Transport and Telecommunication, 2013, Volume 14, No 2, 167–174
Transport and Telecommunication Institute, Lomonosova 1, Riga, LV-1019, Latvia
DOI 10.2478/ttj-2013-0014

THE CONCEPT DEFINITION OF MATHEMATICAL MODELLING OF THE SECURED INFORMATION-TELECOMMUNICATION SYSTEM WITH REGARD TO CONDITIONS OF THE POSTERIOR UNCERTAINTY

***Sergey Semenov*[1], *Oleksandr Dorokhov*[2], *Denys Grynov*[3]**

[1]*National Technical University "KPI", Kharkiv, Ukraine*
E-mail: s_semenov@urk.net

[2,3]*Kharkiv National University of Economics, Kharkiv, Ukraine*
E-mail: aleks.dorokhov@meta.ua; dgrynov@gmail.com

Factors, which determine the structure and the parameters of secured information-telecommunication system, have been identified. The concept of mathematical modelling of secured information- telecommunication system has been defined. Optimisation factor and criterion of information- telecommunication system have been proposed. Equations of sensitivity, which differ from the known ones by taking into account small changes in the internal parameters of the system under the influence of external factors, are clarified.

Keywords: component; mathematical modelling; information –telecommunication system; adaptive identification, information space

1. Introduction

The problem statement and literature analysis have shown [5] that technical systems can be presented as two subsystems: non-variable (invariant to external influence) and subsystem with variable (changeable) parameters. This representation gives an interpretation of variability conditions of the output coordinates according to the changes the variable subsystem parameters. In this case invariant conditions are expressed in terms of natural frequencies of the system non-variable part. Therefore one of the approaches for modelling complex technical systems is based on the interpretation of the technical characteristics of the system as the input signal and noise ability to initiate the natural frequencies of the variable part of the system. This is the approach, which takes into account the structural features (structural position, change of parameters) of external influences.

Structural-functional analysis of secured information-telecommunication systems (ITS) in [1, 2, 4, 5] allows stating that as a control object, such system is characterized by various kinds of uncertainties. Mathematical models roughness, often uncontrolled changes of the internal subsystems parameters, influence on the subsystem of uncontrollable external factors can be referred to such kind of uncertainties. Therefore some of the authors prefer to use fuzzy data and knowledge modelling tools, fuzzy selection, methods of the theory of adaptive systems in solving problems in management of information systems.

According to the sources [1–4, 7] identification theory takes one of the central places in solving synthesis of mathematical models tasks.

Analysis of the literature [1–8] has shown that a wide range of approaches is used in solution of identification of management objects in information systems problems. The most effective of these are based on the use of parametric models of dynamic systems. Some control subsystems with slowly variable and invariable parameters (management subsystems, software and mathematical supply) [6] use inertialess dynamic models (for instance trend model or regression model). But in subsystems with rapidly changing parameters (subsystems of information and technical support) inertial dynamic and neighbourhood models are widespread.

Studies [2, 7] have shown, that in case of inertialess models use, their structure is assigned as transfer functions $F(A, t)$ (trend model) or $F(A, U, t)$ (regression model). These functions are known with precision up to parameters vector $A(t)$ and input vector $U(t)$, as well as sets χ and ξ of uncontrollable and controllable disturbance (interference) variables in conformity with ($\chi(t)\in\chi\subset\Psi\subset R^q$ and $\xi(t)\in\xi\subset\Psi\subset R^n$), where $\Psi=\chi\times\xi$ is an external interference space, R_q and R_n are appropriate environmental uncontrollable and controllable structural and functional parameters of the environment. As a whole it simplifies modelling process to some degree, but it limits the range of solving problems up to static and quasi static objects management systems.

