Method of analysis the functional stability of the software of the infocommunication system in cyber-attack conditions

Sergey S. Kochedykov
Candidate of Technical Sciences, Associate Professor
Voronezh institute of the Federal Penitentiary Service
Irkutskaya St., 1, Voronezh, Russia, 394072
infosec36@mail.ru

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

Sergey Yu. Kobzistyy
Candidate of Technical Sciences, Associate Professor
Voronezh institute of the Federal Penitentiary Service
Irkutskaya St., 1, Voronezh, Russia, 394072
akobzuk@yandex.ru

Pavel V. Markin
National Research University of Electronic Technology
Shokin Square, 1, Zelenograd, Moscow, Russia, 124498
mrkinp@bk.ru

CEUR-WS.org/Vol-2514/paper115.pdf

Abstract: The paper proposes a new method for analyzing the functional stability of software, information and communication systems, which allows to evaluate the systems performance and take into account external and internal destructive effects caused by cyber attacks. In the paper, a criterion of functional stability is formulated using the theory of integro-differential calculus and the theory of fuzzy sets, a quantitative and qualitative method for analyzing the functional stability of software, information and communication systems is developed.

Keywords: information and communication systems, cyberattack, functional stability, method of analysis.

Introduction

Applications in all fields of information and communication systems have contributed to the fact that the attackers for decades, actively committed various crimes in the sphere of high technologies [1]. Currently, they are actively developing various cyber-attacks that affect the information security of critical information infrastructure throughout the country.

Under the cyber attacks should understand targeted information and technical impact using tools and capabilities of information and other technologies unauthorized destructive impact of the attacker on the objects of a global network, on the processes of its functioning, violating the stability of its operation and its information security [2-5]. Thus, as information technology impact can make cyber attacks, financial damage from which is very significant. The financial

Copyright © 2019 for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

damage caused by cyber-attacks [5] show that existing solutions for information security, not fully able to protect against this type of attack [5-6].

To protect from these threats is currently developed and widely used various systems to detect and counter cyber attacks [7, 8]. However, such systems do not account for the functional stability of the software infocommunication systems under conditions of cyber attacks that does not allow to build system of diagnosing and implement recovery information and communication systems.

1 Formulation of the problem

Under the functional sustainability of information and communication systems will understand their ability to perform their functions in the presence of the destructive factors of different nature. Interest in the analysis and evaluation of the functional stability of the software infocommunication systems emerged simultaneously with the emergence of complex systems [9-10]. The approach to solving this problem was originally based on the identification of the concepts "reliability" and "stability" and was to transfer well-known statistical methods of classical reliability theory into a new soil. In methodological terms, this approach differed little from the estimation of the reliability of technical devices. With minor modifications it remains up to the present time.

However, with the development of information technology, especially in the direction of the need to protect them from external destructive influences, due to the large number of types of cyber attacks [11], it is understood that the theory of reliability in relation to the assessment of sustainability software infocommunication systems in terms of destructive effects has a conceptual incompleteness. First of all, in this theory, the dominant factors in determining the reliability of systems that are random defects and errors in their design, development and operation, and factors of destruction of special software modules at the expense of purposeful influences virtually invisible to researchers. In addition, the identification of the concepts "reliability" and "sustainability" often leads to fuzzy identification of causes of failures in the operation of information communication systems: internal destructive effects are taken for external and Vice versa. As a result of difficult implementation measures for the detection, identification and monitoring of destructive impacts on the objects of information and communication systems. In view of the foregoing problem of analyzing the sustainability of information and communication systems in terms of destructive impacts are relevant both in theoretical and in practical terms.

The aim in this section is to develop a method for solving this problem. The specific objectives of the study are as follows:

- choose a representative criterion for evaluating the stability of software infocommunication systems in terms of destructive influences, reflecting both random and targeted (intentional) nature of these impacts;
- to develop a method to analyze the functional stability of the software infocommunication systems in terms of destructive impacts according to the introduced criterion.

2 Criteria for functional stability of the software infocommunication systems

To select a representative criterion for evaluating the functional stability of the software infocommunication systems in terms of destructive effects, we introduce into consideration the following continuous and differentiable function $E_1(t),\ldots,E_N(t)$, characterizing the current functionality of each software module included in the software infocommunication systems N – the total number of the software module in the software infocommunication systems; t – the current time. To measure the values of these functions and giving them physical meaning, we introduce into consideration $[0,1]$ - a scale with interval gradations $[0 \div k_1)$, $[k_1 \div k_2)$ and $[k_2 \div 1]$, which will be interpreted in the following way: if $E_i(t) \subset [0 \div k_1)$, then the i-th software module subjected to destructive effect ceases to perform its function ("unhealthy") $E_i(t) \subset [k_1 \div k_2)$, then the i-th software module subjected to destructive exposure, continues to perform its function, but not in full ("working part") $E_i(t) \subset [k_2 \div 1]$, then the i-th software module subjected to destructive exposure, continues to perform its function in full ("healthy". Let: $\mu_{1i}(t)$ – the probability that $E_i(t) \subset [0 \div k_1)$; $\mu_{2i}(t)$ – the probability that $E_i(t) \subset [k_1 \div k_2)$; $\mu_{3i}(t)$ – the probability that $E_i(t) \subset [k_2 \div 1]$, when the normalizing condition: $\frac{1}{N}\sum_{i=1}^{N}(\mu_{1i}(t)+\mu_{2i}(t)+\mu_{3i}(t))=1$. Then the criterion of stability of functioning of the software infocommunication systems in terms of destructive effects can be written in the following form:

