertainty characteristics of nodes and edges as lower and upper limits $\{Э_i^{(l)}, Э_i^{(u)}\}; \{\lambda_{ij}^{(l)}, \lambda_{ij}^{(u)}\}$, $i, j = \overline{1;N}, i \neq j$

↓

Generation η arrays of random numbers corresponding to $H_i^{(\xi)}(Э)$, $H_{i,j}^{(\xi)}(\lambda)$, $\xi = \overline{1;\eta}$ and calculation on their basis an array of random values of average target efficiency $H_Э^{(\xi)}$, $\xi = \overline{1;\eta}$

↓

On the base of the $H_i^{(\xi)}(Э)$ $H_{i,j}^{(\xi)}(\lambda)$, $H_Э^{(\xi)}$ was formulated the dependence

$H_Э = f_2(H_i(Э), H_{ij}(\lambda))$

↓

Setting a limitations $\varepsilon_0^{(Э_\Sigma)}$ on the variability of the statistical uncertainty index the average target efficiency, determining the limits $Э_\Sigma^{(l)}$, $Э_\Sigma^{(u)}$, the range of possible values $Э_\Sigma$

↓

Estimation based on the dependence $H_Э = f_2(H_i(Э), H_{ij}(\lambda))$ and $\{Э_\Sigma^{(l)}, Э_\Sigma^{(u)}\}$ limitations on the values $\{Э_i^{(l)}, Э_i^{(u)}\}$, $\{\lambda_{ij}^{(l)}, \lambda_{ij}^{(u)}\}$

Fig. 2. Scheme of statistical experiment.

In the experiment as the uncertainty characteristic of the average target efficiency $H_Э$ was the distribution density $f(Э_\Sigma)$ of the average target efficiency $Э_\Sigma$. As the uncertainty characteristics of system components $H_i(Э), H_{ij}(\lambda)$ were interval limits of possible values $\{Э_i^{(l)}, Э_i^{(u)}\}$, $\{\lambda_{ij}^{(l)}, \lambda_{ij}^{(u)}\}$. These limits were determined by the rules:

$Э_i^{(l),(u)} = Э_i^{(\varnothing)}(1 \pm \alpha_Э)$; $\lambda_{ij}^{(l),(u)} = \lambda_{ij}^{(\varnothing)}(1 \pm \alpha_\lambda)$,

where the sign "–" corresponds to the lower limit of the interval of possible values of the graph component characteristic; the "+" sign corresponds to the upper limit;

the index "$\varnothing$" corresponds to the basic values of the characteristic.

Note that the interval uncertainty characteristics estimates in accordance with the principle of maximization of entropy [13, 14] can be associated a law of random variable distribution.

Fig. 3 shows the model (states graph) of the system [15, 16]. Table 1 shows the base values of average target efficiencies $(Э_i^{(b)}, i = \overline{1;4})$. The base values of the transitions intensities $(\lambda_{ij}^{(b)}, i, j = \overline{1;4}, i \neq j)$ were taken to be the same and equaled ten. During the study, $\alpha_Э, \alpha_\lambda$ took a different value $(\alpha_Э \in [0;1], \alpha_\lambda \in [0;1])$. Fig. 4 shows estimates of the distribution densities $f(Э_\Sigma)$, corresponding to different $\alpha_Э, \alpha_\lambda$ for different uncertainty distribution by the graph components:

(A) The statistical uncertainty corresponds to the graph nodes, the nominal values of the transitions intensities correspond to the edges;

[1] In the development of the program for conducting a statistical experiment and processing the results of the experiment, the undergraduate student of the Department of Technical Cybernetics of the Ufa State Aviation Technical University Teslenko V.V. actively participated.

(B) The statistical uncertainty corresponds to the graph edges, the nominal values of the average target efficiency correspond to the nodes;

(C) The statistical uncertainty corresponds to both the edges and the nodes of the graph.

