SYSTEM APPROACH TO ESTIMATION OF GUARANTEED SAFE OPERATION OF COMPLEX ENGINEERING SYSTEMS

Nataliya Pankratova

Abstract: *A system approach to estimation of guaranteed safe operation of complex engineering systems is proposed. The approach is based on timely and reliable detection, estimation, and forecast of risk factors and, on this basis, on timely elimination of the causes of abnormal situations before failures and other undesirable consequences occur. The principles that underlie the strategy of the guaranteed safety of CES operation provide a flexible approach to timely detection, recognition, forecast, and system diagnostic of risk factors and situations, to formulation and implementation of a rational decision in a practicable time within an unremovable time constraint.*

Keywords: system approach, time constraints, multiple-factor I risks, abnormal mode, diagnostics, survivability, serviceability, safety

ACM Classification Keywords: *H.4.2. INFORMATION SYSTEM APPLICATION: type of* system strategy
Conference topic: *Applied Program Systems*

Introduction

The analysis of failures and accidents reveals their most important causes and the shortcomings of the existing principles of control of serviceability and safety of modern plant and machinery [1, 2]. One of such causes is the specific operation of diagnostic systems intended to detect failures and malfunctions. Such an approach to safety excludes a priori prevention of abnormal mode, which thus may become an abnormality, accident, or a catastrophe. Therefore, there is a practical need to qualitatively change the diagnostic system to account for the principles and structure of control of serviceability and safety of modern complex engineering systems (CESs) under the real conditions of multiple-factor risks.

We believe it expedient to consider a safety control problem as a system problem involving the detection of risk factors whose influence may result in abnormal situations. At the same time it is taken into consideration that safety and functioning control is implemented under conditions of incompleteness and uncertainty of dynamics of the transition of a normal to abnormal mode. The normal mode is not permanent and changes considerably at different stages of a system operation cycle. These conditions are met by the operation of many CES, the modes of which during operation differ fundamentally.

System approach is based on the suggested conceptual foundations of system analysis, multicriterion estimation, and forecast of risk situations. The main idea of the suggested concept consists in the replacement of the typical principle of detection of the operability state turning into the inoperability state based on detection of failures, malfunctioning, faults, and forecast of reliability of an object by a qualitatively new principle [3]. The essence of this principle is the timely detection and elimination of the causes of a possible changeover of an operability state to an inoperability state based on the system analysis of multifactor risks of abnormal situations, a credible estimation of margin of permissible risk for different modes of operation of a complex engineering object, and a forecast of the main operability indicators of an object during the assigned operating period.

The purpose of the paper is to propose a system strategy for the guaranteed safety operation of a CES as a unified complex of a methodology of serviceability and safety and its implementation as a toolkit of technical diagnostics of the CES while in service.

1. Main principles of problem solution and realization strategy

First, note the principal differences between the given problem of guaranteed safe operation of CESs and typical control problems. The main difference is that the initial information about a complex object contains only a small part of information about its state, properties, functioning processes, and operational capability characteristics. This information represents only the state and work characteristics of such objects in normal mode. Undoubtedly, this information is enough for decision making during the complex object control only on the condition that the normal mode continue for a long time. However, in real objects in view of existing technical diagnosis systems, oriented toward failure and malfunction detection, it is impossible to ensure that a malfunction or a failure will not appear within the next 5–10min. It is a priori unknown how much time it will take to repair a malfunction. It may take from a few minutes up to several hours or even days and months. And, consequently, the possible damage is a priori unknown, and thus the safety control system is, essentially, a recorder of information about facts and damage. A fundamentally different system approach can be realized on the basis of the proposed principle of timely detection of causes of abnormal situations, prompt prevention of regular situations from becoming abnormal or emergency, revealing risk factors, predicting basic survivability parameters of an object during a specified period of its operation as fundamentals of the guaranteed safety in the CES dynamics, eliminating the causes of possible nonserviceability based on systems analysis of multiple-factor I risks of abnormal situations [3].

The key idea of the strategy is to provide (under actual conditions of the operation of a complex system) timely and reliable detection and estimation of risk factors, prediction of their development during a certain period of operation, and timely elimination of the causes of abnormal situations before failures and other undesirable consequences occur.

Strategy realization is based on the following principles:

- system consistency in purposes, problems, resources, and expected results as to the measures of providing safety operation of the complex system;
- timely detection, guaranteed recognition, and system diagnostics of risk factors and situations;
- prompt forecasting, reliable assessment of abnormal situations;
- formation and realization of a rational solution in a practicable time within an unremovable time constraints.

Let us formulate the mathematical problem of recognizing an abnormal situation in the dynamics of a dangerous industrial object.

For each situation $S_k^\tau \in S_\tau$, the set $M_k^\tau \in M_\tau$ of risk factors is known to be formed as $M_k^\tau = \left\{ \rho_{q_k}^\tau \mid q_k = \overline{1, n_k}^\tau \right\}$. For each risk factor $\rho_{q_k}^\tau \in M_k^\tau$, given are a fuzzy information vector $I_q^\tau = \left\{ I_{q_k}^\tau \mid q_k = \overline{1, n_k}^\tau; k = \overline{1, K_\tau} \right\}$ and its components:

$$I_{qk}^\tau = \left\{ \tilde{x}_{q_k j_k p_k}^\tau \mid q_k = \overline{1, n_k}^\tau;\ j_k = \overline{1, n_{q_k}}^\tau;\ p_k = \overline{1, n_{q_k j_k}}^\tau \right\},$$

$$\tilde{x}_{q_k j_k p_k}^\tau = \left\langle x_{q_k j_k p_k}^\tau,\ \mu_{H_{q_k j_k p_k}}\left(x_{q_k j_k p_k}^\tau\right) \right\rangle;\ x_{q_k j_k p_k}^\tau \in H_{q_k j_k p_k}^\tau;\ \mu_{H_{q_k j_k p_k}} \in [0,1];$$

$$H_{q_k j_k p_k}^\tau = \left\langle x_{q_k j_k p_k}^\tau \mid x_{q_k j_k p_k}^- \le x_{q_k j_k p_k}^\tau \le x_{q_k j_k p_k}^+ \right\rangle.$$

For each situation $S_k^\tau \in S_\tau$ and each risk factor $\rho_{q_k}^\tau \in M_k^\tau$, $M_k^\tau \in M_\tau$, it is necessary to recognize an abnormal situation in the dynamics of a dangerous industrial object and ensure the survivability of the complex system during its operation.