Nowadays designers increasingly turn to the methods of constructing dynamic inertia models, during modelling of complex technical systems. These methods allow solving problems of adaptive identification. It is especially important in conditions of a priori uncertainty, which is characteristic for secured information-telecommunication system. In such models cause and effect connections in structural-functional spaces R of the object under investigation on a set of posterior data $I_{an}=\left\{Y(t), U(t), \chi(t),\ \xi(t), t\in R^t\right\}$ can be described by expressions

$$S(t)=F_1(S,A_1,U,\chi,\xi,t,\tau), \tag{1}$$

$$Y(t)=F(S,A,U,\chi,\xi,t), \tag{2}$$

and a set of dynamic processes in management objects can be described by differential equation with one input and one output [2]

$$\begin{aligned}&a_0y^{(m)}+a_1y^{(m-1)}+...+a_my=\\&=b_0u^{(k)}+b_1u^{(k-1)}+...+b_ku+\xi+\chi,\end{aligned} \tag{3}$$

where $S(t)\in R^s$ is a vector of management object internal state, $\tau\in\Im$ is some time interval (time interruption), F_1, F are internal non-linear operators, the structure of which is known up to the vectors of desired parameters $A_1(t), A(t)$, belonging to restricted but a priori unknown zone (region) $G_A\subseteq R^v$, $Y(t)$ is vector of the system output parameters.

According to the expression (3) we can obtain the operator object representation through the transfer function and pass to its finite-difference representation [2].

If $t=n\tau$, where $n=0,1,...,$ τ is a data monitoring interval, and $\wp$ is a shift backward operator: $\wp y(n)=y(n-1)$.

Then

$$D_y(\wp)y(n)=D_u(\wp)u(n)+\xi(n)+\chi(n)\,, \tag{4}$$

where $D_y(\wp)=a_0\wp^m+a_1\wp^{m-1}+...+a_m$, $D_u(\wp)=b_0\wp^k+b_1\wp^{k-1}+...+b_m$.

If $\xi(n),\chi(n)$ are random sequences, then expression (4) will be an auto regression equation – slide average, and at $D_u(\wp)=1$ – a slide average model.

In case when no restrictions are imposed on management influence U and uncontrollable external influence χ, i.e. unlimited external disturbance can influence on management object (secured ITS) during the period $\tau\in J=\left[t_0,t_k\right]$, $t_0\le\tau\le t$, the equation (4) with dynamic specification for $\xi(n),\chi(n)$ can be presented as [2]:

$$\begin{aligned}&Y(t)=F(A,Y(\tau_1),U(\tau_2),\chi(\tau_3),\xi(\tau_4),\tau_i\in\left[t_{\tau_i},t\right],\\&t_{\tau_i}\ge t_0, i=\overline{1,4}.\end{aligned} \tag{5}$$

The equation (5) obtained from (1, 2) is a dynamic representation of secured ITS in space $\{U,\chi,\ \xi,\ Y\}$.

It is clear from (5), that dynamic properties of secured ITS can be determined both by its inner structure and by dynamic properties of input $U(t)$ and disturbances $\chi(t)$ and $\xi(t)$.

Studies [1–4] have shown that it is expediently to present equations (3)–(5) in matrix shape due to the use of computer facility means in management systems. Such mathematic representation of the processes, proceeding in secured ITS, makes it possible to take into account external factors which affect at the system.

2. Problem Statement of Secured ITS Mathematical Modelling

Let’s present secured ITS as a management object in the form of two subsystems set (*Q1* is static (with fixed parameters), *Q2* – dynamic (with variable parameters)), and also in the form of the system state coordinates matrix *X*.

In this case for dynamic (non-linear) object of management, which is secured ITS, the equation in state space assumes the following form:

$$\overline{X}_1 = A_{1,1}X_1 + \Phi(X_1) + A_{1,2}X_2 + BU + \Phi_1(E\chi) + Z\xi \, , \tag{6}$$

$$\begin{gathered} Y = C_{1,1}X_1 + C_{1,2}X_2 + \Phi_2(X_2) + \\ + C_{1,3}\overline{X_2} + DU + \Phi_1(E\chi) + Z\xi + \zeta , \end{gathered} \tag{7}$$