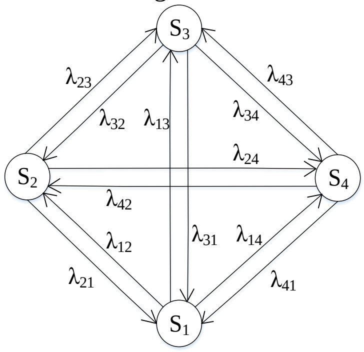

Fig. 3. States graph of the system.

Table 1. Characteristics of graph nodes.

System state	S_1	S_2	S_3	S_4
Base value of average target efficiency	10	20	30	40

At estimating $f(Э_\Sigma)$ value η was taken 10^4. To determine the number of grouping intervals in the histograms construction, the Sturges rule was used:

$$n = \mathbf{int}(1 + 3.3\mathbf{lg}\eta)$$

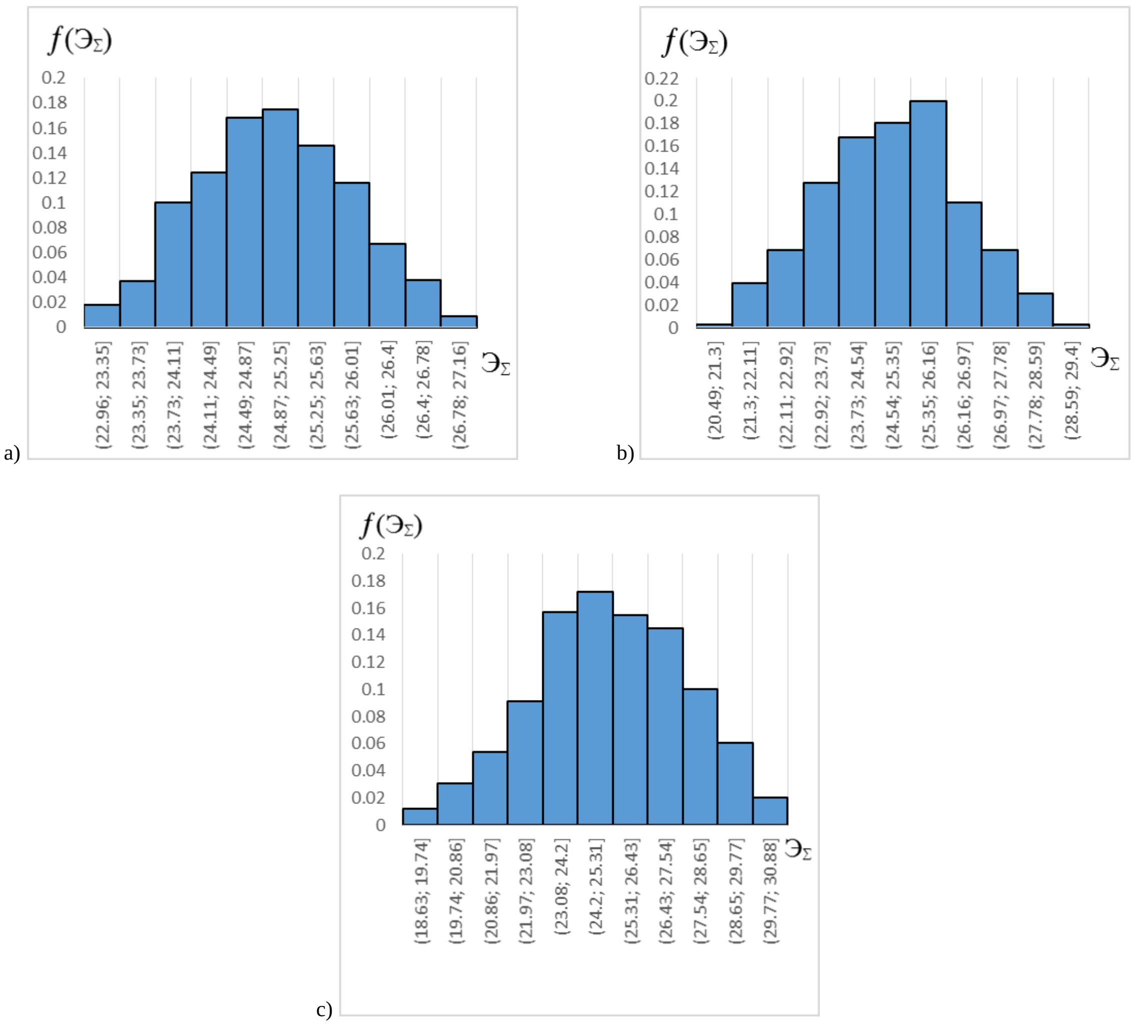

Fig. 4. Estimates of the distribution densities by: a) $\alpha_Э = 0, \alpha_\lambda = 0.2$; b) $\alpha_Э = 0.2, \alpha_\lambda = 0$; c) $\alpha_Э = 0.2, \alpha_\lambda = 0.2$.

The constructed estimates $f(Э_\Sigma)$ became the basis for constructing $H_Э$, for various combinations of characteristics the statistical uncertainty of the graph components. Fig. 5 shows the resulting dependencies, corresponding to different values $\varepsilon_0^{(Э_\Sigma)}$