- if $\frac{1}{N}\sum_{i=1}^{N}\mu_{3i}=1$, the software operates steadily, that is, in spite of the destructive effects, the system is able to perform its functions in full;
- if $\frac{1}{N}\sum_{i=1}^{N}\mu_{1i}=1$, the software operates extremely unstable, that is, destructive effects led to the fact that the system has lost the ability to carry out its functions;

- if $\frac{1}{N}\sum_{i=1}^{N}\mu_{2i}(t)=1$, the software operates is unstable, that is, destructive effects led to the fact that the system has partially lost the ability to carry out its functions. Note two circumstances associated with the use of criteria. First, the essence does not change when you assign more or fewer gradations on the evaluation scale functions $E_1(t),\ldots,E_N(t)$ when one changes the threshold intervals $[0\div k_1)$, $[k_1\div k_2)$ и $[k_2\div 1]$. The selection of these parameters is the subject of the agreement and should be in the process of assessing the sustainability of individual information and communication systems with the features of its construction and functions. Secondly, when using this criterion, the effect of destructive impacts on software infocommunication systems is reflected via the changes of values of functions $E_1(t),\ldots,E_N(t)$ therefore the main objective of sustainability appraisal is to assess the current functionality of the software modules of the software infocommunication systems in terms of destructive impacts, expressed by the functions $E_1(t),\ldots,E_N(t)$

3 The analysis of the current functionality of the software modules of information and communication systems. A quantitative approach

We proceed from the fact that the process of functioning of each software module in the software infocommunication systems without taking into account its links with other modules occurs according to the logistic law that is formally expressed by equations of the following form:

$$\frac{dE_i(t)}{dt}=E_i(t)\rho_i\left(1-E_i(t)\right);\quad i=\overline{1,N}, \tag{1}$$

where N – the number of the software module in the software; ρ_i – the dimensionless coefficient characterizing the ability of the i-th program module to increase its functionality $(0<\rho_i<1)$, the greater the value, the faster this module comes into operation after a stop.

This means that the functionality of each software module without taking into account its links with other modules change over time along an S-curve with saturation $E_i(t)=\left(1-\frac{E_i^0-1}{E_i^0 e^{\rho_i(t-t_0)}}\right)^{-1};i=\overline{1,N},$ which is the solution of equation (1) in which the symbol $E_i^0\left(0<E_i^0<1\right)$, designated starting functionality of the i-th program module at a time t_0.

Let result destructive influences in software infocommunication systems were implemented "K" malicious software modules. In response to this, in the same software environment was introduced by the "M" modules that can find and eliminate (block) malicious modules. We also assume that:

– the functionality of malware and blocking software modules without regard to their relations with other modules change over time by the same law, and functionality of software modules from the software infocommunication systems, that is, for all $i=(N+1),\ldots,K$ и $i=(K+1),\ldots,M$ true:

$$\frac{dE_i(t)}{dt}=E_i(t)\rho_i\left(1-E_i(t)\right);\quad i=\overline{(N+1),K};i=\overline{(K+1),M},$$

and, accordingly,

$$E_i(t)=\left(1-\frac{E_i^0-1}{E_i^0 e^{\rho_i(t-t_0)}}\right)^{-1};\quad i=\overline{(N+1),K};i=\overline{(K+1),M},$$

where all components have the same meaning as before.

- the mutual influence of software module (native and introduced by cyber criminals) on the functionality of each other in proportion to their current functionality, that is, for all $i=1,2,\ldots,N$ the relation is valid:

$$f_i\left(E_1(t),\ldots,E_{N+K+M}(t)\right)=E_i(t)\rho_i\left(1-\rho_i\sum_{j=1}^{N+K+M}c_{ij}E_j(t)\right);\quad i=\overline{1,N+K+M}, \tag{2}$$

where $c_{ij}(-1\le c_{ij}\le 1)$ and $(c_{ij}=1,i=j)$ – the coefficients absolute values of which serve as a measure of the relative influence of software module at each other, and their meaning is as follows:

— if $c_{ij}=0$ and $c_{ji}=0$, between i-th and j-th the software module is no interference, and therefore, the functionality of one software module does not depend on the state of other, in particular, may be that cybercriminals introduced malicious modules do not affect the operation of the software infocommunication systems, and blocking modules do not affect the work of malware;

— if $c_{ij} < 0$ and $c_{ji} < 0$, between i-th and j-th software module there is a mutually destructive influence, and the results of their functioning will depend on the nature of this influence, that is, from the absolute values of the coefficients c_{ij} and c_{ji}; such a situation may occur, for example, when cybercriminals introduced malicious modules have a negative impact on the operation of the software infocommunication systems, and means of struggle in turn inhibit the operation of malicious programs;