We will consider the safety of a system as its ability to timely prevent the normal operation mode from becoming an abnormal one, an accident, or a catastrophe based on prompt detection of significant risk and to prevent it from becoming a catastrophic risk. The safety is characterized by the following parameters: the degree of risk η_i which is the probability of undesirable consequences; risk level W_i, which is the damage because of undesirable consequences of any risk factors at any instant of time $T_i \in T^{\pm}$ during the operation of the complex system; resource of the admissible risk of abnormal mode T_{pr}, which is the period of operation of the complex system in a certain mode during which the degree and level of risk do not exceed a priori specified admissible values. The safety parameters are evaluated by solving the general problem of analysis of multiple-factor I risks [4, 5].

The system consistency of the rates of diagnostics and the rates of processes in various operation modes of CES is provided by a unified algorithm for safety control in abnormal situations [6]. This algorithm implements procedures of diagnostics and assessment of abnormal situations during the transition from the normal mode into a sequence of abnormal situations. Based on this, a database and a scenario of a sequence of abnormal situations are formed, and the possibility whereby the complex object passes from abnormal situations to the normal mode is determined.

The strategy of system control of CES serviceability and safety is realized based of a diagnostic unit as an information platform of engineering diagnostics of the CES.

2. Information platform for engineering diagnostics of CES operation

The diagnostic unit, which is the basis of a safety control algorithm for complex objects in abnormal situations, is developed as an information platform (fig. 1).

Let us detail some of these modules of the information platform of engineering diagnostics (IPED).

Data accessing of the Initial Information during CES Operation. By a CES we mean an engineering object consisting of several multi-type subsystems that are system-consistent in tasks, problems, resources, and expected results. Each subsystem has functionally interdependent parameters measured with sensors. To this end, groups of sensors are connected to each subsystem, each having different parameters (time sampling, resolution, etc.), depending on what is its nature.

The engineering diagnostics during the CES operation requires samples of size N_{01} and N_{02}, where $N_{01}(N_{01} >> 200)$ is the total sample size during the CES real-mode operation; $N_{02}(N_{02} << N_{01}; N_{02} = 40 \div 70)$ is the size of the basic sample required to estimate the FDs. The initial information is reduced to a standard form, which makes it possible to form FDs from discrete samples. In view of the proposed methodology, biased Chebyshev polynomials are taken as basic approximating functions, which normalizes all the initial information to the interval [0, 1].

Recovery of Functional Dependences based on Discrete Samples. In the general case, the initial information is specified as a discrete array [7]

$$\mathrm{M}_0 = \left\langle \mathrm{Y}_0, \mathrm{X}_1, \mathrm{X}_2, \mathrm{X}_3 \right\rangle,$$

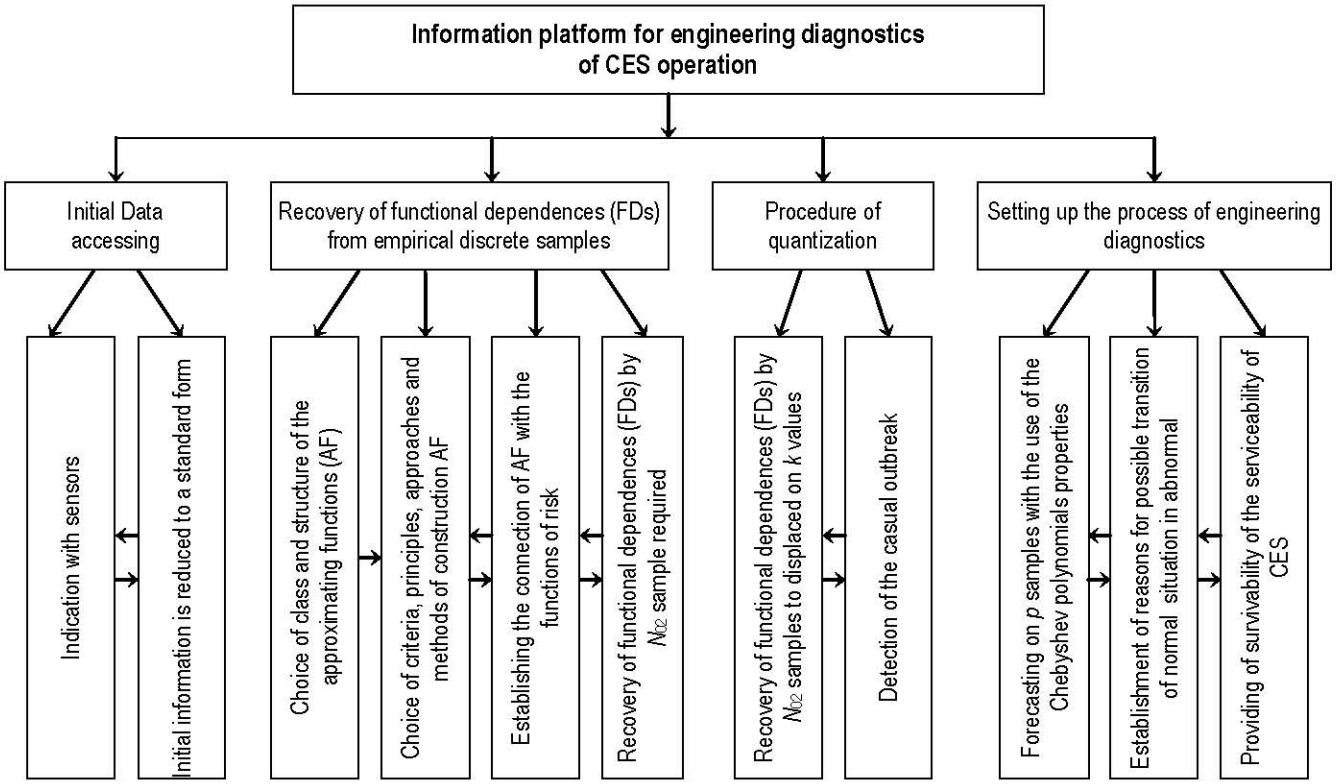

Fig. 1 Structural diagram of information platform for engineering diagnostics

$$\mathrm{Y}_0=\left(\mathrm{Y}_i \,\middle|\, i=\overline{1,m}\right),\ \mathrm{Y}_i=\left(\mathrm{Y}_i[q_0] \,\middle|\, q_0=\overline{1,k_0}\right),\ \mathrm{X}_1=\left(\mathrm{X}_{1j_1} \,\middle|\, j_1=\overline{1,n_1}\right),\mathrm{X}_{1j_1}=\left(\mathrm{X}_{1j_1}[q_1] \,\middle\|\, q_1=\overline{1,k_1}\right),$$