where $\overline{X}_1$ is a measurable state vector of the subsystem *Q1* of object, $A_{1,1} \in A \in R^{mxm}$ is a state vector of the subsystem *Q1*, A is a state matrix, $X_1 \in R^{1\times m}$ is a subsystem *Q1* state coordinates vector, $A_{1,2} \in A \in R^{mxm}$ is a subsystem *Q2* state vector, $X_2 \in R^{1\times m}$ is a state coordinates vector of the subsystem *S₂*, $\chi \in R^{1\times m}$ is a vector of non-controllable external influence, $U \in R^{1\times k}$ is an input vector, $Y \in R^{1\times n}$ is an output vector, $C_{1,1} \in C \in R^{n\times m}$ is an input vector of the subsystem *Q1*, $C_{1,2} \in C \in R^{n\times m}$ is an input vector of the subsystem *Q2*, $C_{1,3} \in C \in R^{n\times m}$ is a vector characterizing connection between subsystems *Q2* and *Q1*, $\overline{X}_2$ is a measurable state vector of the subsystem *Q2* of object, $C \in R^{nxm}$ is an unobservable matrix of the system functioning inner errors, $B \in R^{mxk}$, $E \in R^{nxm}$, $Z \in R^{nxm}$, $D \in R^{nxk}$, $\zeta \in R^n$ are unobservable vectors of the measurement errors, $\Phi : R^n \times R \to R^n$, $(\Phi_1 : R^n \times R \to R^n)$, $(\Phi_2 : R^n \times R \to R^n)$ are non-linear vector functions.

If matrices A, B, C, D, E, Z are parameterised with accuracy up to some conditional vectors *AA, BB, CC, BD, EE,* Z_Z then expression (6) will present itself as a condition equation, and expression (7) will be a measurement (observation) equation.

The generalized structure of the system under consideration is presented on Figure 1.

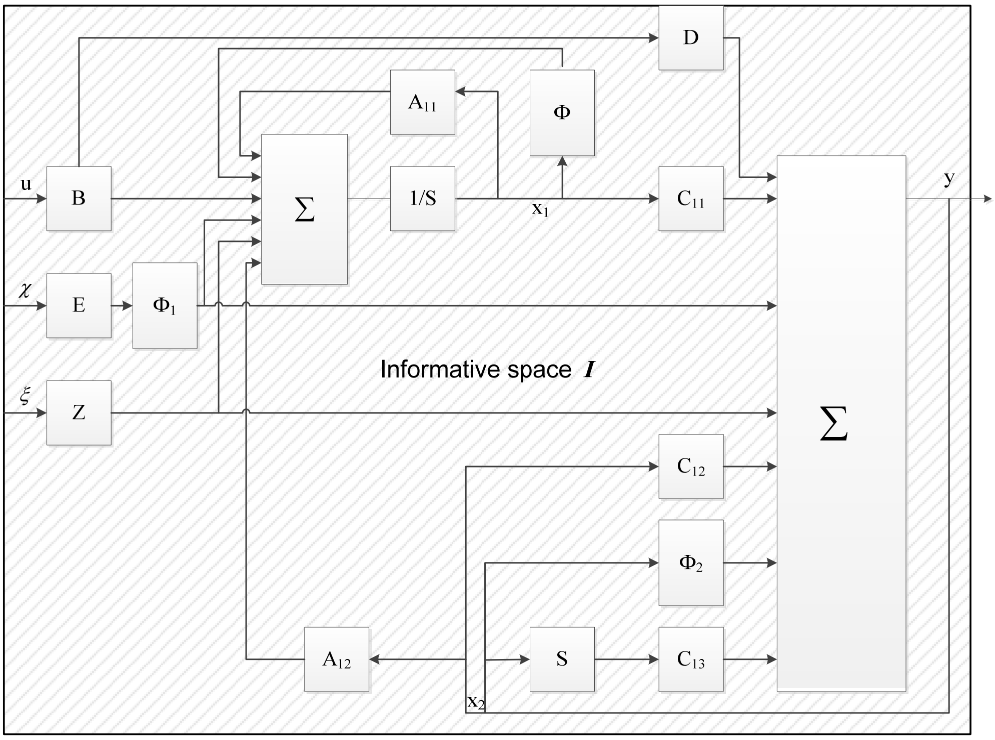

Figure.1 Generalized block diagram of non-linear object of control in ITS

The Figure 1 shows that the set of input signals spaces *U*, conditions *X*, external influences $\Psi = \chi \times \xi$, system parameters S, and also non-linear vector functions *Φ*, *Φ1*, *Φ2* forms information space of the management objects in secured ITS:

$$I = U \times X \times \Psi \times J \times S \times \varPhi \times \varPhi_1 \times \varPhi_2,$$

where J is an observation interval for management object in a secured ITS.