— if $c_{ij} > 0$ and $c_{ji} > 0$, between i-th and j-th a software module has a mutually beneficial effect, and the results of their functioning will depend on the nature of the facilitating relationship, that is, from the absolute values of the coefficients c_{ij} and c_{ij}; such a situation may occur, for example, when the software modules information and communication systems support the functioning of each other, or when the anti-malware programs help each other to solve the problem of blocking these programs;

— if $c_{ij} < 0$ and $c_{ji} > 0$ or $c_{ij} > 0$ and $c_{ji} < 0$, then i-th and j-th the software module simultaneously have on each other both useful and destructive impact, and the results of these effects will depend on the absolute values of the coefficients c_{ij} and c_{ji}; such a situation may occur, for example, then, the operation of the software module occurs in conditions of destructive impacts, which influence can be both positive and destructive, depending on the coefficients c_{ij} and c_{ji};).

Given the assumptions made and assumptions the operation of the software infocommunication systems in terms of destructive effects can be described by a system consisting of $(N + K + M)$ equations:

$$\begin{aligned} &\frac{dE_i(t)}{dt} = E_i(t)\rho_i\left(1 - \sum_{i=1}^{N+K+M} c_{ij}E_j(t)\right)\left(i = \overline{1,(N+K+M)}\right) \\ &E_i(t_0) = E_i^0\left(i = \overline{1,(N+K+M)}\right). \end{aligned} \tag{3}$$

Given the necessary initial data and solving the system of equations (3) numerically (using, for example, Mathcad), we assess the current functionality of the software modules $E_1(t), \ldots, E_N(t)$ depending on the nature of destructive impacts, defined by the matrix $\|c_{ij}\|, i = \overline{1,(N+K+M)};\ j = \overline{1,(N+K+M)}$.

Above it was assumed that the mutual influence of software module on the effectiveness of each other is described by a linear function (2). Let us consider the case where this effect is non-linear. In this case instead of (3) have:

$$\begin{cases} \dfrac{dE_i(t)}{dt} = E_i(t)\varphi_i\left(E_1(t),\ldots,E_{N+K+M}(t)\right); \\ E_i(t) \le 1; E_i(0) = E_i^0; \left(i = \overline{1,(N+K+M)}\right). \end{cases} \tag{4}$$

where the functions $\varphi_i\left(E_1(t),\ldots,E_{N+K+M}(t)\right); \left(i = \overline{1,(N+K+M)}\right)$ Express the nonlinear interdependence of functionality of the software module information and communication system is susceptible to destructive influences.

Let consider the system of equations (4) has a unique positive solution $\left(E_1^*(t),\ldots,E_{N+K+M}^*\right)$, the corresponding point of intersection of the graphs of functions $E_i(t) = f_i\left(E_1(t),\ldots,E_{N+K+M}(t)\right); \left(i = \overline{1,(N+K+M)}\right)$. Then, for stable stationary equilibrium (4) is enough to satisfy the inequality:

$$\bigvee_{i=1}^{N}\left(\frac{df_i\left(E_1(t),\ldots,E_{N+K+M}(t)\right)}{dE_i(t)} > \frac{df_{i+1}\left(E_1(t),\ldots,E_{N+K+M}(t)\right)}{dE_i(t)}\right). \tag{5}$$

Applying the rule of differentiation for implicit functions, we come to the inequality:

$$\bigvee_{i=1}^{N+K+M}\left[\begin{array}{l} \left|\dfrac{\partial f_i\left(E_1(t),\ldots,E_{N+K+M}(t)\right)}{\partial E_i(t)} \cdot \dfrac{\partial \varphi_{i+1}\left(E_1(t),\ldots,E_{N+K+M}(t)\right)}{\partial E_{i+1}(t)}\right| > \\ > \left|\dfrac{\partial f_i\left(E_1(t),\ldots,E_{N+K+M}^{RE}(t)\right)}{\partial E_{i+1}(t)} \cdot \dfrac{\partial \varphi_{i+1}\left(E_1(t),\ldots,E_{N+R+M}(t)\right)}{\partial E_i(t)}\right| \end{array}\right],$$

or in other notation:

$$\forall_{i=1}^{N+K+M}\left[\left|\omega_{ii}\cdot\omega_{(i+1)(i+1)}\right|>\left|\omega_{i(i+1)}\cdot\omega_{(i+1)i}\right|\right] \quad (6)$$
$$(0<\omega_{ii},\omega_{(i+1)(i+1)},\omega_{i(i+1)},\omega_{(i+1)i}\le 1),$$

where $\omega_{ii},\omega_{(i+l)(i+l)}$ and $\omega_{l(i+l)},\omega_{(i+l)i}\sqrt{b^2-4ac}$ – the coefficients characterizing the change in functionality of the software module.

The meaning of the inequality (5) is the following: to ensure sustainable operation mode of the information communication systems in terms of the destructive impacts it is necessary that the joint effect of implementation of all measures for the protection of software (expressed by the left part of inequality (5)), dominated the cumulative effect of malware (expressed right-hand side of inequality (5)).

Difficulties of practical realization of the above-mentioned methods are associated primarily with the need for timely receipt of source data required for the solution of systems of differential equations (3)-(4). In addition, the process of solving a large number of interrelated differential equations (of the order of 150-500 equations) are not always successful. In these cases, the aid comes a qualitative approach to the evaluation of the sustainability of information and communication systems in terms of destructive impacts, based on experts.