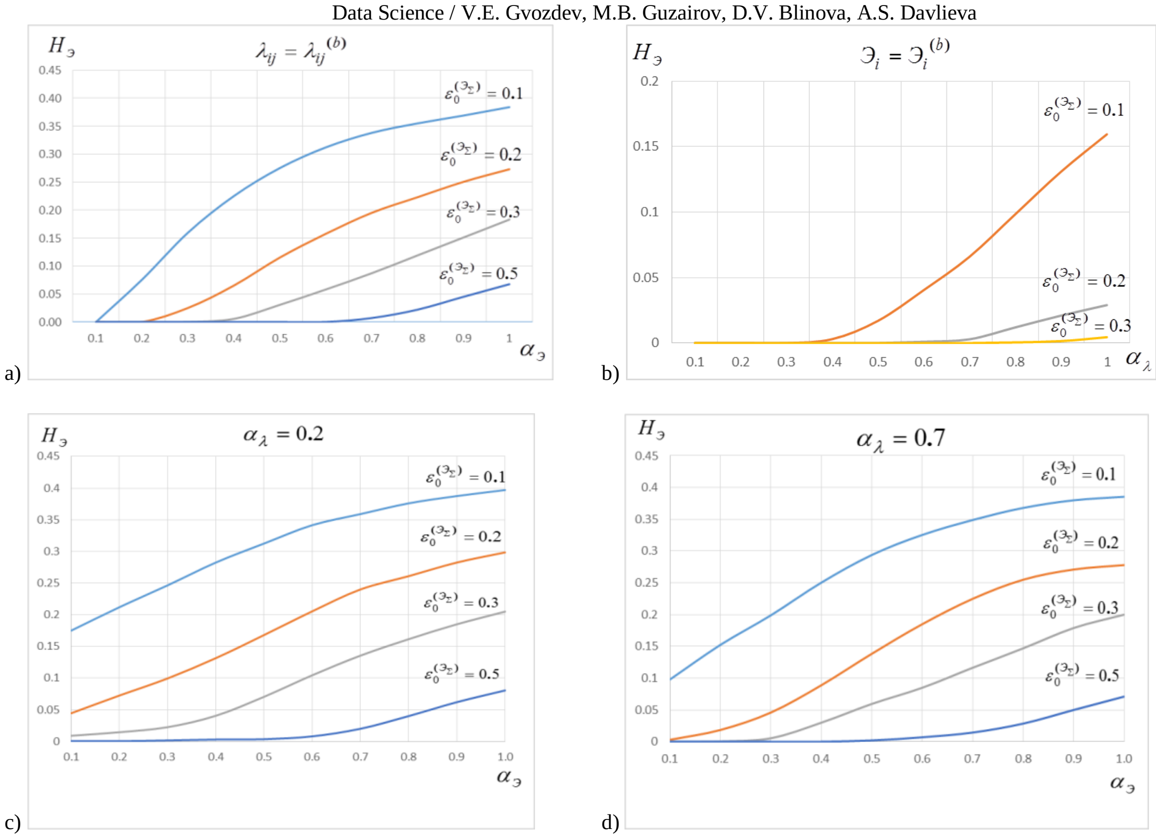

Fig. 5. Uncertainty characteristics dependences of average target efficiency on uncertainty characteristics of graph components.

The resulting dependences $H_{Э}$ allow us to solve a direct problem: an estimation of uncertainty characteristics of target average efficiency $H_{Э}$ on the information basis on model components parameters variability; and the inverse problem: an estimation limitations on the parameters variability of graph's nodes and edges based on the limitations on the characteristics of the target average efficiency.

An example of solving a direct problem. Given: $\varepsilon_0^{(Э_\Sigma)}$; $\alpha_{Э}$. It is believed that the variability of transitions intensities is absent. It is required to estimate the expected uncertainty $H_{Э}$. The scheme for solving the problem is shown in Fig. 6.

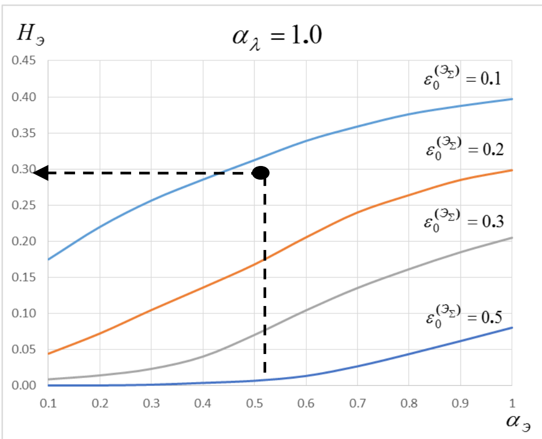

Fig. 6. An example of solving a direct problem.

An example of solving an inverse problem.