In practice information space I is not completely observable and thus it is covered by some information set I, which contains available to measure sets U, χ, ξ and X.

In this case the set I is collection of vectors $U(t) \in U$, $\chi(t) \in \chi \subset \Psi$, $\xi(t) \in \xi \subset \Psi$, $Y(t) \in Y \subseteq X$, observable at J,

$$I_{an} = \{ U \in U \ , \ \ \chi \in \Psi, \xi \in \Psi \ , \ \ Y \in R^{m \times n} \ |U(t), \ \ \chi(t), \ \ Y(t), \ \ t \in J\},$$

where I_{an} is the set of measurable (posterior) data.

However, studies have shown, that for a complete description of the secured ITS it is necessary to include prior information about possible external signals, factors and corresponding disturbances and variations in secured ITS together with I_{an} in the set I. So it is expediently to present I as:

$$I = \{I_{an}, I_a\},$$

where I_{an}, I_a are appropriate sets of measurable (posterior) and a prior data about protected ITS condition.

It should be noted that it is expediently to regard the set ξ of controllable external disturbances as predictable (known a priori) part of information space I, and corresponding vector $\xi(t)$ – as element of the set I_a to simplify mathematic model of secured ITS.

Then characteristics of ITS secure to external influences can be analysed on the example of the following system:

$$\overline{x(t)} = A(t)x(t) + B(t)u(t) + E(t)\chi(t), \tag{8}$$

$$y(t) = C(t)x(t) + D(t)u(t) + E(t)\chi(t) + \zeta(t), \tag{9}$$

$$x(t_0) = x_0, \tag{10}$$

where $x(t) \in X$ is an m-dimensional state coordinates vector of the system, $u(t) \in U$ is a *k*-dimensional control vector, $A(t), B(t), E(t), C(t), D(t), \zeta(t)$ are continuous matrices of unobservable measurement errors, $\chi(t)$ is an m-dimension vector of uncontrollable external influences.

System protection characteristic can be regarded both concerning external disturbances and concerning a reconstruction of system inner parameters (fine adjustment). In the first case invariance of the output coordinates to external influences $\chi(t)$ should become the final result, in the second case – to small variations of matrix parameters $A(t), B(t), E(t), C(t), D(t), \zeta(t)$.

Thus, the speculation about the connection between the property of ITS secure and the property of its invariance to external influences, or parametric insensitivity is proposed in the problem statement of mathematical modelling.

Let us assume that matrices $A(t), B(t), E(t), C(t), D(t), \zeta(t)$ are related to some parameters $p = (p_1, p_2, \ldots, p_n)$. If p is constant and equal p_0, then the set of simultaneous equations (8–10) will have a unique solution $x(t)$ or $y(t)$ at any $u(t)$ and $\chi(t)$, determined at $t \in \left[t_0, t_f\right)$. Small variation of vector state X and output coordinate $\delta\, y(t)$ arises at small parameter changes p_0 ($p_0 + \Delta p$).

Small variables influence can be analysed by the sensitivity functions:

$$\dot{U}_j = A(t)U_j + \frac{df}{dp_j}, \quad (j = 1, \ldots J), \tag{11}$$

$$\dot{\chi}_j = E(t)\chi_j + \frac{df}{dp_j}, \quad (j = 1,\ldots J), \tag{12}$$

where $f \equiv A(t)x(t) + B(t)u(t) + E(t)\chi(t)$, and functions U_j and χ_j are graded as:

$$U_j = \frac{dx}{dp_j}, \; \chi_j = \frac{d\dot{x}}{dp_j}.$$

Along with it:

$$\delta x(t_f) = \overline{\Phi}(\aleph_U(t_f)\delta p + \aleph_\chi(t_f)\delta p), \tag{13}$$