4 A qualitative approach

In this case, the probability $\mu_{ji}(t)$ will be interpreted as membership functions of the current state of the software module to one of the three selected grades are: "unhealthy", "healthy", "working partially", and thus used to obtain their estimates of the theory of fuzzy sets, namely, those sections where we are talking about methods of fuzzy expert evaluation.

There are several expert methods for constructing membership functions. The most adequate for solving security problems should be recognized the method of pairwise comparisons or the method of Saaty. The essence of this method in our case is the following. The group of experts consisting of four persons proposed to evaluate the membership function value $E_i(t)$, characterizing the degree of protection of the i-th object of infocommunication systems from unauthorized access at time t, to the evaluation gradations $\left[0 \div k_1\right)$, $\left[k_1 \div k_2\right)$ и $\left[k_2 \div 1\right]$), using the scale presented in table 1.

Table 1 – Scale of Saaty

Rating	Qualitative assessment	Description accessories
1	Of equal importance	The degree of belonging of the same
3	Weak superiority	The arguments about the preference of one element over another is unconvincing
5	The significant superiority	There is strong evidence of preference of one element over another
7	Obvious superiority	Convincing evidence for the preference
9	Absolute superiority	Evidence of the superiority of one element over another is undeniable
2,4,5,5	Intermediate value between adjacent ratings	Compromise

Their assessment of the expert is in the form of pairwise comparison matrix $A=\left\|a_{ij}\right\|$, the elements of which a_{ij} show the degree of belonging of element standing in the i-th row and j-th column, to the numerous in comparison with the item standing in the j-th row and i-th column. If the expert in their assessments not allow logical contradictions, then the matrix elements will be related by the ratio $a_{ij}=1/a_{ji}$. If we now find the eigenvector λ algebraic system of equations $Aw=\lambda w$ (or in another form $(A-\lambda E)w=0$, where E – the identity matrix, i.e. a matrix where the main diagonal filled with ones, and all the other terms equal 0), then we can calculate the components of the eigenvector w, which characterize the membership function of this element. Let the results of a survey of experts and use the scale of belonging (table. 1) composed of matrix of paired comparisons

$$A=\begin{bmatrix} 1 & 4 & 6 & 7 \\ 1/4 & 1 & 3 & 4 \\ 1/6 & 1/3 & 1 & 2 \\ 1/7 & 1/4 & 1/2 & 1 \end{bmatrix}.$$

The first step we find the eigenvector *w* for which the condition $Aw = \lambda w$. It is necessary to find the values λ, in which the determinant of the matrix $(A - \lambda E)$ is equal to zero. We write the equation

$$\begin{bmatrix} 1-\lambda & 4 & 6 & 7 \\ 1/4 & 1-\lambda & 3 & 4 \\ 1/6 & 1/3 & 1-\lambda & 2 \\ 1/7 & 1/4 & 1/2 & 1-\lambda \end{bmatrix} = \lambda^4 - 4\lambda^3 - 1,687\lambda - 0,133 = 0,$$

solving which, we find its roots:

$$\lambda_1 = -0,782;\ \lambda_2 = 0,12 - 0,645i;\ \lambda_3 = -0,12 + 0,645i;\ \lambda_4 = 4,102.$$

Therefore, $\lambda_{max} = 4,102$.

Next, go to the find module eigenvector w, appropriate found your own value λ_{max}. For this purpose, we solve the matrix equation:

$$\begin{bmatrix} -3,102 & 4 & 6 & 7 \\ 1/4 & -3,102 & 3 & 4 \\ 1/6 & 1/3 & -3,102 & 2 \\ 1/7 & 1/4 & 1/2 & -3,102 \end{bmatrix} \cdot \begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ w_4 \end{bmatrix} = 0,$$

which for computational convenience is convertible to normal:

$$\begin{cases} -3.102w_1 + 4w_2 + 6w_3 + 7w_4 = 0; \\ 0.25w_1 - 3.102w_2 + 3w_3 + 4w_4 = 0; \\ 0.166w_1 + 0.333w_2 - 3.102w_3 + 2w_4 = 0; \\ 0.142w_1 + 0.25w_2 + 0.5w_3 - 3.102w_4 = 0; \end{cases}$$

at $w_1 + w_2 + w_3 + w_4 = 1$.

Since this system of equations has only the trivial solution, then for finding the eigenvector w model one of the equations by the normalization condition for the $\sum_{i=1}^{4} w_i = 1.$. By solving the resulting system we get eigenvector:

$$w_1 = 0.617;\ w_2 = 0.224;\ w_3 = 0.097;\ w_4 = 0.062$$
$$(\text{при } \lambda_{max} = 4,102).$$

The obtained results allow to construct a function $\mu(E_i)$, characterizing the grade of membership function values $E_i(t)$ at time t to one of the graduations of zero – w_1, low level – w_2, normal level – w_3, a high level – w_4, presented in figure 1.