$$\mathrm{X}_2=\left(\mathrm{X}_{2j_2} \,\middle|\, j_2=\overline{1,n_2}\right),\ \mathrm{X}_{2j_2}=\left(\mathrm{X}_{2j_2}[q_2] \,\middle\|\, q_2=\overline{1,k_2}\right),\mathrm{X}_3=\left(\mathrm{X}_{3j_3} \,\middle|\, j_3=\overline{1,n_3}\right),\ \mathrm{X}_{3j_3}=\left(\mathrm{X}_{3j_3}[q_3] \,\middle\|\, q_3=\overline{1,k_3}\right),$$

where the set Y_0 determines the numerical values $\mathrm{Y}_i[q_0]\Rightarrow\langle\ \mathrm{X}_{1j_1}[q_1],\mathrm{X}_{2j_2}[q_2],\ \mathrm{X}_{3j_3}[q_3]\ \rangle$ of the unknown continuous functions $y_i=f_i(x_1,x_2,x_3)$, $i=\overline{1,m}$; $x_1=(x_{1j_1}\,|\,j_1=\overline{1,n_1})$, $x_2=(x_{2j_2}|\,j_2=\overline{1,n_2})$, $x_3=(x_{3j_3}|\,j_3=\overline{1,n_3})$. To each value of $q_0\in[1,k_0]$ there corresponds a certain set $q_0\Leftrightarrow\langle q_1,q_2,q_3\rangle$ of values $q_1\in[1,k_1]$, $q_2\in[1,k_2]$, $q_3\in[1,k_3]$.. The set Y_0 consists of k_0 different values $\mathrm{Y}_i[q_0]$. In the sets $\mathrm{X}_1,\mathrm{X}_2,\mathrm{X}_3$ a certain part of values $\mathrm{X}_{1j_1}[q_1]$, $\mathrm{X}_{2j_2}[q_2]$, $\mathrm{X}_{3j_3}[q_3]$ for some values $q_1=\hat{q}_1\in\hat{Q}_1\subset[1,k_1]$, $q_2=\hat{q}_2\in\hat{Q}_2\subset[1,k_2]$, $q_3=\hat{q}_3\in\hat{Q}_3\subset[1,k_3]$ repeats each, but there are no completely coinciding sets $\langle\mathrm{X}_{1j_1}[q_1],\mathrm{X}_{2j_2}[q_2],\mathrm{X}_{3j_3}[q_3]\rangle$ for different $q_0\in[1,k_0]$. We have also $n_1+n_2+n_3=n_0$, $n_0\le k_0$.

It is known that $x_1\in D_1, x_2\in D_2, x_3\in D_3$, $\mathrm{X}_1\in\hat{D}_1,\mathrm{X}_2\in\hat{D}_2,\mathrm{X}_3\in\hat{D}_3$, where

$$D_s=\left\langle x_{sj_s}\,\middle|\,d^-_{sj_s}\le x_{sj_s}\le d^+_{sj_s},\ j_s=\overline{1,n_s}\right\rangle,\quad s=\overline{1,3};$$

$$\hat{D}_s = \left\langle \mathrm{X}_{s j_s} \middle| \hat{d}^{-}_{s j_s} \le \mathrm{X}_{s j_s} \le \hat{d}^{+}_{s j_s},\ j_s = \overline{1, n_s} \right\rangle, \quad s = \overline{1,3};$$

$$d^{-}_{s j_s} \le \hat{d}^{-}_{s j_s}, \quad d^{+}_{s j_s} \ge \hat{d}^{+}_{s j_s}.$$

It is required to find approximating functions $\Phi_i(x_1, x_2, x_3)$, $i = \overline{1,m}$, that characterize the true functional dependences $y_i = f_i(x_1, x_2, x_3)$, $i = \overline{1,m}$, on the set D_s with a practicable error.

Since the initial information is heterogeneous as well as the properties of the groups of factors under study, which are determined, respectively, by the vectors x_1, x_2, x_3, the degree of the influence of each group of factors on the properties of approximating functions should be evaluated independently. To this end, the approximating functions are formed as a hierarchical multilevel system of models. At the upper level, the model determining the dependence of the approximating functions on the variables x_1, x_2, x_3 is realized. Such a model in the class of additive functions, where the vectors x_1, x_2, x_3 are independent, is represented as the superposition of functions of the variables x_1, x_2, x_3:

$$\Phi_i(x_1, x_2, x_3) = c_{i1}\Phi_{i1}(x_1) + c_{i2}\Phi_{i2}(x_2) + c_{i3}\Phi_{i3}(x_3), i = \overline{1, m}. \qquad (1)$$

At the second hierarchical level, models that determine the dependence $\Phi_{is}(s = 1,2,3)$ on the components of the variables x_1, x_2, x_3, respectively, and represented as

$$\Phi_{i1}(x_1) = \sum_{j_1=1}^{n_1} a^{(1)}_{ij_1}\Psi_{1j_1}(x_{1j_1}), \Phi_{i2}(x_2) = \sum_{j_2=1}^{n_2} a^{(2)}_{ij_2}\Psi_{2j_2}(x_{2j_2}),$$
$$\Phi_{i3}(x_3) = \sum_{j_3=1}^{n_3} a^{(3)}_{ij_3}\Psi_{3j_3}(x_{3j_3}). \qquad (2)$$

are formed.