$$\delta y(t_f) = \overline{\Phi_1}\begin{bmatrix} C(t_f)\left[\aleph_U(t_f)\delta p\right] + \\ +D(t_f)\left[\aleph_U(t_f)\right] + \\ +E(t_f)\left[\aleph_\chi(t_f)\right] \end{bmatrix}, \tag{14}$$

where $\aleph_U$ and $\aleph_\chi$ are sensitivity matrices:

$$\aleph_{\mathrm{U}} = \begin{vmatrix} u_{11} & . & . & . & u_{1j} \\ . & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & . \\ u_{n1} & . & . & . & u_{nj} \end{vmatrix}, \quad \aleph_\chi = \begin{vmatrix} \chi_{11} & . & . & . & \chi_{1j} \\ . & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & . \\ \chi_{n1} & . & . & . & \chi_{nj} \end{vmatrix},$$

$\overline{\Phi}$ and $\overline{\Phi}_1$ are non-linear vector functions.

If one of the vector $\delta y(t_j)$ components or all of them are equal to null, the system (partly or correspondingly fully) will be called parametrically insensible. If matrices of sensitivity $\aleph_U$ and $\aleph_\chi$ are square ($N = J$), then the system controllability analyses will be reduced to degeneration of the matrices $\aleph_U$ and $\aleph_\chi$.

Hence the following theorems are claimed.

Theorem 1. ITS will be protected and controlled, if its output vector $y(t)$ values are fully invariant to input influences $u(t)$ and $\chi(t)$.

Theorem 2. The output Y of secured ITS will be fully controllable, if the sensitivity of matrices lines $\aleph_U$ and $\aleph_\chi$ are linearly independent.

Dos-attack emulation from three directions has been performed to assess the adequacy of mathematical models in the anomalous operation mode. In this case, the node 4 is the main source of malicious traffic. Besides the node 4 uses nodes 2 and 3 for the parallel generation of malicious traffic with the use of malicious software (Hping 2 and Server Attack By-C-4), pre-established on these sites.

The results of the study of mathematical and simulation model of ACPP in the anomalous operation mode are shown on Figures 2, 3 (graphs of the "experimental" (Figure 2 a) and the "theoretical" (Figure 3 a) usage of the CPU of computer systems (Z_1, Z_2, Z_3) from the time of operation of nodes in anomalous conditions ($mean\left(\hbar_i\left(t\right)\right) / mean\left(f\left(x_1, u_1, t\right)\right) \approx 16$), and the density distribution histograms of the random variable Z_i, which have been obtained from the experiment (Figure 2b) and mathematical modelling (Figure 3 b)).

The evaluation of the adequacy of developed mathematical model ACPP in conditions of external destructive influences has been made as in the previous example (by consent of Pearson). The results of this assessment are presented in Table 1.

As it is shown in Table 1, all the numerical values of the criterion in the given conditions is less than "table" values of the Pearson criterion. This fact indicates the correctness of the hypothesis and, therefore, the adequacy of the developed mathematical model ACPP in anomalous operating conditions.

Let's compare the results of mathematical modelling ACPP, which are obtained using the developed model, with the results of the Lenzheven model in the mode of anomalous operating conditions. For this purpose let's verify the hypothesis of the coincidence of the distribution of "theoretical" (by Lenzheven) and "experimental" general set of values obtained by permission of Pearson just as in the previous example.