Given: $H_{Э}$; $\varepsilon_0^{(Э_\Sigma)}$; α_λ. It is required to estimate the possible value $\alpha_{Э}$. Fig. 7 shows an example of solving an inverse problem with the selected value α_λ. Thus, the proposed technique allows us to formalize the procedure for making conclusions about the vulnerability of the data processing and control system based on the analysis the characteristics of the external behavior of the system.

5. Conclusion

Nowadays DPCS play more and more of a substantial role as a vital component in systems that control complex objects. This promotes posing the problem of developing theoretical basis and development tools for managing the functional security of DPCS. One of the key tasks in solving such a problem is analyzing vulnerabilities of DPCS. They are affected by internal properties (construction, component properties) and by external environment in which the system is operated. The allowed level of the vulnerability is determined by whether the deviation of the systems behavior from the base behavior is affecting the quality of control of a complex object.

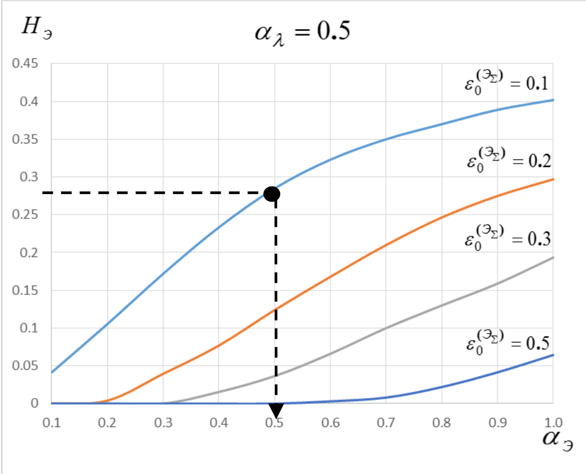

Fig. 7. An example of solving an inverse problem.