At the third hierarchical level, models that determine the functions $\Psi_{1j_1}, \Psi_{2j_2}, \Psi_{3j_3}$ are formed, choosing the structure and components of the functions $\Psi_{1j_1}, \Psi_{2j_2}, \Psi_{3j_3}$ $\Psi_{1j_1}, \Psi_{2j_2}, \Psi_{3j_3}$ being the major problem. The structures of these functions are similar to (2) and can be represented as the following generalized polynomials:

$$\Psi_{sj_s}(x_{j_s}) = \sum_{p=0}^{P_{j_s}} \lambda_{j_s p}\varphi_{j_s p}(x_{sj_s}), s = 1,2,3. \qquad (3)$$

In some cases, in forming the structure of the models, one should take into account that the properties of the unknown functions $\Phi_i(x_1, x_2, x_3), i = \overline{1, m}$, are influenced not only by a group of components of each vector x_1, x_2, x_3 but also by the interaction of their components. In such a case, it is expedient to form the dependence of the approximating functions on the variables x_1, x_2, x_3 in a class of multiplicative functions, where the approximating functions are formed by analogy with (I)-(3) as a hierarchical multilevel system of models

$$[1+\Phi_i(x)]=\prod_{s=1}^{S_0}[1+\Phi_{is}(x_s)]^{c_{is}};[1+\Phi_{is}(x_s)]=\prod_{j_s=1}^{n_s}[1+\Psi_{sj_s}(x_{sj_s})]^{a^s_{ij_s}};$$
$$[1+\Psi_{sj_s}(x_{sj_s})]=\prod_{p=1}^{P_{j_s}}[1+\varphi_{j_sp}(x_{sj_s})]^{\lambda_{j_sp}}. \quad (4)$$

We will use the Chebyshev criterion and for the functions φ_{j_sp}, we will use biased Chebyshev polynomials $T_{j_sp}(x_{j_sp})\in[0,1]$. Then the approximating functions are found based on the sequence $\Psi_1,\Psi_2,\Psi_3\to\Phi_{i1},\Phi_{i2},\Phi_{i3}\to\Phi_i$ which will allow obtaining the final result by aggregating the corresponding solutions. Such an approach reduces the procedure of forming the approximating functions to a sequence of Chebyshev approximation problems for inconsistent systems of linear equations [8, 9].

Due to the properties of Chebyshev polynomials, the approach to forming the functional dependences makes it possible to extrapolate the approximating functions set up for the intervals $[\hat{d}^-_{j_s},\hat{d}^+_{j_s}]$ to wider intervals $[d^-_{j_s},d^+_{j_s}]$, which allows forecasting the analyzed properties of a product outside the test intervals.

Quantization of Discrete Numerical Values. The quantization is applied in order to reduce the influence of the measurement error of various parameters on the reliability of the solution being formed. The procedure of quantization of discrete numerical values is implemented as follows.

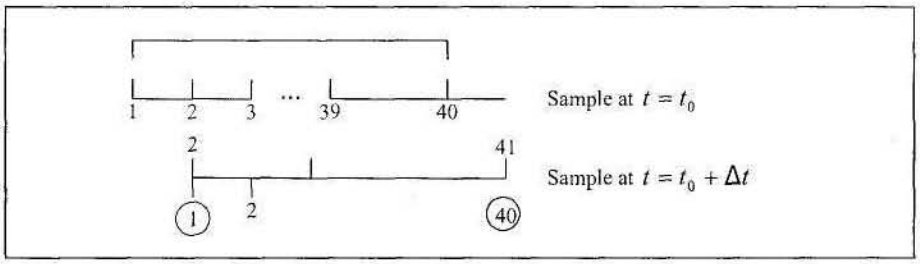

Fig. 2. Sample at $t=t_0$ and $t=t_0+\Delta t$

As the base reference statistic for each variable $x_1,...,x_n,y_1,...,y_m$, the statistic of random samples in these variables of size $N_{01}\geq 200$ is taken.

As the base dynamic statistic in the same variables, the statistic of the sample of the dynamics of the object for the last N_{02} measurements is taken. Therefore, the very first measurement of the original sample should be rejected and measurements should be renumbered in the next measurement $N_{02}+N_2$. Figure 2 schematizes the sample for the instant of time $t=t_0, N_{02}=40$ and $t=t_0+\Delta t(t=1,2,3,...,t_k,...,T)$.

For the current dynamic parameters, we take the statistics of samples of size $N_{02}+N_2$ biased by N_2 with respect to the statistics of samples of size N_{02}.

Processing of each sample in each variable should involve the following procedures:

— evaluating $\Phi_i^k(x_1^k,...,x_j^k,...,x_n^k), i=\overline{1,m}, j=\overline{1,n}$, in the form (2) or (4) for each k-th measurement for $t=t_k$;

— setting up a step function of the first level

$$Z_{1j}=\sum_{p=1}^{M_1} d_{jp}U(\hat{x});U(\hat{x})=\begin{cases}0,\hat{x}<0\\1,x\geq 0,\end{cases}\hat{x}=x_j-x_p;d_{jp}=\begin{cases}0{,}15 \text{ if } p=1,\\0{,}1 \quad \text{if } p=\overline{2,9},\\1 \quad\ \text{if } p=10,\end{cases}$$

$x=0{,}1\cdot p;p=\overline{1,10};M_1=10;$

— setting up a step function of the second level

$$Z_{2j}=\sum_{p=1}^{M_2} d_{jp}U(\hat{x});M_2=10;x_p^0=\begin{cases}0{,}5 \quad \text{if } p=1,\\0{,}1 \quad \text{if } p=\overline{2,9},\\1{,}15 \text{ if } p=10,\end{cases}d_{jp}=\begin{cases}0{,}1 \text{ if } p=\overline{1,9},\\1 \quad \text{if } p=10.\end{cases}$$

Forecasting Nonstationary Processes. The models for predicting nonstationary processes are based on the original sample of the time series for the initial interval D_0 and base dynamic model of processes (I)-(3). To this end, we will use the well-known property of Chebyshev polynomials that functions are uniformly approximated on the interval [0, 1]. The essence of the approach is as follows. The initial data are normalized for the interval $D=\{t\mid t_0^-\leq t\leq t^+\},D=D_0\cup D_0^+$, which includes the initial observation interval $D_0=\{t\mid t_0^-\leq t\leq t^+\}$ and the prediction interval $D_0^+=\{t\mid t_0^+<t\leq t^+\}$. Then, to determine the dynamic model of the processes as the estimated approximating functions (1) or (4) based on the initial data, the system of equations is formed for the interval D_0 as follows:

$$0{,}5a_0+\sum_{n=n_1}^{N} a_nT_n^*(\tau_{k_1})-\hat{y}_{k_1}=0;k_1=\overline{1,K_0}; \tag{5}$$

$$\hat{y}_{k_1}=y(\tau_{k_1}),\tau_{k_1}\in[0,\tau_{k_1}^+],\tau_{k_1}^+=\frac{t_k^+-t_0^-}{t^+-t_0^-}<1,t_k\in D_{K_0},D_{K_0}\subset D_0.$$

The dynamic model of the process within the observation interval D_0 is determined by solving system (5) and is described by

$$\Phi_1(\tau_1)=0{,}5a_0^0+\sum_{n=n_1}^{N} a_n^0T_n^*(\tau_1);\tau_1\in D_0. \tag{6}$$

The dynamic forecasting model is based on the extrapolation of function (6) to the interval D_0^+ and is expressed by the formula

$$\Phi_2(\tau_2)=0{,}5a_0^0+\sum_{n=n_1}^{N} a_n^0T_n^*(\tau_2);\tau_2\in D_0^+. \tag{7}$$

The dynamic model of the process within the given interval $D=D_0\cup D_0^+$ based on (6) and (7) is described by the

$$\Phi_0(\tau)=\begin{cases}\Phi_1(\tau_1)\ \text{if}\ \tau_1\in D_0,\\ \Phi_2(\tau_2)\ \text{if}\ \tau_2\in D_0^+,\end{cases}.$$

Models for long-term and short-term forecast differ by both the ratio of observation and forecast intervals and the order of the Chebyshev polynomials used in the model.