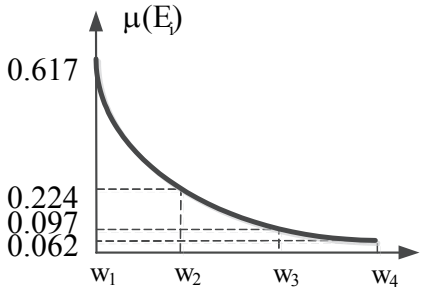

Figure 1 – membership function of fuzzy evaluation value $E_i(t)$

As can be seen from this figure, the degree of belonging of security of the i-th object from unauthorized access to ground level is 52%, to a low of 22% to a normal level of 10% and to a high level – 5%. In the terminology accepted in the theory of fuzzy sets, the evaluation expressed by the formula:

$E_i(t) = 0.52$ / ⟨ the zero level ⟩ +0.22 / ⟨ low level ⟩ + 0,01 / ⟨ normal level ⟩ + 0,05 / ⟨ a high level ⟩.

Conclusion: the most probable, we must assume that at a given moment of time the i-th module of the software infocommunication systems subject to destructive influences will be infected by the malicious software introduced by the cyber criminals.

5 The algorithm risk assessment functional stability

The proposed method of analysis of the current functionality of the software module information and communication system allows and without conducting numerical experiments to give a rapid assessment of the risk of violation of stability of the system as a result of destructive impacts [12]. This push from the concept of stationary equilibrium equations describing the dynamics of the process, treating it in the following way: the process described by (3) or (4), has the property of equilibria, if $t \to \infty$ this system of equations has a solution with coordinates $(E_1^*,...,E_{N+K+M}^*)$, otherwise, i.e. when (3) or (4) does not have solutions, the process has no stationary equilibrium. The lack of stationary equilibrium in the equations describing the studied process, suggests that the functioning of the software infocommunication systems under the influence of destructive impacts occur in the transition transient regime, the system that fails (partially or completely), then enters into the mode of normal operation. The risk of loss of stability is characterized as "undetermined."

The presence in the system of equations (3) or (4) the point or area stationary equilibrium eliminates this uncertainty and suggests that:

a) if $\underset{i=1}{\overset{N}{\forall}}\left(E_i^* \gg 0\right)$, the risk of loss of stability software infocommunication systems from destructive influences can be described as "normal";

б) if $\underset{i=1}{\overset{N}{\forall}}\left(E_i^* \le 0\right)$, the risk of loss of stability software infocommunication systems from destructive influences can be described as "maximum";

Based on the foregoing, the formula for risk assessmen (R) loss of stability of information and communication systems as a result of destructive effects, can be written in the following form:

$$R = \begin{cases} \text{"undefined"} - \text{if } (5.3)-(5.4) \text{ there is no point of stationary equilibrium;} \\ \text{"normal"} - \text{if } (5.3)-(5.4) \text{there is a point of stationary equilibrium and } \underset{i=1}{\overset{N}{\forall}}\left(E_i^* \gg 0\right) \\ \text{"maximum"} - \text{if } (5.3)-(5.4) \text{ there is a point of stationary equilibrium, but } \underset{i=1}{\overset{N}{\forall}}\left(E_i^* \le 0\right). \end{cases} \quad (7)$$

In the case where the risk according to the formula (5.7) is evaluated as "normal", it is possible to switch to a more accurate assessment. The reasoning in this case is as follows. Let the operation of information communication systems occurs in the linear $N+K+M$ - dimensional phase space with coordinates $\langle E_1,...,E_{N+K+M}\rangle$. Let this process has a stationary equilibrium point with coordinates $(E_1^*,...,E_{N+K+M}^*)$, and his current position at the time t is specified by coordinates $[E_1(t),...,E_N(t)]$. When rating current level of risk of loss of stability R(t) you can be guided by the following rule [4] farther the trajectory of the process from the point of stationary equilibrium, the greater the risk, and, conversely, the closer "pressed" trajectory of the process to the point of equilibrium, the less risk. Then an assessment of the risk of loss of stability software infocommunication systems as a result of destructive impacts on point in time can be obtained using the formula [7]:

$$R(t) = \left\{ \frac{1}{R^*} \sqrt{\sum_{i=1}^{N} \left[E_i^* - E_i(t) \right]^2} \right\} 100\%, \quad (8)$$

where $R^* = \sqrt{\sum_{i-1}^{N} \left(E_i^*\right)^2}$.

Thus, the risk of buckling of the software infocommunication systems from the destructive effects obtained by implementing the following algorithm, presented in figure 2.

Step 1. The input source data of the current functionality.

Step 2. We write the system of differential equations (3) or (4) describing the dynamics of the process of cyberbully.

Step 3. Based on the initial conditions and the initial data produced by the analysis (3) or (4) to determine the point of stationary equilibrium, determined by the coordinates of this point $(E_1^*,...,E_{N+K+M}^*)$.

Step 4 and 5. Using the formula (7), estimate the level of risk in qualitative gradations of "normal", "uncertain", "maximum". If you find that the level of risk is "uncertain" or "maximum" assessment completed.

Step 6. If R = «normal», then, solving the system of differential equations (3) or (4) using a numerical method, the determined values of the coordinates of the current process $[E_1(t),...,E_{N+K+M}(t)]$.

Step 7. Using the formula (5) evaluate the risk at the time t.