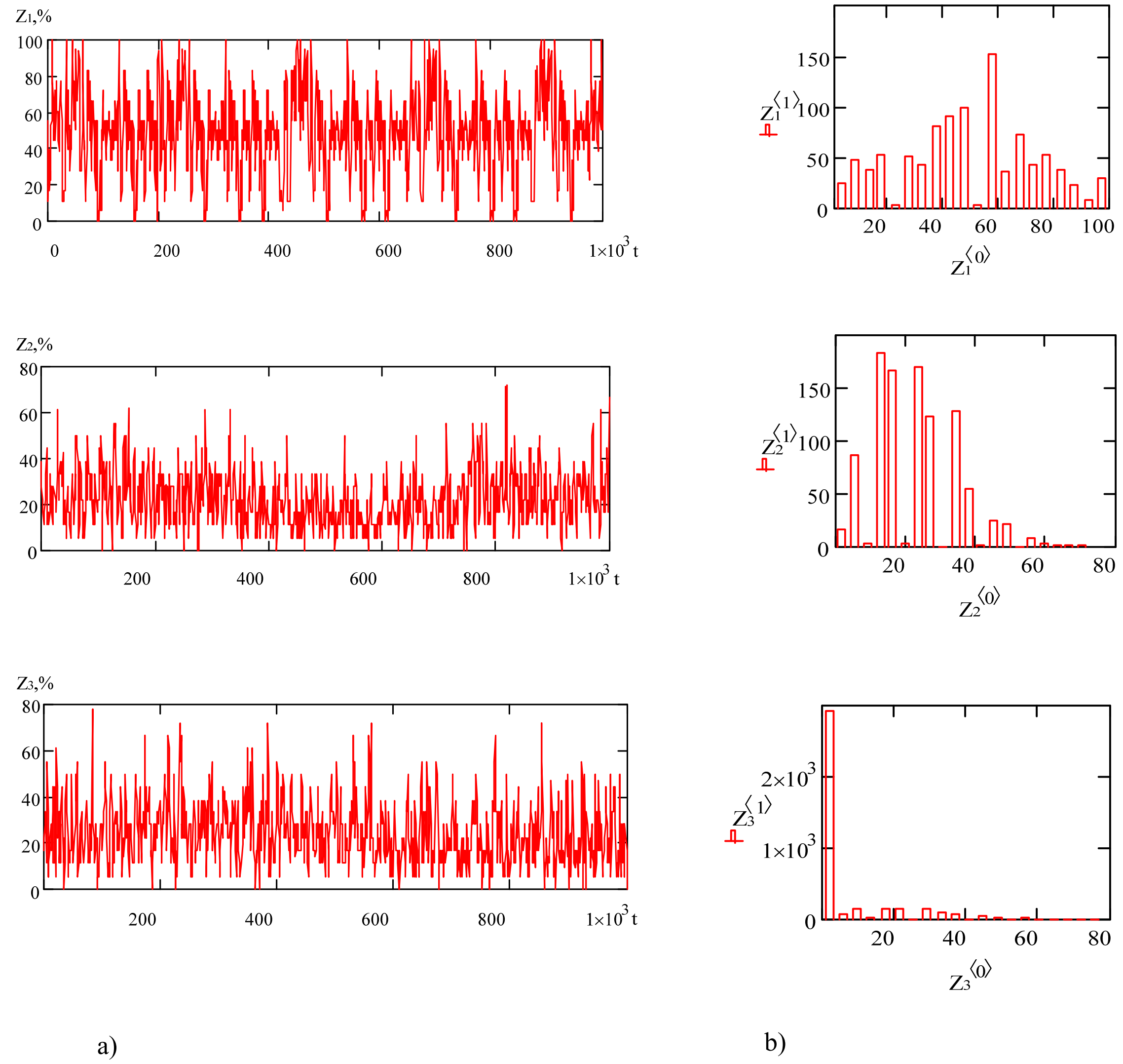

Figure 2. Graphs of the "experimental" usage of the CPU of computer systems from the time of operation of nodes in anomalous conditions

Table 2 shows the results of suggested hypothesis verification for the equations of Lenzheven in anomalous operating conditions.

Thus, the obtained above estimates of investigated models suggest that the use of the developed model ACPP improves the accuracy of the results compared with the Lenzheven model to 10% in given conditions.

System conduct dependence from external factors (sensitivity) is an important characteristic of the secured ITS. Along with this data, that is comprised in sensitivity matrices, are the components of the set I_a of priori information about secured ITS. At the same time, according to analyses, an accuracy of decision-making of the necessary adjustment of the system internal parameters depends not only on the analysed priori (I_a), but also on posterior (I_{an}) information about the state of the ITS security.