Setting up the Process of Engineering Diagnostics. We will use the system of CES operation models to describe the normal operation mode of the object under the following assumptions and statements.

Each stage of CES operation is characterized by the duration and by the initial and final values of each parameter y_i determined at the beginning and the end of the stage, respectively. The variations of y_i within the stage are determined by the corresponding model.

All the parameters y_i are dynamically synchronous and inphase in the sense that they simultaneously (without a time delay) increase or decrease under risk factors.

The control $U=(U_j \mid j=\overline{1,m})$ is inertialess, i.e., there is no time delay between the control action and the object's response.

The risk factors $\rho_{q_k}^{\tau} \mid q_k=\overline{1,n_k^{\tau}}$ change the effect on the object in time; the risk increases or decreases with time.

The control can slow down the influences of risk factors or stop their negative influence on the controlled object if the rate of control exceeds the rate of increase in the influence of risk factors. The negative influence of risk factors is terminated provided that the decision is made and is implemented prior to the critical time T_{cr}. At this moment the risk factors cause negative consequences such as an accident or a catastrophe.

To analyze an abnormal mode, let us introduce additional assumptions as to the formation of the model and conditions of recognition of an abnormal situation.

The risk factors $\rho_{q_k}^{\tau} \mid q_k=\overline{1,n_k^{\tau}}$ are independent and randomly vary in time with a priori unknown distribution.

The risk factors can influence several or all of the parameters y_i simultaneously. A situation of the influence of risk factors is abnormal if at least two parameters y_i simultaneously change, without a control, their values synchronously and in phase during several measurements (in time).

The influence of risk factors will be described as a relative change of the level of control. The values of each risk factor vary discretely and randomly.

Based on acceptable assumptions, let us present additional models and conditions to detect an abnormal situation. Denote by $\tilde{y}_i$ the value of the parameter y_i influenced by the risk factors; $F_i(\rho_{q_k})$ is the function that takes into account the level of influence of the risk factors on the i th parameter y_i; ρ_{q_k} is the value of the q th risk factor at the instant of time t_k.

According to item 8, we assume that the value of $\tilde{y}_i[t_k]$ at the instant of time t_k is determined by

$$\tilde{y}_i[t_k]=\frac{1}{m}\sum_{j=1}^{m}\tilde{b}_{ij}\sum_{r=0}^{R_j}a_{jr}T_r^*(U_j);\ \tilde{b}_{ij}=b_{ij}\cdot F_i(\rho_{q_k}), \qquad (8)$$

where the function $F_i(\rho_{q_k})$ should correspond to the condition whereby $\tilde{y}_i = y_i$ in the absence of the influence of risk factors (i.e., for $\rho_{q_k} = 0$). Therefore, one of the elementary forms of the function $F_i(\rho_{q_k})$ is

$$F_i(\rho_{q_k}) = 1 - \prod_{q_k=1}^{n_{q_k}} (1 - c_{iq_k}\rho_{q_k}). \quad (9)$$

Note that risk factors can vary in time continuously (for example, pressure continuously changes as an aircraft lifts) or abruptly (for example, during cruise flight at a certain height, pressure may change abruptly at the cyclone-anticyclone interface). The most complex is the case where one risk factors vary continuously and others abruptly.

We will recognize risk situations by successively comparing $\tilde{y}_i[t_k]$ for $\tilde{y}_i[t_k]$ for several successive values of $t_k, k = \overline{1, k_0}$, where $k_0 = 3 \div 7$. As follows from item 2 of the assumptions, the condition of a normal situation is synchronous and inphase changes of $\tilde{y}_i$ for several (in the general case, for all) parameters, whence follows a formula for different instants of time t_k for all of the values of i and for the same instants of time t_k for different values of i (different parameters):

$$\operatorname{sign}\Delta\tilde{y}_i[t_1, t_2] = \ldots = \operatorname{sign}\Delta\tilde{y}_i[t_k, t_{k+1}] = \ldots = \operatorname{sign}\Delta\tilde{y}_i[t_{k_0-1}, t_{k_0}], \quad (10)$$

$$\operatorname{sign}\Delta\tilde{y}_1[t_k, t_{k+1}] = \ldots = \operatorname{sign}\Delta\tilde{y}_i[t_k, t_{k+1}] = \ldots = \operatorname{sign}\Delta\tilde{y}_n[t_k, t_{k+1}], i = \overline{1, n}. \quad (11)$$

As follows from (10) and (11), given an abnormal situation on the interval $[t_1, t_{k_0}]$, the following inequalities hold simultaneously:

- the inequality of the signs of increment $\Delta\tilde{y}_i$ for all the adjacent intervals $[t_k, t_{k+1}]$ for $k = \overline{1, k_0}$ for each parameter $\tilde{y}_i, i = \overline{1, n}$;
- the inequality of the signs of increment $\tilde{y}_i, i = \overline{1, n}$, for all of the parameters $\tilde{y}_i$ for each interval $[t_k, t_{k+1}]$, $k = \overline{1, k_0}$.

Conditions (10) and (11) are rigid; for practical purposes, it will suffice to satisfy the conditions for the representative number (3-5), which determine the parameters $\tilde{y}_i$ but not for all parameters i. The corresponding quantities in (10) and (11) are defined by

$$\Delta\tilde{y}_i[t_k, t_{k+1}] = \tilde{y}_i[t_{k+1}] - \tilde{y}_i[t_k], \quad (12)$$

where $\tilde{y}_i[t_k]$ are defined by (8); we assume that $\rho_{q_k}[t_{k+1}] > \rho_{q_k}[t_k]$ i.e., the dependence of each risk factor is a function of time, which increases, or $\rho_{q_k}[t_{k+1}] < \rho_{q_k}[t_k]$ i.e., the dependence is a decreasing function.