As can be seen from this algorithm, when assessing the risk of loss of stability software infocommunication systems from destructive impacts it becomes necessary to determine the conditions under which the process described by (3) or (4) has a point of stationary equilibrium. For (4) this question we already considered. Consider it to (3).

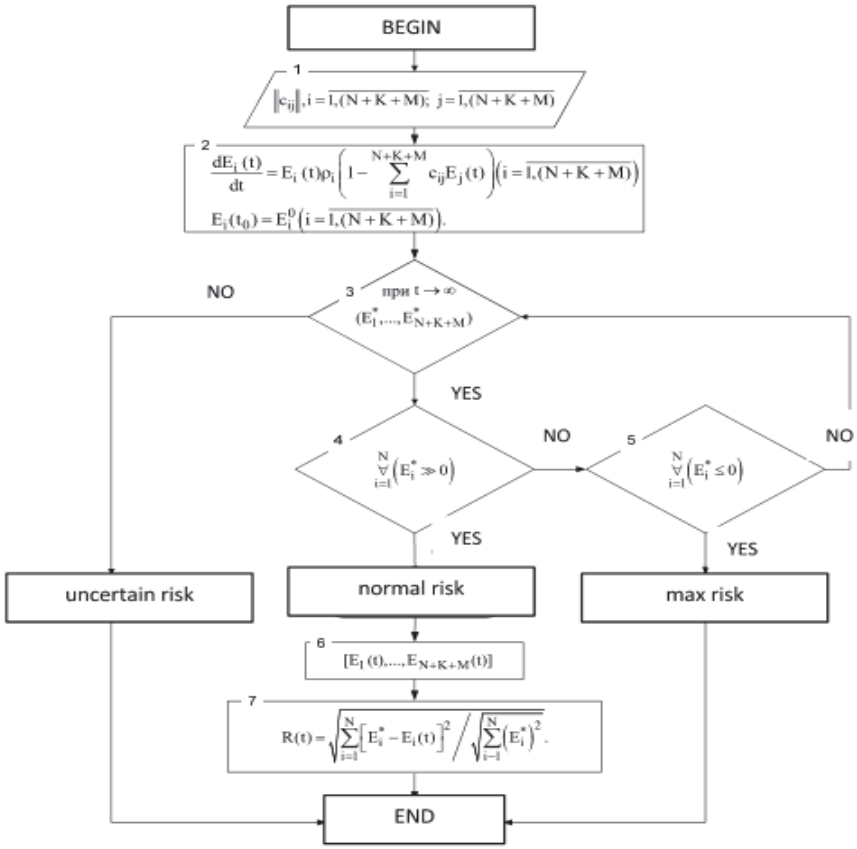

Figure 2 — The algorithm of risk assessment of functional stability

From (5.3) we see that the coordinates of the point it is a stationary equilibrium solutions of the following system of linear algebraic equations:

$$\sum_{j=1}^{N+K+M} c_{ij}E_j = 1(i=\overline{1,(N+K+M)}). \qquad (9)$$

We illustrate what has been said with an example. Let the software be some conditional infocommunication systems consists of three modules, the relationships between which are characterized by the coefficients

$$(c_{ij})=\begin{pmatrix}1,0 & 0,5 & 0,3\\ 0,7 & 1,0 & 0,5\\ 0,4 & 0,6 & 1,0\end{pmatrix}.$$

Using (9), we obtain the system of equations

$$\left.\begin{aligned}1.0x_1+0.5x_2+0.3x_3=1\\ 0.7x_1+1.0x_2+0.5x_3=1\\ 0.4x_1+0.6x_2+1.0x_3=1\end{aligned}\right\},$$

for which, as is easily seen, rightly (11) as

$$\Delta = \begin{vmatrix} 1.0 & 0.5 & 0.3 \\ 0.7 & 1.0 & 0.5 \\ 0.4 & 0.6 & 1.0 \end{vmatrix} = 0,53 > 0\ ; \quad \Delta_1 = \begin{vmatrix} 1.0 & 0.5 & 0.3 \\ 1.0 & 1.0 & 0.5 \\ 1.0 & 0.6 & 1.0 \end{vmatrix} = 0,33 > 0\ ;$$

$$\Delta_2 = \begin{vmatrix} 1.0 & 1.0 & 0.3 \\ 0.7 & 1.0 & 0.5 \\ 0.4 & 1.0 & 1.0 \end{vmatrix} = 0,09 > 0\ ; \quad \Delta_3 = \begin{vmatrix} 1.0 & 0.5 & 1.0 \\ 0.7 & 1.0 & 1.0 \\ 0.4 & 0.6 & 1.0 \end{vmatrix} = 0,27 > 0\ ,$$

and thus runs the necessary and sufficient condition for a stationary equilibrium of the considered process. In this case the only equilibrium point $\left(E_1^*, E_2^*, E_3^*\right)$ has coordinates (0.52, 0.14, 0.43), which suggests that the risk of loss of stability in such a system is not beyond the norm.