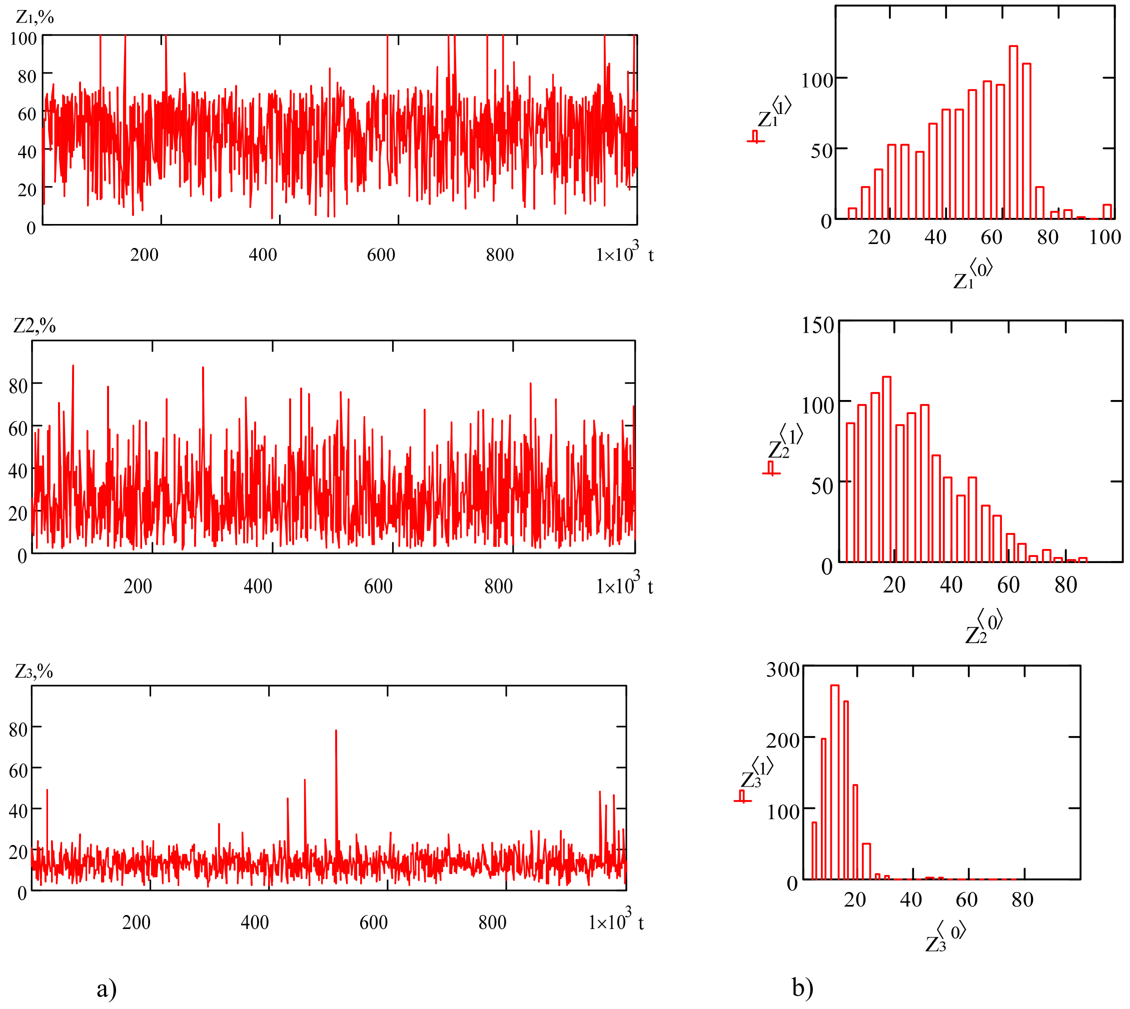

Figure 3. Graphs of the "theoretical" usage of the CPU of computer systems from the time of operation of nodes in anomalous conditions

Table 1. The results of the test of suggested hypothesis in anomalous operating conditions

N of the node	1	2	3
The number of degrees of freedom	4		
The level of significance	0,975		
"Table" Pearson criterion K	0,484		
"Measured" Pearson criterion K_{meas}	0,305194	0,405687	0,027477

Table 2. The results of suggested hypothesis verification for the equations of Lenzheven in anomalous operating conditions

N of the node	1	2	3
"Measured" Pearson criterion K_{meas}	1,86164	1,54982	1,04523

Let's carry out the choice of secured ITS optimisation index in terms of I_{an} and I_a. For this we assume that measurement and analysis of data $I_{an}(t), \forall t \in J$ can be carried out, the set I_s of generalized quantitative estimates for the elements of the set I_{an} and the set I_ψ of input data perturbations can be formed according to the current level of prior information I_a, status and sensitivity characteristics values of matrices $\aleph_U$ and $\aleph_\chi$.