The practical importance of recognizing an abnormal situation based on (10) and (11) is in the minor alteration of $\tilde{y}_i[t_k]$ subject to risk factors since the "indicator" of the change is the sign of the difference in (10) and (11) rather than the value defined by (12). In other words, such an approach is much more sensitive than typical approaches used in diagnostics. Moreover, it allows "filtering" random changes and random measurement errors $\tilde{y}_i$ for separate i according to (10) or for individual $[t_k, t_{k+1}]$ according to (11).

3. Diagnostic of the circulating water system

A real circulating water system (with functional circuit shown on Fig. 3) is examined as an example of system strategy implementation for the guaranteed safety of the CTS functioning. The main purpose of the system: ensuring given water consumption $Q_1 \le 0.045$ m³/s for cooling of the technical plant (TP) (priority object) and

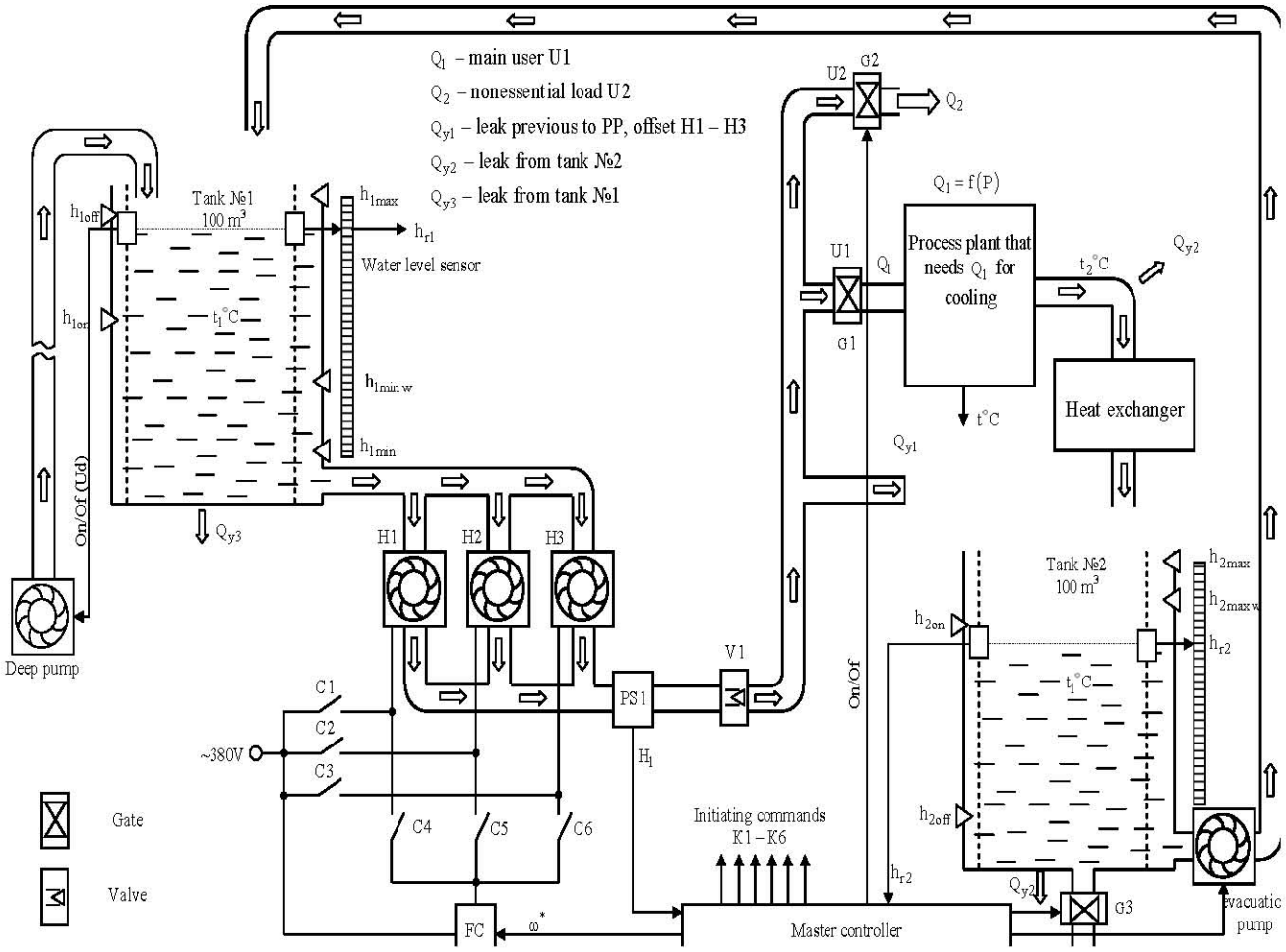

Fig. 3. A function chart of a deep water supply system

additional non-critical consumption $Q_2 \le 0.045$ m³/s used by the support equipment. The full regular consumption $Q_n = Q_1 + Q_2$.

The circulating water system consists of:

- deep-well replenishment pump;
- pump installation of three pumps, two of which are unregulated;
- pressure sensor (PS1) at the pump installation output (for the feedback of the pressure stabilization system);
- regulated gates G1, G2, G3;
- valve V1;
- water cooling system of the technological process;
- heat exchanger intended for cooling of the discharge water (e.g. water-cooling tower)
- output tank №2 for the discharge water collection;

- pump for return of the discharge water to the tank №1;
- operation controller (K1-K6);
- frequency converter (FC) for the regulated pump rotating velocity control;
- switching equipment for engaging and disengaging of unregulated pumps.

Engaging the replenishment pump occurs: if the water level in the tank №1 is lower than $h_{1on} = 50$ m^3, disengaging given $h_{1off} = 80$ m^3, if the return pump is off; if the water level is lower than $h_{1on} = 40$ m^3, disengaging given $h_{1off} = 60$ m^3, if the return pump is on. When engaged, the deep-well pump provides pump delivery $Q_{dn} = 0.05$ m^3/s. A water level sensor is installed in the tank №1, providing the h_{r1} signal. Lowering of the water level to less than 40 m^3 with engaged return pump means an abnormal mode (leak).