$$E_1^* = \frac{\begin{vmatrix} 1 & & \alpha_{1(N+K+M)} \\ \dots & \dots & \dots \\ 1 & & \alpha_{(N+K+M)(N+K+M)} \end{vmatrix}}{\Delta}, \dots, E_{N+K+M}^* = \frac{\begin{vmatrix} \alpha_{11} & \dots & 1 \\ \dots & \dots & \dots \\ \alpha_{(N+K+M)1} & \dots & 1 \end{vmatrix}}{\Delta}. \tag{10}$$

It follows that a necessary and sufficient condition under which the process described by (3) has a point of stationary equilibrium, it is inequality to zero of the determinant of the system of equations (9), and coincidence of characters $\Delta_1, \dots, \Delta_N$, standing in the numerator of the formula (10), with the sign of the determinant Δ. In formal way this condition can be written as:

$$\{\Delta \neq 0\} \wedge \left\{ \bigwedge_{i=1}^{N+K+M} \left[\operatorname{sign}(\Delta_i) = \operatorname{sign}(\Delta) \right] \right\}. \tag{11}$$

The method of evaluation of the current functionality of the software modules of infocommunication systems and an algorithm for assessing the risk of loss of stability is inextricably linked with the concept of stationary equilibrium equations describing the considered process. It is possible to introduce a metric based on the following rules: the farther is located the trajectory of the process from the point of equilibrium, the greater the risk, and, conversely, the less risk the closer "pressed" trajectory of the process to the point of equilibrium.

By default, it was about the local stability of the process of functioning of information and communication systems. But as we know from the General theory of control [5], local stability of stationary equilibrium does not necessarily follow its global stability, that is convergence of the solution (3) or (4) the coordinates $(E_1^*, \dots, E_{N+K+M}^*)$ from any point $(E_1^0, E_2^0, \dots, E_{N+K+M}^0)$ $N+K+M$ - dimensional phase space $\langle E_1, \dots, E_{N+K+M} \rangle$. For example, information communication systems, software consists of three software modules, and the functioning of which is described by the equations

$$\left.\begin{aligned} \frac{dE_1(t)}{dt} &= E_1(t)\left[2.0 - 0.8E_1(t) - 0.7E_2(t) - 0.5E_3(t)\right]; \\ \frac{dE_2}{dt} &= E_2(t)\left[2.1 - 0.2E_1(t) - 0.9E_2(t) - E_3(t)\right]\ ; \\ \frac{dE_3}{dt} &= E_3(t)\left[1.5 - E_1(t) - 0.3E_2(t) - 0.2E_3(t)\right]\ , \end{aligned}\right\}, \tag{12}$$

fixed point $(E_1^*, \dots, E_{N+K+M}^*)$ = (1.0, 1.0, 1.0) is locally but not globally stable because, for example, from the initial point with coordinates (0.5, 1.0, 2.0), the process proceeds not to the point (1.0, 1.0, 1.0), and to the point (0.0, 0.0, 0.75). In such cases, we can assume that for the operation of the software module information and communication systems in terms of destructive impacts will be characterized by the cyclic mode, when the system is to perform its functions, then enter the zone of failure.

To determine the conditions under which local stability of stationary equilibrium is always followed by global stability, we use theorem V. Voltaire [5]. This theorem States: positive steady state of a dissipative system is globally stable. Explain its meaning. Dissipative (by Voltaire) is a system of equations of the form (3) or (4), if there exists a set of $(N+K+M)$ positive numbers $\xi_1, \dots, \xi_N$, that the quadratic form

$$\Phi\left(E_1, \dots, E_{N+K+M}\right) = \sum_{i,j=1}^{N+K+M} \xi_i b_{ij} E_i E_j \tag{13}$$

under any valid $(E_1,...,E_{N+K+M})$ takes negative values, i.e. it is negative definite: $\Phi(E_1,...,E_{N+K+M}) < 0$. Therefore, in order to ensure that the positive stationary point of equation (3) or (4) is globally stable, it is necessary to calculate (13) and show that it is negative definite. For the practical implementation of this operation should switch from (13) to its equivalent form

$$\Phi(E_1,...,E_{N+K+M}) = \sum_{i,j=1}^{N+K+M} \tilde{b}_{ij} E_i E_j, \tag{14}$$

where $\tilde{b}_{ij} = \frac{1}{2}(\xi_i b_{ij} + \xi_i b_{ji})$.

Then the condition for negative definiteness of the quadratic form (13) takes a fairly simple view. It boils down to the requirement that all principal minors of the matrix $-\tilde{B} = (-\tilde{b}_{ij})$ was positive, i.e.

$$-\tilde{b}_{11} > 0, \begin{vmatrix} -\tilde{b}_{11} & -\tilde{b}_{12} \\ -\tilde{b}_{21} & -\tilde{b}_{22} \end{vmatrix} > 0, ...,$$
$$\begin{vmatrix} -\tilde{b}_{11} & -\tilde{b}_{12} & ... & -\tilde{b}_{1(N+K+M)} \\ -\tilde{b}_{21} & -\tilde{b}_{22} & ... & -\tilde{b}_{2(N+K+M)} \\ ... & ... & ... & ... \\ -\tilde{b}_{(N+K+M)1} & -\tilde{b}_{(N+K+M)2} & ... & -\tilde{b}_{(N+K+M)(N+K+M)} \end{vmatrix} > 0. \tag{15}$$

It is easy to show that (15) is equivalent to the following inequality is satisfied

$$(\tilde{b}_{jj} \times \tilde{b}_{kk}) > \left[\left(\sum_{\substack{i=1 \\ i \neq j}}^{N+K+M} |\tilde{b}_{ij}| \right) \left(\sum_{\substack{i=1 \\ i \neq k}}^{N+K+M} |\tilde{b}_{ik}| \right) \right] (i \neq k, j, k = 1,...,(N+K+M)). \tag{16}$$

If the condition (16) possible deviations software infocommunication systems from the standard mode of operation will be temporary in nature. After some time (depending on the inertial properties of software modules), despite the destructive impacts, software infocommunication systems will return to normal operation mode.