Data $I_{an}(t)$ analysis of the set I_{an} can be carried out both a priori and in the course of solving identification tasks (revealing of secured ITS structural and parametrical singularities). The sets I_{Ω_A} and

I_{Ω_s} of additional estimation information about an object restrictions and characteristics are formed as a result of this analysis. Moreover, $I_{\Omega_A} \subset I_{\Omega_s}$, and Ω_A – is restricted but a priori unknown system of inner parameters mode (range).

We will choose the system time functioning characteristic in the safety mode $T_{without}(I_{an})$ as the index of ITS protection level.

Under safe operating conditions of the ITS we will understand such mode of operation, which provide basic security services (confidentiality, authenticity, integrity, access control, involvement).

Let's present chosen ITS level protection index as functions:

$$T(I_{an}) = T(A \in R^{m\times m}, U \in U\ , \chi \in \Psi\ , t \in J\ \big| A \in \Omega_A, U \in I_s, \chi \in I_\psi) .$$

After this we can formulate the optimisation task proceeding on the assumption that values of the sensitivity matrices $\aleph_U$ and $\aleph_\chi$ enter into set I_a .

It is necessary to find such conversion F of set I_{an} and additional data I_{Ω_A} , I_{Ω_s} and I_ψ about secured ITS to provide maximization of system time functioning in safe mode at prescribed level of a priori information I_a :

$$\forall t \in J\ ,\quad F : \mathrm{I}_{\text{an}} \times I_a \to \mathrm{I}_{\text{an}} \times I_s \Rightarrow \max_{I_s, I_\psi} T(I_{an}) . \qquad (15)$$

It is clear from (15) that optimisation task solving should be considered from system position. And one of the system functions has to be at the set I_{an} analysis with a view to the synthesis of evaluation method, which takes into consideration real conditions of secured ITS functioning the most completely. Conversion F is interpreted in the wide sense and presents operators cortege, collection of algorithms, techniques and procedures, which allow realizing them into conversions chain in 15. According to this attention should be directed on the fact that the use of prior data I_a as a whole and sensitivity matrices $\aleph_U$ and $\aleph_\chi$ data in particular will allow reducing class of conversions F .

3. Conclusions

Thus, characteristic peculiarities of secured ITS have been revealed as a result of analyses. It has allowed to work-out the mathematical modelling conception and to formulate the statement of the problem, which consists of finding the function maximum of the system operation time in safety mode.

References

1. Khalil, H. K. (2002). *Nonlinear Systems*, 3rd Edition. Upper Saddle River, NJ: Prentice Hall.
2. Semenov, S. G., Klimov, S. B., Engalichev, S. O. (2011). The modern approach to the synthesis of secure information technology systems of integrated type. *Management systems, navigation and communication*, 2(18). 265–268. (In Russian)
3. Semenov, S. G., Davydov, V. V. (2011). A dynamic model of information system based on the observed structure-information portrait. *Journal of the National Technical University «HPI»*. 36, 156–163. (In Russian)
4. Semenov, S. G. (2011). Structural and functional analysis of modern information systems with the development of a comprehensive indicator of the effectiveness of their operation. *Information Processing Systems,* 2(18), 145–150. (In Russian)
5. Semenov, S. G., Smirnov, A. A., Meleshko, E. V. (2012). *Models and methods of network management for telecommunication systems and networks.* Monograph. Kharkiv: NTU «HPI». (In Russian)
6. Tomovich, R., Vukobratovich, M. (1972). *The general theory of sensitivity*. Sov. Radio. (In Russian)