In this article a solution is given to estimate the possible deviation in components parameters of the model OF DPCS (such parameters reflect physical and information properties of the system). This solution is based of the limitations on alternation of the integral factor that shows the behavior of the system in different modes of operation, this behavior is the target efficiency of the system. Proposed solution follows known demands: inner properties of the system must be so that customer demands are fulfilled (Kano’s model). The described solution makes it possible to solve not only the direct problem - making a conclusion whether the vulnerability of the data processing system is negligible with respect to alternations in parameters of this systems components but the inverse as well, finding tolerable levels in alterations in systems components parameters from an acceptable level of uncertainty of targeted efficiency’s index.

Acknowledgements

This work was supported by RFBR grant No. 17-07-00351 "Methodological basics of dependability assurance of transmission systems telemetry information with use of intelligent data analysis technologies".

References

[1] Lipaev VV. Functional security of software. Moscow: SYNTEG, 2004; 348 p.
[2] Antamoshkin AN, Morgunova ON. Technique to study the effectiveness of complex hierarchical systems. Vestnik SibGAU 2006; 2 (9): 9–13.
[3] Makhutov NA, Reznikov DO. Vulnerability assessment of technical systems and its place in the risk analysis procedure. Problems of risk analysis 2008; 5(3): 72–85.
[4] Mladen AV. Software Reliability Engineering. Proceedings of the Annual Reliability and Maintainability Symposium. Los Angeles, California, USA, January 24-27, 2000.
[5] Abde lMoez W, Nassar D, Shereshevsky M, Gradetsky N, Gunnalan R, Ammar HYuB, Mili M. Error Propagation in Software architectures. Proceedings of the Software Metics. 10th International Symposium, Washington, DC, USA. IEEE Computer Society, 2004; 384–393.
[6] Khoshgoflaar TM, Munson JC. Predicting software development errors using complexity metrics. IEEE of Selected Areas in Communications 1990; 8(2): 253–261.
[7] Bellini P, Bruno I, Nesi P, Rogai D. Comparing fault-proneness estimation models. Proc. of 10th IEEE International Conference on Engineering of Complex Computer Systems, 2005; 205–214.
[8] Maevsky DA, Yaremchuk SA. Estimating the number of software defects based on the complexity metrics. Electrotechnic and computer systems: Scientific and Technical Journal 2012; 7(83): 113–120.
[9] Michael CC, Jones RC. On the uniformity of error propagation in software. Proceedings of the Annual Conference on Computer Assurance, 1996; 68–76.
[10] Liu XF. Software quality function deployment. IEEE Potentials 2000; 19(5): 14–16.
[11] Shindo H. Application of QFD to Software and QFD Software Tools. Pre-Conference Workshops of the Fifth International Symposium on Quality Function Deployment and the First Brazilian Conference on Management of Product Development. Belo Horizonte, Brazil, 1999.
[12] GOST R 51901.5-2005 Risk management. Application guide of reliability analysis methods. Moscow, Standartinform, 2005; 44 p.
[13] Kuzin LT. Fundamentals of cybernetics. Vol. 1. Mathematical foundations of cybernetics. Textbook for students of technical colleges. M.: Energy, 1973; 504 p.
[14] Jaynes ET. Information theory and statistical mechanics. The Physical Review 1957; 106(4): 620–630.
[15] Gvozdev VE, Blinova DV, Davlieva AS, Teslenko VV. Construction of basic functioning efficiency models of the hardware-software complexes, based on the mathematical statistics methods. Software Engineering 2016; 7(11): 483–489.
[16] Gvozdev VE, Blinova DV, Davlieva AS, Teslenko VV. Effect assessment of the system parameters variability on the functional vulnerability'indexes of the hardware-software systems. Information Technologies for Intelligent Decision Making Support (ITIDS'2017). Proceedings of the 5th International Conference, Ufa, Russia, May 16-19, 2017. (in press)