The water return pump is engaged when the water level in the tank №2 is higher than $h_{2on} = 80$ m^3, disengaging when lower than $h_{2off} = 20$ m^3. The return pump provides pump delivery $Q_{dn2} = 0.05$ m^3/s. A water level sensor is installed in the tank, providing the h_{r2} signal.

If the water level in the tank №1 is higher than 97 м^3 and the return pump is on, it is forced to disengage to avoid an overflow of the tank №1. Its operation is recommenced when the h_{r1} level decreases to 95 m^3.

Only the water run through the technical plant and the cooling system is put into the tank №2. After the second usage water is discharged into a sewer system.

The pump installation of the three forcing pumps (P1 – P3) is mounted to supply water to the consumers: two pumps work in regular mode, one is the emergency pump. Each pump productivity is $Q_{nn} = 0.05$ m^3/s. The pump installation works in pressure stabilization mode, which is ensured by the pressure sensor PS1. Water comes through the valve V1 into the mains system.

Overall water consumption over a small measurement time interval T_s can be determined from the tank water level change by the formula (under the hypothesis that the deep-well pump condition is invariable during the measurement time interval):

$$Q = 3600\left(h_{r(k-1)} - h_{r(k)}\right)\Big/T_s + U_{d1}Q_{dn1} + U_{d2}Q_{dn2}, k = 1,2...n\,.$$

Two consumer groups (U1,U2) with maximum regular consumption levels $Q_1 \le 0.045$ m^3/s, $Q_2 \le 0.045$ m^3/s are connected to the mains system. The water supply to the consumer U2 is not a critical factor and can be cut off by closing the regulated valve G2. The water supply to the technical plant (consumer U1) is compulsory, its failure leads to a accident.

The TP water supply needs in a regular mode are fully satisfied, i.e. necessary heat removing is assured and the TP temperature is in the permissible limit.

Temperatures up to 75 $^\circ$C are considered the permissible limit. A situation is abnormal under temperatures in range from 75 $^\circ$C до 85 $^\circ$C and emergency after the 85 $^\circ$C threshold.

The temperature is regulated by a separate PI controller, outputting the hydraulic resistance value of the gate G1 at the TP input, which, in turn, controls the water consumption in TP.

In compliance with the requirements of the developed IPED instrument, throughout the bottom of the tanks and in a number of reference points of the water system sensors were installed, providing measures every 20 seconds,

modeling time – 10000 s. The measures of the water level sensors h_{r1} и h_{r2} in the tanks №1 and №2, respectively, the head H_1 at the input of the technical plant, the temperature T of the technical plant and their arguments are provided during 10000 seconds (500 samples).

Real-time monitoring of the technical diagnostics is conducted in the water system operation process with the purpose of timely exposure of potentially possible abnormal situations and guaranteeing the serviceability of the system's functioning. In compliance with the developed methodology of the guaranteed CTS functioning safety at the starting phase $t = t_0$, functional recovery $y_i = f_i(x_1,...,x_j,...)$ is performed using N_{02} =50 given discrete samples of values h_{r1}, H_1, T, h_{r2} and their arguments. Here $y_1 = h_{r1}(x_{11}, x_{12}, x_{13})$, $y_2 = H_1(x_{21}, x_{22}, x_{23})$, $y_3 = T(x_{31}, x_{32}, x_{33}, x_{34}, x_{35})$ and $y_4 = h_{r2}(x_{41}, x_{42}, x_{43}, x_{44})$, where x_{11} is the overall water consumption; x_{12} - deep-well pump productivity; x_{13} - return pump productivity; x_{21} - overall