Conclusion

Proposed method of analysis of the functional stability of the software infocommunication systems in terms of destructive impacts developed in two ways: quantitative – based on the use of the theory of integro-differential calculus, and quality – based on the theory of fuzzy sets. This is done in order to fend off uncertainty about the source of the data needed to solve the problem, as well as for hedging in case of loops standard programs designed for solving large systems of nonlinear differential equations.

Using this method has allowed us to develop an algorithm for the rapid evaluation of risk of violation of the functional stability of the software infocommunication systems from destructive attacks [12]. The idea of this algorithm is that the concept of stability is associated with the concept of stationary equilibrium equations describing the function of the software infocommunication systems. It is possible to introduce a metric based on the following rules: the farther is located the trajectory of the estimated process from the point of equilibrium, the greater the risk, and, conversely, the less risk the closer "pressed" trajectory of the process to the point of equilibrium.

In general, the above material suggests that using mathematical tools can adequately simulate the operation of the software infocommunication systems in terms of destructive impacts, and to formulate and solve the problem of stabilization of the process in real time.

The developed method may be used for the design of advanced systems to detect and counter cyber attacks. For example, this method can be used to use the quick risk evaluation of the functional stability of information and communication systems in terms of cyber attacks.

In this case, you might encounter the following problem which may need the intervention of man can professionally and psychologically to cope with the task, to achieve the maximum effect of protecting transmitted and processed information [13]. The following stage of countering cyber attacks can serve as tools of diagnosing the state of the actuators of the system [14] and intelligent security system using artificial intelligence, using the conceptual approaches of the immune system [15], which will help to reduce the impact of negative effects on the information system from cyber attacks [16]. Further research is needed to develop a methodology description of the information process as a discrete stream [17] for the subsequent evaluation of the effectiveness of all systems support the activities of information and communication systems in terms of cyber attacks. But it is not included in the scope of this article, so we look forward to further scientific cooperation of authors and commend the leaders of the scientific project.

References

[1] 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.

[2] 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.

[3] 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.

[4] V.I. Novoseltsev, T.I. Kasatkina, A.V. Dushkin, 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.

[5] T.I. Kasatkina , A.V. Dushkin , 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.

[6] 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.

[7] S.S. Kochedykov, A.V. Dushkin, 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.

[8] E.V. Grechishnikov, M.M. Dobryshin, S.S. Kochedykov and V.I. Novoselcev. Algorithmic model of functioning of the system to detect and counter cyber attacks on virtual private network // IOP Conf. Series: Journal of Physics: Conf. Series 1203 "Applied Mathematics, Computational Science and Mechanics: Current Problems", 2019. – DOI: 10.1088/1742-6596/1203/1/012064.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] I.V. Goncharov, N.I. Goncharov, P.A. Parinov, S.S. Kochedykov, A.V. Dushkin. Probabilistic Analysis of the Influence of Staff Qualification and Information-Psychological Conditions on the Level of Systems Information Security Probabilistic Analysis of the Influence of Staff Qualification and Information-Psychological Conditions on the Level of Systems Information Security // Probabilistic Modeling in System Engineering. UK, London: IntechOpen, pp. 233-253. – DOI: 10.5772/intechopen.75079.

[14] 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.

[15] L.V. Stepanov, E.V. Grechishnikov, V.I. Novoseltsev and S.S. Kochedykov. Conceptual approach to building information security systems for telecommunication systems using artificial immune systems // IOP Conf. Series: Journal of Physics: Conf. Series 1202 “International Scientific Conference on Informatics: Problems, Methodologies and Technologies”, 2019. – DOI: 10.1088/1742-6596/1202/1/012031.

[16] Yu.Yu. Gromov, V.I. Sumin, S.S. Kochedykov and V.I. Novoselcev. Evaluating the efficiency of mitigation tools against negative external actions on the information system // IOP Conf. Series: Journal of Physics: Conf. Series

1203 International Conference "Applied Mathematics, Computational Science and Mechanics: Current Problems", 2019. – DOI: 10.1088/1742-6596/1203/1/012078.
[17] V.I. Sumin, T.E. Smolentseva, S.S. Kochedykov and V.S. Zarubin. Description of the information process as a discrete stream // IOP Conf. Series: Journal of Physics: Conf. Series 1202 "International Scientific Conference on Informatics: Problems, Methodologies and Technologies", 2019. – DOI: 10.1088/1742-6596/1202/1/012016.
[18] 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.
[19] 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.