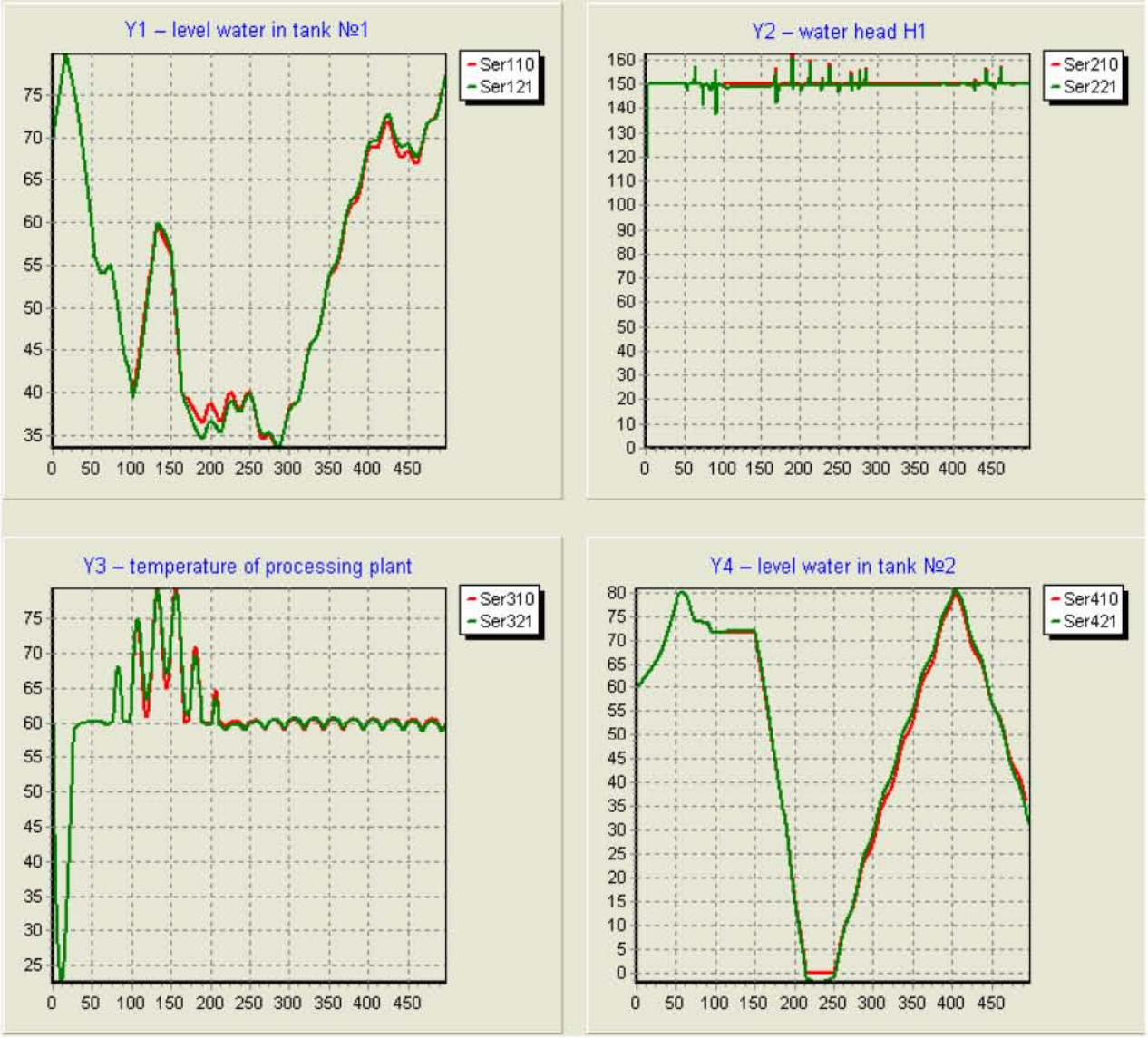

Fig.4. Distribution of the functional dependences Y1 and Y4 of the water level in the tanks №1 and №2; Y2 of the water head H1 and Y3 of the temperature of TP

water consumption; x_{22} - number of engaged pumps (1 to 3); x_{23} - regulated pump velocity; x_{31} - cooling water temperature; x_{32} - pressure H_1; x_{33} - heat loss ΔP; x_{34} - given TP temperature; x_{35} - hydraulic resistance value at the TP input; x_{42} - return pump productivity; x_{43} - valve G3 state (open valve provides water leak at 0.1 m^3/s speed); x_{44} - water pressure H_1.

Abnormal mode is caused by the heat exchanger malfunction, i.e. heated in TP water is not cooled to the necessary temperature but is returned to the tank №1. This leads to the cooling water temperature of 57° C at 3000 s time, significantly reducing its cooling quality. As a result, the TP temperature increases. At some moments the gate G1is open (minimal hydraulic resistance value), providing maximum possible water flow into TP. As these factors could cause TP overheat, a decision is made at 3000 s time to open the water drain gate G3 and to disengage the return pump. The deep-well replenishment pump injects cold water at 20 ° C temperature that gradually lowers the cooling water temperature and ceases abnormal temperature situation. At the same time the water level in the tank №1 is close to 50 m^3, which could potentially lead to an emergency situation caused by the water level in the tank №1 in case of an additional leak or a deep-well pump shutdown. Consumer U2 can be cut off if necessary. The complete escape from abnormal situation is possible only after recommencing the heat exchanger's work and engaging the return pump. The heat exchanger is assumed to be repaired at 5000 second, closing the gate G3 and permitting to engage the return pump when the water level in the tank №2 reaches h_{2on}. This happens at the time 8060 s, when the return pump starts to pump warm water into the tank №1, causing gradual cooling water temperature increase to 28 degrees.

Some results of the monitoring are presented as a time distribution of the estimated functional dependences Y1 and Y4 of the water level in the tanks №1 and №2 Y2, of the water head H1 and Y3 of the temperature of TP.

During the operation of the circulating water system, a data panel displays the diagnostic process quantitatively and qualitatively and the operator obtains the timely preliminary information on the possible transition of the water level h_{r1}, h_{r2} in the tanks №1 and №2, respectively, the head H_1 at the input of the technical plant, the temperature T of the technical plant to an abnormal mode. This allows detecting the cause in due time and making a decision on eliminating the abnormal situation, accident or catastrophe.

The analysis shows that the monitoring of the circulating water system operation by using the developed methodology of the guaranteed safety of CES operation allows making a real-time decision to ensure the survivability of the serviceability of the deep water supply system.

Conclusion

The proposed approach to estimation of guaranteed safe operation of complex engineering systems implemented as an IPED toolkit prevents the inoperativeness and abnormal situations. The real-time complex, system, and continuous estimation of the parameters of object operation detects situations that can bring the object out of the normal-mode operation. The simultaneous monitoring and integrated estimation of the parameters of a finite number of functionally dynamic parameters allow detailing the processes of object operation of any order of complexity. For situations that may cause deviations of the parameters from the normal mode of object operation, a timely decision can be made to change the mode of operation or to artificially correct some parameters to make the operation survivable. The principles that underlie the strategy of the guaranteed safety of CES operation provide a flexible approach to timely detection, recognition, prediction, and system diagnostic of risk factors and

situations, to formulation and implementation of a rational decision in a practicable time within an unremovable time constraint.

Bibliography

[1] Frolov K. V. (gen. ed.), Catastrophe Mechanics [in Russian], Intern. Inst. for Safety of Complex Eng. Syst., Moscow —1995. —389 p.

[2] Troshchenko V. T. (exec, ed.), Resistance of Materials to Deformation and Fracture: A Reference Book, Pts. 1, 2 [in Russian], Naukova Dumka, Kyiv. —1993, 1994. —702 p.

[3] Zgurovsky M. Z., Pankratova N. D., System Analysis: Theory and Applications, Springer, Berlin. —2007. — 475 p.

[4] Pankratova N.and Kurilin B., Conceptual foundations of the system analysis of risks in dynamics of control of complex system safety. P. 1: Basic statements and substantiation of approach // J. Autom. Inform. Sci. — 2001. —33, №. 2. —P. 15-31.

[5] Pankratova N. and Kurilin B., Conceptual foundations of the system analysis of risks in dynamics of control of complex system safety. P. 2: The general problem of the system analysis of risks and the strategy of its solving //J. Autom. Inform. Sci. — 2001. —33, No. 2. —P1-14.

[6] Pankratova N. D., System analysis in the dynamics of the diagnostic of complex engineering systems //Syst. Doslidzh. Informats. Tekhnol. — 2008. —No. 1. —P 33-49.

[7] Pankratova N. D. A rational compromise in the system problem of disclosure of conceptual uncertainty //Cybern. Syst. Analysis. — 2002. —38, No. 4. —P. 618-631.

[8] Lanczos C., Applied Analysis, Prentice-Hall, Englewood Cliffs, N. J. . –1956. –524 p.

[9] Remez E. Ya., Foundations of Numerical Methods of Chebyshev Approximation, Naukova Dumka, Kyiv. — 1969. — 624 p.

Authors' Information

Nataliya Pankratova *– Depute director of Institute for applied system analysis, National Technical University of Ukraine "KPI", Av. Pobedy 37, Kiev 03056, Ukraine; e-mail: natalidmp@gmail.com*

Major Fields of Scientific Research: System analysis, Mechanics of solid body, Applied mechanics, Applied mathematics, System information technology in education.